PWPW
POLSKA WYTWÓRNIA
PAPIERÓW WARTOŚCIOWYCH

POLITYKA PCCE DLA CERTYFIKATÓW

OID: {1 2 616 1 113560 10 3 1 0}

Symbol Dokumentu: P3.032

Data: 04.01.2017 r.

Wersja: 1.6

Spis treści

1 Słownik używanych określeń

1) Ustawa - Ustawa o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września2016 r. (Dz. U. 20016 poz. 1579).
2) Polityka certyfikacji – niniejsza polityka certyfikacji.
3) Polska Wytwórnia Papierów Wartościowych S.A. – Polskie Centrum Certyfikacji Elektronicznej „Sigillum" – podmiot świadczący usługi certyfikacyjne w zakresie objętym niniejszą polityką nazywany dalej Sigillum PCCE.

   Sigillum PCCE świadczy także inne usługi certyfikacyjne, w tym kwalifikowane usługi certyfikacyjne polegające na wystawianiu certyfikatów oraz kwalifikowane usługi certyfikacyjne polegające na wystawianiu znaczników czasu, jednak działalność Sigillum PCCE w tym zakresie nie jest uregulowana niniejszą polityką certyfikacji.
4) Punkt rejestracji – jednostka organizacyjna działająca w imieniu Polskiej Wytwórni Papierów Wartościowych S.A. - Sigillum PCCE, wykonująca zgodnie z niniejszą polityką niektóre funkcje związane ze świadczeniem usług certyfikacyjnych.
5) Algorytm RSA – algorytm kryptograficzny określony jednoznacznie przez identyfikator obiektu „{ joint-iso-ccitt (2) ds. (5) module (1) algorithm (8) encryptionAlgorithm (1) 1 }".
6) Klucz – liczba, symbol lub ciąg liczb lub symboli jednoznacznie wyznaczający przekształcenie kryptograficzne spośród rodziny przekształceń zdefiniowanej przez algorytm kryptograficzny.
7) Para kluczy algorytmu RSA – dwa klucze (*klucz prywatny* i *klucz publiczny*) wyznaczające wzajemnie odwrotne przekształcenia spośród rodziny przekształceń zdefiniowanej przez algorytm RSA.
8) Klucz podpisujący – klucz prywatny służący do składania podpisu elektronicznego; klucz podpisujący stanowi dane służące do składania podpisu elektronicznego w rozumieniu Ustawy.
9) Klucz weryfikujący podpis – klucz publiczny służący do weryfikowania podpisu elektronicznego; klucz weryfikujący podpis stanowi dane służące do weryfikacji podpisu elektronicznego lub dane służące do weryfikacji poświadczenia elektronicznego w rozumieniu Ustawy.
10) Klucz deszyfrujący – klucz prywatny służący do deszyfrowania.
11) Klucz szyfrujący – klucz publiczny służący do szyfrowania.
12) Klucze infrastruktury – klucze kryptograficzne algorytmów kryptograficznych stosowane do innych celów niż składanie lub weryfikacja podpisu elektronicznego lub poświadczenia elektronicznego, a w szczególności klucze stosowane:
    a. w protokołach uzgadniania lub dystrybucji kluczy zapewniających poufność danych,

b. do zapewnienia, podczas transmisji lub przechowywania, poufności i integralności zgłoszeń certyfikacyjnych, kluczy użytkowników, rejestrów zdarzeń,

c. do weryfikacji dostępu do urządzeń, oprogramowania weryfikującego lub podpisującego.

13) Certyfikat klucza weryfikującego podpis – elektroniczne zaświadczenie, za pomocą którego klucz weryfikujący podpis jest przyporządkowany do osoby składającej podpis elektroniczny i które umożliwia identyfikację tej osoby.

14) Certyfikat klucza szyfrującego – elektroniczne zaświadczenie, za pomocą którego klucz szyfrujący jest przyporządkowany do osoby będącej adresatem tych danych i posiadającej możliwość odczytania zaszyfrowanych danych.

15) Certyfikat klucza publicznego – certyfikat klucza weryfikującego podpis lub certyfikat klucza szyfrującego.

16) Poświadczenie elektroniczne – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane umożliwiają identyfikację podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne, oraz spełniają następujące wymagania:

a. są sporządzone za pomocą podlegających wyłącznej kontroli podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne urządzeń służących do składania podpisu elektronicznego i danych służących do składania poświadczenia elektronicznego;

b. jakakolwiek zmiana danych poświadczonych jest rozpoznawalna.

17) Zaświadczenie certyfikacyjne – elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do podmiotu świadczącego usługi certyfikacyjne i które umożliwia identyfikację tego podmiotu lub organu.

18) Ścieżka certyfikacji - uporządkowany ciąg zaświadczeń certyfikacyjnych lub zaświadczeń certyfikacyjnych i certyfikatu 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 certyfikatu poświadczenie elektroniczne zawarte w jednym z nich zostało sporządzone przy pomocy danych służących do składania poświadczenia elektronicznego związanych z drugim z nich; dane służące do weryfikacji pierwszego poświadczenia elektronicznego są dla weryfikującego „punktem zaufania".

19) Punkt zaufania – patrz „ścieżka certyfikacji".

20) Lista CRL – lista unieważnionych i zawieszonych certyfikatów klucza publicznego wystawionych przez dany podmiot świadczący usługi certyfikacyjne oraz ewentualnie unieważnionych zaświadczeń certyfikacyjnych wystawionych przez ten podmiot. Lista jest poświadczona elektronicznie przez podmiot świadczący usługi certyfikacyjne.

21) Lista ARL – lista unieważnionych zaświadczeń certyfikacyjnych wystawionych przez dany podmiot świadczący usługi certyfikacyjne. Lista jest poświadczona elektronicznie przez podmiot świadczący usługi certyfikacyjne. Podmiot nie musi wystawiać listy ARL, jeśli informacje o unieważnionych zaświadczeniach certyfikacyjnych zawiera w wystawianej przez siebie liście CRL.

22) Subskrybent usług certyfikacyjnych – osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która zawarła z Sigillum PCCE umowę o świadczenie usług certyfikacyjnych i której imię, nazwisko, pseudonim lub nazwa została umieszczone w certyfikacie.

23) Strona ufająca – osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która w granicach określonych w polityce certyfikacji może działać w oparciu o certyfikat lub zaświadczenie certyfikacyjne. Stroną ufającą jest również subskrybent, jeśli wykonuje działania w oparciu o wystawiony zgodnie z niniejszą polityką certyfikat lub zaświadczenie certyfikacyjne.

24) Odbiorca usług certyfikacyjnych - subskrybent usług certyfikacyjnych lub strona ufająca.

25) Sponsor certyfikatu – osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej lub organ władzy publicznej, którego dane zostały umieszczone w certyfikacie, w imieniu której działa subskrybent posługując się certyfikatem. Sponsor certyfikatu finansuje usługi certyfikacyjne świadczone na rzecz danego subskrybenta. Ma on prawo unieważnić certyfikat jeśli jego dane znajdują się w certyfikacie (art. 21 ust. 2 pkt. 5 Ustawy). Ilekroć w niniejszej Polityce używana jest definicja „Sponsor" rozumie się przez to podmiot określany mianem „Zamawiający" w Umowach o świadczenie usług certyfikacyjnych i innej dokumentacji.

26) Kwalifikowane usługi certyfikacyjne – usługi certyfikacyjne świadczone przez podmiot posiadający wpis w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne, zgodnie z polityką odpowiadającą temu wpisowi.

27) Komponent techniczny - sprzęt stosowany w celu wygenerowania lub użycia danych służących do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego.

28) Moduł kluczowy – urządzenie współpracujące z komponentem technicznym, przechowujące klucze infrastruktury lub dane służące do składania bezpiecznych podpisów elektronicznych lub poświadczeń

elektronicznych, lub klucze chroniące te dane, lub przechowujące części tych kluczy lub danych.

29) Bezpieczne urządzenie służące do weryfikacji podpisu elektronicznego – urządzenie służące do weryfikacji podpisu elektronicznego spełniające wymagania określone w Ustawie.

Określenia wykorzystywane w niniejszej polityce certyfikacji, a niezdefiniowane powyżej należy interpretować zgodnie z definicjami zawartymi w Ustawie.

2 Wprowadzenie

Niniejszy dokument stanowi politykę certyfikacji Sigillum Polskiego Centrum Certyfikacji Elektronicznej , w zakresie świadczenia usług certyfikacyjnych polegających na wystawianiu certyfikatów.

Niniejszą politykę certyfikacji należy rozpatrywać łącznie z odpowiadającym jej regulaminem certyfikacji, opracowanym i opublikowanym przez Sigillum PCCE.

Celem świadczenia przez Sigillum PCCE usług certyfikacyjnych, obok usług kwalifikowanych, jest udostępnienie klientom Sigillum PCCE szerszego wachlarza możliwości zastosowań certyfikatów, niż jest to przewidziane w Ustawie o podpisie elektronicznym.

We wszystkich aspektach, w których jest to możliwe, świadczenie usług certyfikacyjnych przez Sigillum PCCE podlega takim samym rygorom bezpieczeństwa, jakie są przewidziane w Ustawie w stosunku do certyfikatów kwalifikowanych. Różnice w wymaganiach bezpieczeństwa w stosunku do wymagań nałożonych Ustawą występują jedynie tam, gdzie jest to niezbędne dla obsługi innych klas certyfikatów, nie obejmowanych ustawową definicją kwalifikowanych certyfikatów. W szczególności mechanizmy i procedury stosowane w celu ochrony klucza prywatnego Sigillum PCCE służącego do wystawiania certyfikatów zgodnie z niniejszą polityką, jak również procedury weryfikacji tożsamości potencjalnego subskrybenta – osoby fizycznej, spełniają wymogi Ustawy.

2.1 Ważne informacje dla subskrybentów i stron ufających

Każdy odbiorca usług certyfikacyjnych świadczonych przez Sigillum PCCE ma obowiązek zapoznania się i zrozumienia niniejszego dokumentu. Subskrybent ma obowiązek zapoznania się z dokumentem przed podpisaniem umowy o świadczenie usług certyfikacyjnych, natomiast strona ufająca przed użyciem jakiegokolwiek certyfikatu klucza publicznego lub innych danych poświadczonych elektronicznie przez Sigillum PCCE wystawionych zgodnie z niniejszą polityką certyfikacji.

2.2 Identyfikator polityki

Nazwa polityki	Polityka PCCE dla certyfikatów
Kwalifikator polityki	Polityka PCCE dla certyfikatów
Wersja polityki	1.5
Status wersji	finalna
Numer referencyjny /OID (ang. *Object Identifier*)	{ iso(1) member-body(2) PL(616) organisation(1) Sigillum-Polskie Centrum Certyfikacji Elektronicznej(113560) polityki certyfikacji(10) 3 1 0 }

Data wprowadzenia w życie	05.01.2017 r.
Data wygaśnięcia	Do odwołania
Odnośny Regulamin Certyfikacji	Regulamin PCCE dla certyfikatów

W celu uzyskania dalszych informacji dotyczących usług Sigillum PCCE prosimy o kontakt z:

Polska Wytwórnia Papierów Wartościowych S.A.

Sigillum Polskie Centrum Certyfikacji Elektronicznej

00-222 Warszawa, ul. Sanguszki 1

e-mail: sigillum@pwpw.pl,

www.sigillum.pl

tel: +48 prefix 22 530 2756

2.3 Rozpatrywanie skarg

Skargi na działalność punktów rejestracji oraz działalność Sigillum PCCE są rozpatrywane przez Kierownika Sigillum PCCE.

Adresy kontaktowe do Sigillum PCCE zostały zamieszczone w rozdziale 2.2.

3 Profil certyfikacji

W ramach niniejszej polityki certyfikacji Sigillum PCCE wystawia następujące rodzaje certyfikatów kluczy publicznych subskrybentów usług certyfikacyjnych:

1. certyfikaty służące do weryfikacji podpisów elektronicznych w poczcie elektronicznej o następującym poziomach odpowiedzialności:
    - certyfikat Sigillum Basic bez gwarancji finansowych,
    - certyfikat Sigillum Professional o gwarancji do 20.000 zł,
    - certyfikat Sigillum VIP o gwarancji do 100.000 zł;
2. certyfikaty do zapewniania poufności danych;
    - certyfikat Sigillum Cryptogram bez gwarancji finansowych
3. certyfikaty służące do weryfikacji podpisów elektronicznych w poczcie elektronicznej oraz do zapewnienia poufności danych w poczcie elektronicznej o następujących poziomach odpowiedzialności w przypadku weryfikacji podpisów elektronicznych w poczcie elektronicznej:
    - certyfikat Sigillum Basic bez gwarancji finansowych,
    - certyfikat Sigillum Professional o gwarancji do 20.000 zł,
    - certyfikat Sigillum VIP o gwarancji do 100.000 zł;
4. certyfikaty obiektowe - służące do uwierzytelnienia oraz zapewnienia poufności w komunikacji z serwerem:
    - certyfikat Sigillum Serwer o gwarancji do 200.000 zł;
5. certyfikaty służące do weryfikacji podpisów elektronicznych służących do zapewniania integralności i autentyczności kodu aplikacji
    - certyfikat Sigillum Code Sign bez gwarancji finansowych
6. certyfikaty umożliwiające logowanie użytkowników do systemów informatycznych
    - certyfikaty Sigillum Login bez gwarancji finansowych

W przypadku certyfikatów Sigillum Basic dopuszcza się możliwość dołączenia opcji umożliwiających logowanie użytkowników do systemów informatycznych.

Sigillum PCCE, zgodnie z niniejszą polityką, może wystawiać również:

1. zaświadczenia certyfikacyjne kluczy publicznych dla innych centrów certyfikacji (certyfikacja wzajemna lub hierarchia centrów certyfikacji) lecz tylko wtedy, gdy centrum, którego klucz publiczny ma się znaleźć w zaświadczeniu spełnia wymagania niniejszej polityki;

2. samopodpisane zaświadczenia certyfikacyjne (tzw. *autocertyfikaty*) – służące do zapewnienia integralności przy dystrybucji kluczy publicznych Sigillum PCCE, wykorzystywanych do weryfikacji zaświadczeń certyfikacyjnych i certyfikatów wystawianych zgodnie z niniejszą polityką;
3. zaświadczenia certyfikacyjne służące – przy wymianie kluczy Sigillum PCCE – do poświadczenia nowego klucza publicznego Sigillum PCCE przy użyciu dotychczasowej pary kluczy Sigillum PCCE oraz do poświadczenia dotychczasowego klucza publicznego Sigillum PCCE przy użyciu nowej pary kluczy Sigillum PCCE (tzw. *certyfikaty zakładkowe*);
4. certyfikaty kluczy publicznych służących do zapewnienia niezaprzeczalności nadania, uwierzytelnienia i zapewnienia poufności w wymianie informacji pomiędzy podmiotami funkcjonującymi w ramach Sigillum PCCE.

Subskrybentami usług certyfikacyjnych realizowanych zgodnie z niniejszą polityką certyfikacji mogą być osoby fizyczne spełniające wymagania określone w Ustawie. Osoby te mogą występować w imieniu własnym lub w imieniu innych podmiotów („sponsorów"). Informacja o roli subskrybenta jest umieszczana w certyfikatach kluczy publicznych.

Przed wystawieniem certyfikatu pomiędzy każdym z subskrybentów a Sigillum PCCE zostaje zawarta umowa o świadczenie usług certyfikacyjnych. Umowa musi być podpisana własnoręcznie przez subskrybenta lub odpowiednio umocowanego reprezentanta subskrybenta (w przypadku osób prawnych i jednostek organizacyjnych) oraz osobę reprezentującą Sigillum PCCE.

Przed wystawieniem certyfikatu, tożsamość subskrybenta lub odpowiednio przedstawiciela subskrybenta jest weryfikowana na podstawie ważnego dowodu osobistego lub paszportu, spełniających funkcje dokumentów podstawowych. Dodatkowym dokumentem akceptowanym przy weryfikacji tożsamości subskrybenta jest prawo jazdy wydane po 1 lipca 1999 roku.

Niniejsza Polityka dopuszcza notarialne potwierdzenie tożsamości Subskrybenta i/lub Zamawiającego. W takim przypadku Subskrybent i/lub Zamawiający składa podpis własnoręczny w obecności notariusza na wymaganych dokumentach, co notariusz potwierdza, a następnie Subskrybent i/lub Zamawiający dostarcza tak przygotowany komplet dokumentów do Sigillum PCCE.

W szczególnych przypadkach (wydzielony projekt) dopuszcza się wydawanie certyfikatu bez zawarcia umów subskrybenckich. Warunkiem jest zawarcie Umowy głównej, której zapis przenosi pełną odpowiedzialność za: weryfikację tożsamości osób odbierających certyfikat, poprawność danych zawartych w certyfikatach oraz prawidłowość procesu wydania certyfikatu, na zamawiającego.

Sigillum PCCE, realizując niniejszą politykę certyfikacji, może działać samodzielnie lub za pośrednictwem punktów rejestracji. Punktami rejestracji mogą być jednostki organizacyjne PWPW SA, a także osoby fizyczne, prawne i jednostki organizacyjne nieposiadające osobowości prawnej, po podpisaniu stosownej umowy z Sigillum PCCE. Kompetencje punktów rejestracji mogą dotyczyć obsługi odbiorców usług certyfikacyjnych, w tym generowania kluczy subskrybentów, a także podejmowania decyzji o wystawieniu, zawieszeniu, uchyleniu zawieszenia bądź unieważnieniu certyfikatu. Kompetencje punktów rejestracji nie mogą obejmować w szczególności posługiwania się kluczem prywatnym służącym do wystawiania certyfikatów zgodnie z niniejszą polityką, generowania certyfikatów i zaświadczeń certyfikacyjnych, generowania list CRL, a także publikowania certyfikatów, zaświadczeń certyfikacyjnych i list CRL.

Niniejszą politykę certyfikacji należy rozpatrywać łącznie z odpowiadającym jej regulaminem certyfikacji, opracowanym i opublikowanym przez Sigillum PCCE.

Niniejsza polityka certyfikacji stanowi własność intelektualną PWPW SA, podmioty inne niż Sigillum PCCE nie mają prawa do wystawiania certyfikatów zawierających oznaczenia zgodności z niniejszą polityką bez uprzedniej zgody Sigillum PCCE.

4 Postanowienia polityki certyfikacji

4.1 Użytkownicy i zastosowanie

Niniejsza polityka certyfikacji dotyczy odbiorców usług certyfikacyjnych świadczonych przez Sigillum PCCE.

Sigillum PCCE wystawia zgodnie z niniejszą polityką, po zawarciu umowy z subskrybentem, certyfikat spełniający dokładnie jedno z wymienionych poniżej określeń:

1) certyfikaty służące do weryfikacji podpisów elektronicznych w poczcie elektronicznej o następnych poziomach odpowiedzialności:
    - certyfikat Sigillum Basic bez gwarancji finansowych,
    - certyfikat Sigillum Professional o gwarancji do 20.000 zł,
    - certyfikat Sigillum VIP o gwarancji do 100.000 zł;
2) certyfikaty do zapewnienia poufności danych:
    - certyfikat Sigillum Cryptogram bez gwarancji finansowych
3) certyfikaty służące do weryfikacji podpisów elektronicznych w poczcie elektronicznej oraz do zapewnienia poufności danych w poczcie elektronicznej o następujących poziomach odpowiedzialności w przypadku certyfikatów do (dla podpisu elektronicznego):
    - certyfikat Sigillum Basic bez gwarancji finansowych,
    - certyfikat Sigillum Proffessional o gwarancji do 20.000 zł,
    - certyfikat Sigillum VIP o gwarancji do 100.000 zł;
4) certyfikaty obiektowe - służące do uwierzytelnienia oraz zapewnienia poufności w komunikacji z serwerem:
    - certyfikat Sigillum Serwer o gwarancji do 200.000 zł.
5) certyfikaty służące do weryfikacji podpisów elektronicznych służących do zapewniania integralności i autentyczności kodu aplikacji
    - certyfikat Sigillum Code Sign bez gwarancji finansowych
6) certyfikaty umożliwiające logowanie użytkowników do systemów informatycznych
    - certyfikaty Sigillum Login bez gwarancji finansowych

Nie określa się szczegółowych wymagań, które musi spełnić aplikacja odbiorcy usług certyfikacyjnych wykorzystująca certyfikaty wystawione zgodnie z niniejszą polityką i związane z nimi klucze prywatne. Odpowiedzialność za prawidłowy dobór aplikacji, stosownie do rodzaju zabezpieczanych danych, spoczywa w pełni na odbiorcy usług certyfikacyjnych.

4.2 Prawa i obowiązki odbiorców usług certyfikacyjnych

4.2.1 Obowiązki subskrybenta usług certyfikacyjnych

Przed złożeniem wniosku o certyfikat i podpisaniem umowy o świadczenie usług certyfikacyjnych, subskrybent zobowiązany jest do zapoznania się z treścią niniejszej polityki certyfikacji.

Subskrybent ma obowiązek wykorzystywania kluczy prywatnych związanych z certyfikatami wydanymi zgodnie z niniejszą polityką w aplikacjach i urządzeniach zapewniających stopień zabezpieczeń odpowiedni dla rodzaju zabezpieczanych danych. Klucze i certyfikaty mogą być wykorzystywane jedynie w taki sposób, na jaki pozwala odpowiednie rozszerzenie X.509 umieszczone w certyfikacie, określające dopuszczalny zakres zastosowań klucza.

Subskrybent ma obowiązek zachowania poufności kluczy prywatnych związanych z certyfikatami wystawionymi zgodnie z niniejszą polityką. Poziom ochrony tych kluczy powinien być odpowiedni dla rodzaju zabezpieczanych danych.

W przypadku utraty klucza prywatnego związanego z certyfikatem wydanym w ramach niniejszej polityki oraz w przypadku ujawnienia tego klucza osobie trzeciej lub uzasadnionego podejrzenia, że ujawnienie takie mogło nastąpić – subskrybent (i/lub sponsor) jest zobowiązany do niezwłocznego zgłoszenia Sigillum PCCE faktu wystąpienia takiego zdarzenia w celu unieważnienia certyfikatów związanych z tym kluczem.

Subskrybent oraz Sponsor jest zobowiązany do określenia w umowie o wystawienie certyfikatu i w formularzu zgłoszenia certyfikacyjnego prawdziwych i pełnych danych w zakresie wymaganym przez umowę.

W przypadku zmiany danych zapisanych w certyfikacie i dotyczących subskrybenta, jest on zobowiązany do niezwłocznego zgłoszenia tego faktu Sigillum PCCE w celu unieważnienia certyfikatu i ewentualnie wystawienia nowego, zawierającego poprawne dane.

Po otrzymaniu certyfikatu subskrybent jest zobowiązany do sprawdzenia jego poprawności. W przypadku wystąpienia jakichkolwiek nieprawidłowości, w szczególności nieprawidłowych wartości pól określających tożsamość subskrybenta, jest on zobowiązany do niezwłocznego zgłoszenia tego faktu Sigillum PCCE celem unieważnienia certyfikatu i wygenerowania nowego certyfikatu z prawidłowymi danymi.

Subskrybent jest zobowiązany do ponoszenia kosztów świadczenia usług certyfikacyjnych według cennika obowiązującego w Sigillum PCCE w dniu podpisania umowy o świadczenie usług certyfikacyjnych.

4.2.2 Obowiązki strony ufającej

Przed wykorzystaniem klucza publicznego zawartego w certyfikacie wystawionym zgodnie z niniejszą polityką, strona ufająca musi zweryfikować ważność certyfikatu na podstawie odpowiedniej ścieżki certyfikacji, przy czym ścieżka certyfikacji zostaje zweryfikowana

poprawnie, gdy wszystkie zaświadczenia certyfikacyjne i certyfikaty zawarte w ścieżce, są w określonym czasie ważne i posiadają identyfikatory polityk certyfikacji z określonego przez weryfikującego zbioru dopuszczalnych polityk certyfikacji

Przy weryfikacji ważności certyfikatu, strona ufająca ma obowiązek posługiwania się aktualnymi listami CRL wystawionymi przez podmioty świadczące usługi certyfikacyjne.

Strona ufająca ma obowiązek ochrony integralności klucza publicznego stanowiącego punkt zaufania. W przypadku jakiejkolwiek wątpliwości co do integralności i prawdziwości klucza, strona ufająca ma obowiązek ją wyjaśnić, na przykład poprzez porównanie kryptograficznego skrótu (tzw. *odcisk palca*, ang. *fingerprint*) z posiadanego klucza publicznego odpowiednio ze skrótem opublikowanym przez podmiot świadczący usługi certyfikacyjne.

4.2.3 Obowiązki sponsora

Obowiązki sponsora określa umowa zawarta pomiędzy sponsorem a Sigillum PCCE.

4.3 Odpowiedzialność prawna i ograniczenia odpowiedzialności Sigillum PCCE

Sigillum PCCE odpowiada wobec odbiorców usług certyfikacyjnych za wszelkie szkody spowodowane niewykonaniem lub nienależytym wykonaniem swoich obowiązków, chyba że niewykonanie lub nienależyte wykonanie tych obowiązków jest następstwem okoliczności, za które Sigillum PCCE nie ponosi odpowiedzialności i którym nie mogło zapobiec mimo dołożenia należytej staranności.

W przypadku, gdy Sigillum PCCE działa za pośrednictwem punktów rejestracji, odpowiada za działania punktów rejestracji tak, jak za działania własne.

Sigillum PCCE nie odpowiada za jakiekolwiek szkody, które powstały lub mogły powstać dla odbiorców usług certyfikacyjnych lub osób trzecich, wynikające z przyczyn innych niż niewykonanie lub nienależyte wykonanie obowiązków przez Sigillum PCCE lub podmioty działające w jego imieniu. W szczególności Sigillum PCCE nie odpowiada za:

1) skutki nieprawidłowego użycia klucza prywatnego subskrybenta;
2) skutki użycia przez nieuprawnioną osobę klucza prywatnego subskrybenta;
3) skutki nieprawidłowej, niezgodnej z niniejszą polityką, weryfikacji certyfikatów wystawionych przez Sigillum PCCE;
4) skutki wynikające z posługiwania się prawidłowo zweryfikowanym lecz nieważnym certyfikatem, w okresie pomiędzy unieważnieniem certyfikatu a opublikowaniem listy CRL, a także później, jeśli odbiorca usług certyfikacyjnych posługiwał się listą CRL wystawioną wcześniej niż 1 godzinę przed datą weryfikacji ważności certyfikatu;

5) skutki wynikające z niemożności wykorzystywania unieważnionych lub zawieszonych certyfikatów, jeśli Sigillum PCCE i punkty rejestracji działające w jego imieniu prawidłowo zrealizowały procedury obowiązujące przy zawieszaniu i unieważnianiu certyfikatów, określone niniejszą polityką;

6) działania użytkownika, na które Sigillum PCCE nie ma wpływu.

W przypadku generowania kluczy przez subskrybenta Sigillum PCCE nie ponosi odpowiedzialności za jakość dostarczonych kluczy.

Maksymalna odpowiedzialność, jaka może ciążyć na PWPW S.A. z tytułu realizacji usług certyfikacyjnych objętych Polityką jest ograniczona do:

1) 20.000 PLN-w związku z działaniami wykonanymi przy wykorzystaniu pojedynczego certyfikatu Sigillum Professional wystawionego przez Sigillum PCCE zgodnie z Polityką;

2) 100.000 PLN-w związku z działaniami wykonanymi przy wykorzystaniu pojedynczego certyfikatu SigillumVIP wystawionego przez Sigillum PCCE zgodnie z Polityką;

3) 200.000 PLN-w związku z działaniami wykonanymi przy wykorzystaniu pojedynczego certyfikatu obiektowego Sigillum Serwer wystawionego przez Sigillum PCCE zgodnie z Polityką.

4.4 Odnośne akty prawne

Zapisy niniejszej polityki oraz zapisy umów zawartych na świadczenie usług certyfikacyjnych zgodnie z niniejszą polityką podlegają normom prawnym Rzeczpospolitej Polskiej.

Usługi certyfikacyjne świadczone przez PCCE zgodnie z niniejszą polityką są zgodne z wymaganiami Ustawy w stosunku do podmiotów świadczących usługi certyfikacyjne. W celu interpretacji terminów zawartych w niniejszej polityce należy również rozpatrywać postanowienia Ustawy odnoszące się do świadczenia kwalifikowanych usług certyfikacyjnych.

Wątpliwości interpretacyjne, które nie mogą być rozstrzygnięte na podstawie określonych powyżej aktów prawnych należy interpretować zgodnie z postanowieniami Kodeksu Cywilnego.

W przypadku powstania sporu pomiędzy Sigillum PCCE, a odbiorcą usług certyfikacyjnych, strony podejmą próbę rozstrzygnięcia sporu w drodze polubownego porozumienia. W przypadku nie osiągnięcia porozumienia rozstrzygnięcie sporu zostanie oddane sądowi powszechnemu właściwemu dla siedziby PWPW SA.

4.5 Publikowanie i repozytorium

Sigillum PCCE jest zobowiązane do prowadzenia repozytorium dostępnego dla odbiorców usług certyfikacyjnych.

Repozytorium jest dostępne w sieci Internet pod adresem:

www.sigillum.pl/repozytorium.

Lista zawieszonych i unieważnionych certyfikatów jest generowana i publikowana przez Sigillum PCCE co 12 godzin, a w przypadku wystąpienia zdarzenia unieważnienia, zawieszenia lub uchylenia zawieszenia w terminie do 24 godzin od momentu wystąpienia zdarzenia.

Sigillum PCCE publikuje w repozytorium:

1) wszystkie wersje niniejszej polityki certyfikacji oraz wszystkie wersje tej polityki certyfikacji, które obowiązywały wcześniej, z określeniem okresu ich obowiązywania;
2) aktualny regulamin certyfikacji związany z niniejszą polityką;
3) aktualny klucz publiczny służący do weryfikacji certyfikatów kluczy publicznych i zaświadczeń certyfikacyjnych wystawionych zgodnie z niniejszą polityką certyfikacji;
4) wszystkie zaświadczenia certyfikacyjne wystawione przez Sigillum PCCE zgodnie z niniejszą polityką certyfikacji;
5) aktualną listę unieważnionych certyfikatów i zaświadczeń certyfikacyjnych (CRL), wystawioną zgodnie z niniejszą polityką;
6) wszystkie certyfikaty wystawione przez Sigillum PCCE zgodnie z niniejszą polityką certyfikacji.

4.6 Poufność

Sigillum PCCE przetwarza dane osobowe osób fizycznych będących subskrybentem lub sponsorem usług certyfikacyjnych zgodnie z przepisami ustawy o ochronie danych osobowych zachowując zasady poufności. Sytuacja taka zachodzi, zarówno gdy subskrybent usług certyfikacyjnych, zgodnie z postanowieniami niniejszej polityki, występuje w imieniu własnym oraz działa na własny rachunek albo działa w ramach organizacyjnych osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej.

Klucz prywatny Sigillum PCCE służący do generowania certyfikatów jest chroniony przy zachowaniu środków technicznych i organizacyjnych spełniających wymagania Ustawy.

Klucze prywatne związane z certyfikatami powinny być traktowane jako chronione przez subskrybenta. Wszelkie skutki wynikające z niewłaściwego lub nieuprawnionego użycia tych kluczy ponosi subskrybent.

Obowiązki zachowania poufności kluczy prywatnych subskrybenta związanych z certyfikatami mogą wynikać z innych, nieuwzględnionych w niniejszej polityce dokumentów lub aktów prawnych, w zależności od zakresu zastosowania tych kluczy przez subskrybenta.

4.7 Zmiana postanowień polityki certyfikacji

Każda modyfikacja polityki certyfikacji musi być zatwierdzona przez Radę Zatwierdzania Polityk Certyfikacji Sigillum PCCE. Zmieniona polityka

certyfikacji jest oznaczona nowym, unikalnym numerem wersji oraz numerem OID.

Nowa polityka obowiązuje w stosunku do certyfikatów wystawionych po wejściu jej w życie.

W przypadkach uzasadnionych niezbędnymi, zmieniającymi się wymaganiami na bezpieczeństwo informacji zabezpieczanych przy użyciu dotychczas wystawionych certyfikatów, Rada Zatwierdzania Polityk Certyfikacji Sigillum PCCE może zdecydować, że nowa polityka certyfikacji lub niektóre jej postanowienia obowiązują w stosunku do wszystkich certyfikatów, także tych wydanych w okresie obowiązywania poprzednich wersji polityki.

Jeśli zmiany te nie wynikają z przyczyn leżących po stronie Sigillum PCCE, a są spowodowane np. wymaganiami prawa lub zmieniającymi się warunkami bezpieczeństwa algorytmów kryptograficznych, subskrybentom nie przysługuje prawo do odszkodowania za ewentualne ograniczenia możliwości wykorzystywania certyfikatów.

5 Identyfikacja i uwierzytelnienie

5.1 Rejestracja

5.1.1 Rejestracja subskrybenta będącego osobą fizyczną

Subskrybentami usług certyfikacyjnych realizowanych zgodnie z niniejszą polityką certyfikacji mogą być osoby fizyczne spełniające wymagania określone w Ustawie. Osoby te mogą występować w imieniu własnym lub w imieniu innych podmiotów („sponsorów"). Informacja o roli subskrybenta jest umieszczana w certyfikatach kluczy publicznych w sposób określony Ustawą.

Przed rejestracją subskrybenta, w przypadku gdy występuje także sponsor, musi zostać zawarta umowa pomiędzy Sigillum PCCE, a sponsorem certyfikatu. Umowa ta określa co najmniej:

1) zasady weryfikacji uprawnień subskrybentów do posiadania certyfikatów zawierających oznaczenie sponsora;
2) uprawnienia sponsora do informacji o wystawionych przez Sigillum PCCE certyfikatach zawierających nazwę sponsora oraz zasady rozliczeń kosztów wynikających z takich informacji;
3) uprawnienia sponsora do zawieszania, uchylania zawieszenia oraz do unieważniania certyfikatów zawierających jego nazwę;
4) zasady odpłatności za usługi certyfikacyjne. Koszty certyfikacji mogą być ponoszone bezpośrednio przez sponsora lub też koszty mogą obciążać subskrybenta, przy ewentualnej dalszej refundacji przez sponsora.

Przed rejestracją subskrybenta występującego bez udziału sponsora musi zostać zawarta umowa o świadczenie usług certyfikacyjnych pomiędzy Sigillum PCCE a subskrybentem. Umowa ta określa co najmniej:

1) imię (imiona), nazwisko, numer dokumentu tożsamości, który był wykorzystany do weryfikacji tożsamości;
2) zasady odpłatności za świadczenie usług certyfikacyjnych;
3) uprawnienia subskrybenta do zawieszenia, uchylenia zawieszenia oraz do unieważnienia certyfikatów zawierających jego nazwę.

Umowa pomiędzy Sigillum PCCE a subskrybentem jest podpisywana własnoręcznie przez subskrybenta.
Sigillum PCCE przeprowadza weryfikację tożsamości potencjalnego subskrybenta na podstawie ważnego dowodu osobistego lub paszportu, spełniających funkcje dokumentów podstawowych. Dodatkowym dokumentem akceptowanym przy weryfikacji tożsamości subskrybenta jest prawo jazdy wydane po 1 lipca 1999 roku.
W przypadku certyfikatów Sigillum Basic, Sigillum Cryptogram, Sigillum Code Sign, Sigillum Login wymagany jest tylko jeden dokument podstawowy. W przypadku pozostałych certyfikatów dwa dokumenty.

Mogą to być dwa dokumenty podstawowe bądź jeden podstawowy i jeden dodatkowy.

Niniejsza Polityka dopuszcza także notarialne potwierdzenie tożsamości Subskrybenta i/lub Zamawiającego.

5.1.2 Rejestracja subskrybenta innego niż osoba fizyczna

Prawo do występowania w imieniu potencjalnego subskrybenta przed Sigillum PCCE oraz działającymi na jego rzecz punktami rejestracji, mają osoby upoważnione do zaciągania zobowiązań w imieniu potencjalnego subskrybenta, na podstawie pełnomocnictwa lub odpowiednich dokumentów:

1) oryginału wpisu do ewidencji gospodarczej oraz oryginałów dokumentów potwierdzających przyznanie NIP i REGON – w przypadku spółek cywilnych;
2) oryginału odpisu z rejestru handlowego (wystawionego przez stosowny organ nie wcześniej niż 3 miesiące przed datą wystąpienia z wnioskiem o certyfikat) oraz oryginałów dokumentów potwierdzających przyznanie NIP i REGON – w przypadku spółek prawa handlowego, a także fundacji, stowarzyszeń, spółdzielni, banków, partii politycznych i związków zawodowych;
3) statutu jednostki – w przypadku państwowych jednostek i zakładów budżetowych.

W przypadku, gdy w wyżej wymienionych dokumentach nie zapisano stałego pełnomocnictwa, osoba występująca w imieniu potencjalnego subskrybenta, oprócz wymienionych wyżej dokumentów, musi okazać się oryginałem pełnomocnictwa.

Przed wystawieniem certyfikatu zgodnie z niniejszą polityką, Sigillum PCCE przeprowadza weryfikację tożsamości przedstawiciela potencjalnego subskrybenta na podstawie ważnego dowodu osobistego lub paszportu, spełniających funkcje dokumentów podstawowych (dodatkowym dokumentem akceptowanym przy weryfikacji tożsamości subskrybenta jest prawo jazdy wydane po 1 lipca 1999 roku) oraz podpisuje z subskrybentem umowę o świadczenie usług certyfikacyjnych.

Niniejsza Polityka dopuszcza także notarialne potwierdzenie tożsamości Subskrybenta i/lub Zamawiającego.

5.2 Wystawienie kolejnego certyfikatu

Wystawienie kolejnego certyfikatu odbywa się na takich samych zasadach, jak wystawienie nowego certyfikatu.

5.3 Zawieszenie i unieważnienie certyfikatów

Polityka określa następujące sposoby zarządzania stanem certyfikatu przez subskrybenta lub sponsora:

Sponsor ma 2 możliwości zgłoszenia żądania zawieszania certyfikatu:

1. osobiście w godzinach pracy Punktu Rejestracji, po weryfikacji tożsamości na podstawie zaprezentowanego dowodu tożsamości oraz wypełnionej dyspozycji zawieszenia/ uchylenia zawieszenia/ unieważnienia certyfikatu;
2. pocztą elektroniczną wysyłając dyspozycję podpisaną ważnym podpisem elektronicznym, weryfikowanym za pomocą certyfikatu komercyjnego wystawionego przez Sigillum PCCE, przesłaną na adres wskazany na stronie internetowej Sigillum PCCE przez 24h/7dni/365dni w roku;

Subskrybent ma 3 możliwości zawieszenia certyfikatu:

1. osobiście w godzinach pracy Punktu Rejestracji, po weryfikacji tożsamości na podstawie zaprezentowanego dowodu tożsamości oraz wypełnionej dyspozycji zawieszenia/ uchylenia zawieszenia/ unieważnienia certyfikatu;
2. telefonicznie 24h/7dni/365dni w roku na numer awaryjny dostarczony subskrybentowi w momencie podpisywania umowy oraz prezentowany na stronie internetowej Sigillum PCCE. Zawieszenie odbywa się po podaniu sekretnej frazy przez Subskrybenta;
3. pocztą elektroniczną wysyłając dyspozycję podpisaną ważnym podpisem elektronicznym, weryfikowanym za pomocą certyfikatu komercyjnego wystawionego przez Sigillum PCCE, przesłaną na adres wskazany na stronie internetowej Sigillum PCCE przez 24h/7dni/365dni w roku;

W przypadku uchylenia zawieszenia certyfikatu Sponsor i Subskrybent mają następujące możliwości działania:

1. osobiście w godzinach pracy Punktu Rejestracji, po weryfikacji tożsamości na podstawie zaprezentowanego dowodu tożsamości oraz dyspozycji zawieszenia/ uchylenia zawieszenia/ unieważnienia certyfikatu;
2. pocztą elektroniczną wysyłając dyspozycję podpisaną ważnym podpisem elektronicznym, weryfikowanym za pomocą certyfikatu komercyjnego wystawionego przez Sigillum PCCE, przesłaną na adres wskazany na stronie internetowej Sigillum PCCE przez 24h/7dni/365dni w roku.

Odwołanie zawieszenia certyfikatu następuje tylko na podstawie woli subskrybenta lub sponsora lub jeśli Sigillum PCCE stwierdzi ustanie przyczyn powodujących zawieszenie.

W przypadku unieważnienia certyfikatu Sponsor ma następujące możliwości działania:

1. osobiście w godzinach pracy Punktu Rejestracji, po weryfikacji tożsamości na podstawie zaprezentowanego dowodu tożsamości oraz wypełnionej dyspozycji zawieszenia/ uchylenia zawieszenia/ unieważnienia certyfikatu;

2. pocztą elektroniczną wysyłając dyspozycję podpisaną ważnym podpisem elektronicznym, weryfikowanym za pomocą certyfikatu komercyjnego wystawionego przez Sigillum PCCE, przesłaną na adres wskazany na stronie internetowej Sigillum PCCE przez 24h/7dni/365dni w roku.

Subskrybent natomiast dysponuje następującymi możliwościami unieważnienia certyfikatu:

1. osobiście w godzinach pracy Punktu Rejestracji, po weryfikacji tożsamości na podstawie zaprezentowanego dowodu tożsamości oraz wypełnionej dyspozycji zawieszenia/ uchylenia zawieszenia/ unieważnienia certyfikatu;
2. telefonicznie 24h/7dni/365dni w roku na numer awaryjny dostarczony subskrybentowi w momencie podpisywania umowy oraz prezentowany na stronie internetowej Sigillum PCCE. Unieważnienie odbywa się po podaniu sekretnej frazy przez Subskrybenta;
3. pocztą elektroniczną wysyłając dyspozycję podpisaną ważnym podpisem elektronicznym, weryfikowanym za pomocą certyfikatu komercyjnego wystawionego przez Sigillum PCCE, przesłaną na adres wskazany na stronie internetowej Sigillum PCCE przez 24h/7dni/365dni w roku.

Unieważnienie certyfikatu może być również następstwem zawieszenia certyfikatu, a więc może być wynikiem zaistnienia przesłanek upoważniających Sigillum PCCE do zawieszenia certyfikatu, w przypadku gdy w terminie 7 dni od daty zawieszenia nie zostało ono uchylone.

Umowa o świadczenie usług certyfikacyjnych zawarta pomiędzy Polską Wytwórnią Papierów Wartościowych S.A. - Sigillum PCCE a sponsorem może przewidywać inne wymagania niż określono powyżej dotyczące sposobu uwierzytelnienia subskrybenta występującego w imieniu sponsora lub dotyczące sposobu uwierzytelnienia przedstawicieli sponsora przy unieważnianiu, zawieszaniu lub odwoływaniu zawieszenia certyfikatów.

6 Wymagania operacyjne

6.1 Zgłoszenie certyfikacyjne przy rejestracji

Niniejsza polityka certyfikacji dopuszcza stosowanie następujących wariantów generowania kluczy prywatnych i publicznych subskrybenta:

1) generowanie kluczy przez potencjalnego subskrybenta, za pomocą oprogramowania i ewentualnie komponentu technicznego pozostającego pod kontrolą subskrybenta;
2) generowanie kluczy przez potencjalnego subskrybenta, za pomocą oprogramowania i ewentualnie komponentu technicznego pozostającego pod kontrolą punktu rejestracji;
3) generowanie kluczy przez Sigillum PCCE.

W przypadku generowania kluczy przez potencjalnego subskrybenta, dostarcza on osobiście do Sigillum PCCE zgłoszenie certyfikacyjne w postaci pliku w formacie PKCS#10, zawierającego co najmniej:

1) klucz publiczny zgłaszany do certyfikacji;
2) identyfikator DN potencjalnego subskrybenta, w którym określono co najmniej następujące atrybuty:
    - nazwę powszechną subskrybenta,
    - adres e-mail subskrybenta,
    - nazwa organizacji i jednostki organizacyjnej w przypadku, gdy subskrybent występuje w imieniu organizacji

Zgłoszenie certyfikacyjne jest podpisane kluczem prywatnym związanym z kluczem publicznym zgłaszanym do certyfikacji.

Po potwierdzeniu tożsamości potencjalnego subskrybenta zgodnie z postanowieniami rozdziału 5.1, obsługujący potencjalnego subskrybenta inspektor ds. rejestracji oraz potencjalny subskrybent podpisują własnoręcznie formularz zgłoszenia certyfikacyjnego, następnie potencjalny subskrybent i Sigillum PCCE podpisują umowę o świadczenie usług certyfikacyjnych.

W przypadku gdy Sponsor dokonuje weryfikacji tożsamości we własnym zakresie dostarcza on do Sigillum PCCE oświadczenie o weryfikacji tożsamości subskrybentów zgodnie z zasadami przyjętymi w Sigillum PCCE i opisanymi w niniejszej Polityce.

Zgodnie z art. 14 ust 6 Ustawy niniejsza Polityka dopuszcza notarialne potwierdzenie tożsamości Subskrybenta i/lub Zamawiającego. W takim przypadku Subskrybent i/lub Zamawiający składa podpis własnoręczny w obecności notariusza na wymaganych dokumentach, co notariusz potwierdza, a następnie Subskrybent i/lub Zamawiający dostarcza tak przygotowany komplet dokumentów do Sigillum PCCE.

Po podpisaniu umowy inspektor ds. rejestracji generuje i podpisuje zgłoszenie certyfikacyjne, zawierające wszystkie dane niezbędne do wystawienia certyfikatu, a następnie uruchamia procedurę generowania certyfikatu subskrybenta. Certyfikat będzie zawierał między innymi klucz publiczny oraz dane subskrybenta dostarczone przez niego w formularzu zgłoszenia certyfikacyjnego.

W przypadku generowania kluczy przez Sigillum PCCE lub za pomocą sprzętu lub oprogramowania pozostającego pod kontrolą Sigillum PCCE, potencjalny subskrybent dostarcza osobiście do Sigillum PCCE formularz zgłoszenia certyfikacyjnego.

W przypadku występowania Sponsora, formularz zgłoszenia certyfikacyjnego może dostarczyć odpowiednio umocowany przedstawiciel Sponsora, po uprzednim dostarczeniu przez Sponsora oświadczenia o poprawnej weryfikacji tożsamości subskrybentów.

Po potwierdzeniu tożsamości potencjalnego subskrybenta zgodnie z postanowieniami rozdziału 5.1, obsługujący potencjalnego subskrybenta inspektor ds. rejestracji oraz potencjalny subskrybent podpisują własnoręcznie formularz zgłoszenia certyfikacyjnego, następnie potencjalny subskrybent i Sigillum PCCE podpisują umowę o świadczenie usług certyfikacyjnych.

Po podpisaniu umowy Sigillum PCCE generuje klucze subskrybenta, za pomocą urządzenia (oprogramowanie współpracujące z komponentem technicznym) posiadającego funkcje generowania kluczy przez komponent techniczny, którego konstrukcja:

1) uniemożliwia skopiowanie klucza prywatnego z komponentu technicznego, na którym klucze zostały wygenerowane lub
2) uniemożliwia skopiowanie klucza prywatnego z modułu kluczowego współpracującego z komponentem technicznym, na którym klucze zostały wygenerowane.

Po wygenerowaniu kluczy, inspektor ds. rejestracji Sigillum PCCE tworzy i podpisuje zgłoszenie certyfikacyjne zawierające wszystkie dane niezbędne do wystawienia certyfikatu, a następnie uruchamia procedurę generowania certyfikatu subskrybenta.

Niezależnie od miejsca generowania kluczy, Sigillum PCCE lub punkt rejestracji archiwizuje, przez okres co najmniej 20 lat, następujące dokumenty:

1) podpisaną obustronnie umowę o świadczenie usług certyfikacyjnych;
2) podpisany przez inspektora ds. rejestracji formularz zgłoszenia certyfikacyjnego.

6.2 Wystawienie certyfikatu

Sigillum PCCE wystawia certyfikat na podstawie podpisanego przez inspektora ds. rejestracji formularza zgłoszenia certyfikacyjnego.

Termin początku okresu ważności certyfikatu ustala umowa zawarta pomiędzy Sigillum PCCE a Subskrybentem. Maksymalny okres ważności komercyjnego certyfikatu przewidziany przez politykę certyfikacji wynosi nie więcej niż 2 lata.
Certyfikat publikowany jest Repozytorium. Certyfikat może być odebrany przez subskrybenta w miejscu, do którego subskrybent dostarczył formularz zgłoszenia certyfikacyjnego lub wniosek o wygenerowanie kluczy i certyfikatu.
Osobą odpowiedzialną za dostarczenie certyfikatu do Subskrybenta może być przedstawiciel sponsora.

6.3 Akceptacja certyfikatu

Po odebraniu certyfikatu subskrybent ma obowiązek do niezwłocznego sprawdzenia jego zawartości. W przypadku dostrzeżenia jakichkolwiek pomyłek, w szczególności pomyłek związanych z identyfikacją subskrybenta, ma on obowiązek do niezwłocznego zgłoszenia tego faktu Sigillum PCCE, celem unieważnienia certyfikatu.

Kontrola poprawności certyfikatu musi być przeprowadzona przed pierwszym użyciem klucza prywatnego związanego z certyfikatem.

6.4 Zawieszenie, uchylenie zawieszenia i unieważnienie certyfikatu

Warunki zawieszenia, uchylenia zawieszenia oraz unieważnienia certyfikatu na wniosek sponsora lub subskrybenta, a także dokumenty, na podstawie których realizuje się te czynności, określone zostały w rozdziale 5.3.

Unieważnienie certyfikatu z inicjatywy Sigillum PCCE następuje z jednego z powodów określonych w stosunku do kwalifikowanych certyfikatów w Art. 21 Ust. 2 pkt. 1 do 5 i pkt. 7, oraz ust. 6 Ustawy:

- certyfikat został wystawiony na podstawie nieprawdziwych lub nieaktualnych danych;
- subskrybent lub sponsor nie dopełnił obowiązków określonych w polityce i regulaminie certyfikacji;
- podmiot świadczący usługi certyfikacyjne zaprzestaje świadczenia usług certyfikacyjnych, a jego praw i obowiązków nie przejmuje inny podmiot świadczący usługi certyfikacyjne;
- żąda tego osoba składająca podpis elektroniczny lub osoba trzecia wskazana w certyfikacie;
- odbiorca usług certyfikacyjnych nie przechowywał danych służących do składania podpisu elektronicznego w sposób zapewniający ich ochronę przed nieuprawnionym dostępem w okresie ważności certyfikatu służącego do weryfikacji podpisów.

O każdym przypadku zawieszenia lub unieważnienia certyfikatu subskrybent oraz sponsor – jeśli występuje – są niezwłocznie powiadamiani za pomocą poczty elektronicznej. Odpowiedzialność za prawidłowe zgłoszenie Sigillum PCCE adresu e-mail Subskrybenta lub

Sponsora przy podpisywaniu umowy, a następnie aktualizowanie tego adresu w przypadku jego zmian, spoczywa odpowiednio na Subskrybencie i Sponsorze.

6.5 Odnowienie certyfikatu

Nie ma możliwości odnowienia certyfikatu subskrybenta. Subskrybent w każdej chwili może wystąpić z wnioskiem o wystawienie nowego certyfikatu.

6.6 Środki ochrony technicznej

6.6.1 Generowanie kluczy subskrybenta

Jeśli para kluczy Subskrybenta jest generowana przez Subskrybenta, procedura generowania kluczy musi spełniać warunki określone w niniejszym rozdziale.
W przypadku, gdy klucze są generowane w Sigillum PCCE, klucze te spełniają warunki określone w niniejszym rozdziale.

W stosunku do kluczy służących do składania i weryfikacji bezpiecznych podpisów elektronicznych obowiązują następujące wymagania:

1) zastosowane urządzenia do generowania kluczy oraz same klucze muszą spełniać wymagania określone w Ustawie w stosunku do generowania kluczy związanych kwalifikowanymi certyfikatami, z tym wyjątkiem, że nie ma obowiązku używania generatorów liczb losowych opartych na zjawisku fizycznym (można wykorzystać generatory liczb pseudolosowych);
2) długość pary kluczy algorytmu RSA, rozumiana jako p*q, leży w przedziale 1024-2048 bitów, i jest podzielna przez 128;
3) długości liczb pierwszych *p* i *q*, będących elementami klucza prywatnego, nie mogą się różnić o więcej niż 30 bitów.

6.6.2 Dostarczanie kluczy subskrybenta

Jeśli para kluczy jest generowana w Punkcie Rejestracji, klucz prywatny może być dostarczany Subskrybentowi w następujący sposób:

- klucze prywatne Subskrybent może odebrać osobiście w Punkcie Rejestracji
- klucze prywatne mogą zostać przesłane Subskrybentowi za pośrednictwem usług kurierskich lub pocztowych.

Klucze prywatne dostarczane są Subskrybentowi wraz z zawierającymi je komponentami technicznymi lub z modułami kluczowymi, na których zostały zapisane przez komponent techniczny wykorzystany do ich wygenerowania.

6.6.3 Instalowanie kluczy subskrybenta

W przypadku, gdy klucze subskrybenta były wygenerowane w Sigillum PCCE i dostarczone mu wraz z informacjami pozwalającymi na aktywację klucza prywatnego, subskrybent ma obowiązek do niezwłocznej zmiany danych pozwalających na aktywację klucza prywatnego.

Konieczna jest zmiana pinów przez Subskrybenta, przed rozpoczęciem okresu eksploatacji certyfikatu.

Nie określa się innych wymagań na sposób instalacji kluczy w urządzeniach subskrybenta (oprogramowaniu lub komponentach technicznych).

6.6.4 Kopie zapasowe, archiwa i depozyt kluczy prywatnych subskrybenta

Klucze prywatne subskrybenta związane z certyfikatami służącymi do weryfikacji podpisów elektronicznych nie mogą podlegać procedurom tworzenia kopii zapasowych, archiwizowania ani składania w depozyt.

Sposób postępowania w tym zakresie z kluczami prywatnymi subskrybenta niezwiązanymi z generowaniem podpisów leży w gestii subskrybenta, choć może podlegać postanowieniom dokumentów i aktów prawnych nieuwzględnionych w niniejszej polityce.

6.6.5 Ochrona, aktywacja, dezaktywacja i niszczenie kluczy subskrybenta

Nie określa się w niniejszej polityce wymagań szczegółowych na urządzenia (oprogramowanie i ewentualnie sprzęt), które mogą służyć do przetwarzania kluczy prywatnych subskrybenta związanych z certyfikatami, jak również na sposoby aktywacji i dezaktywacji tych kluczy. Wymagania takie mogą być nałożone przez inne dokumenty, wynikające z zakresu zastosowań tych kluczy przez subskrybenta.

Po unieważnieniu lub przeterminowaniu certyfikatów związanych z kluczami prywatnymi, klucze te mogą podlegać procedurom archiwizacji określonym przez subskrybenta, przy uwzględnieniu zakresu zastosowań tych kluczy przez subskrybenta.

6.7 Profil certyfikatów i list CRL

6.7.1 Profil certyfikatu

Certyfikat

Pole	**Opis/wartość**
tbsCertificate	Poświadczona elektronicznie treść certyfikatu
signatureAlgorithm	Sha-1WithRSAEncryption: { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
signatureValue	Wartość poświadczenia elektronicznego

Poświadczona elektronicznie treść certyfikatu

Pole	**Opis/wartość**
version	„2“
serialNumber	Numer unikalny w ramach certyfikatów wystawionych przez PCCE Sigillum zgodnie z niniejszą polityką
signature	Sha-1WithRSAEncryption: { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
issuer	identyfikator wystawcy certyfikatu
countryName	“PL”
organizationName	“PWPW S.A.”
organizationalUnit	“Sigillum Polskie Centrum Certyfikacji Elektronicznej”
commonName	“Sigillum PCCE – CA”
validity	oznaczenie okresu ważności certyfikatu
notBefore	data i czas początku okresu ważności certyfikatu
notAfter	data i czas końca okresu ważności certyfikatu
subject	identyfikator subskrybenta (format identyfikatora określono poniżej)
subjectPublicKeyInfo	określenie algorytmu używanego przez subskrybenta oraz jego klucz publiczny
algorithm	RsaEncryption: { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }
subjectPublicKey	
modulus	moduł klucza
publicExponent	wykładnik klucza publicznego
Extensions	rozszerzenia certyfikatu

Pole ‘Subject’ certyfikatu może zawierać następujące atrybuty:

1) nazwisko (ang. surename),
2) imię (imiona) (ang. givenName),
3) nazwa powszechna (ang. commonName),

4) organizacja (ang. organizationName),
5) pseudonim (ang. pseudonym),
6) Nazwa stanowiska jakie subskrybent zajmuje w ramach organizacji (ang. Title)
7) jednostka organizacyjna (ang. organizationalUnitName),
8) województwo (ang. stateOrProvinceName),
9) nazwa miejscowości (ang. localityName),
10) adres poczty elektronicznej (ang. emailAddress),
11) adres (ang. postalAddress),
12) numer seryjny – unikalny identyfikator przypisany podmiotowi w ramach jednostki organizacyjnej (ang. serialnumber),
13) opis certyfikatu (ang. description).

Możliwe są następujące warianty formatów pola 'Subject' certyfikatu:

1) pole zawiera przynajmniej następujące atrybuty: nazwa powszechna ,nazwa kraju, nazwisko, imię (imiona), adres poczty elektronicznej, opis certyfikatu;
2) pole zawiera przynajmniej następujące atrybuty: nazwa powszechna ,nazwa kraju, organizacja, nazwa województwa, nazwa miejscowości, adres poczty elektronicznej, opis certyfikatu – dla certyfikatów subskrybentów będących osobami prawnymi lub jednostkami organizacyjnymi, służących do zabezpieczania poczty;
3) pole zawiera przynajmniej następujące atrybuty: nazwa kraju, pseudonim, nazwa powszechna;
4) pole zawiera przynajmniej następujące atrybuty: nazwa kraju, organizacja, nazwa województwa, nazwa miejscowości, nazwa powszechna, opis certyfikatu – dla certyfikatów subskrybentów będących osobami prawnymi lub jednostkami organizacyjnymi, służących do komunikacji z serwerem WWW.

Jeśli pole Subject zawiera atrybuty 'imię', 'nazwisko', 'adres poczty elektronicznej' oraz 'organizacja', 'nazwa województwa', 'nazwa miejscowości', to atrybuty 'imię', 'nazwisko' oraz 'adres poczty elektronicznej' dotyczą subskrybenta, natomiast atrybuty 'organizacja', 'nazwa województwa', 'nazwa miejscowości' dotyczą sponsora, którego przedstawicielem jest subskrybent.

6.7.1.1 Rozszerzenia X.509

Rozszerzenia standardowe:

Pole	**Opis/wartość**	**Krytyczne**
AuthorityKeyIdentifier	Rozszerzenie to identyfikuje klucz publiczny służący do	NIE

	weryfikacji wydanego certyfikatu.	
keyUsage	Rozszerzenie to określa sposób wykorzystania klucza komercyjnego Subskrybenta Dopuszczalne wartości: • digitalSignature • keyEncipherment • keyAgreement • nonRepudiation • dataEncipherment	TAK
extendedKeyUsage	Pole to określa zawężenie obszaru zastosowania klucza, określonego w polu keyUsage. Jest to rozszerzenie opcjonalne. Dopuszczalne wartości: ▪ Server Authentication ▪ Client Authentication ▪ Code Signing ▪ Email Protection ▪ IPSEC End System ▪ IPSEC Tunnel ▪ IPSEC User ▪ Timestamping ▪ OCSP Server ▪ Certificate Trust List Signing ▪ Microsoft Server Gated Cryptography ▪ Encrypted File System ▪ Netscape Server Gated Cryptography ▪ Smart card Logon	NIE
certificatePolicies	określenie lub wskazanie na politykę certyfikacji	NIE
policyIdentifier	OID {1 2 616 1 113560 10 3 1 0} (wskazanie na politykę certyfikacji, zgodnie z którą wystawiony jest certyfikat)	TAK

policyIdentifier	ewentualne wskazania na inne polityki certyfikacji, których wymagania są spełniane przez certyfikat	NIE
subjectAltName	rozszerzenie opcjonalne o dopuszczalnych wartościach: • User Principal Name (UPN) • Domain Controller Globally Unique Identifier (GUID) • Domain Name Server (DNS Name) • rfc822Name (adres email)	NIE
basicConstraints	pusta sekwencja (określenie, czy subskrybent jest użytkownikiem końcowym, czy też podmiotem wydającym certyfikaty)	TAK
CRL Distribution Point	Pole wskazuje na adres serwera, z którego można pobrać listę CRL.	NIE

Rozszerzenia niestandardowe:

Pole	**Opis/wartość**	**Krytyczne**
qcStatements		NIE
qcStatement - QcLimitValue		
statementId	limit transakcji, którą jednorazowo można potwierdzić przy pomocy certyfikatu { id-etsi-qcs 2 }	NIE
statementInfo		NIE
MonetaryValue		NIE
currency	waluta – według ISO 4217	NIE

amount	mantysa	NIE
exponent	wykładnik (kwota graniczna transakcji = mantysa * 10 ^ wykładnik)	NIE
qcStatement - subjectSignatureType		NIE
statementId	określenie roli, w której występuje subskrybent, jeśli w polu 'subject' certyfikatu określono dane sponsora { iso(1) member-body(2) pl(616) organization(1) gov(101) moe(3) pki(1) certificate-extensions(1) 2 }	NIE
statementInfo	weWlasnymImieniu (1), upowaznionyPrzedstawiciel (2), czlonekOrganu (3), organWladzyPublicznej (4)	NIE
Netscape Type extension	Opis: Rozszerzenie umożliwia wykorzystanie aplikacji Subskrybenta z aplikacjami firmy Netscape. Jest to rozszerzenie opcjonalne. Wartość: ▪ SSL Client ▪ SSL Server ▪ S/MIME Client ▪ Object Signing ▪ SSL CA ▪ S/MIME CA ▪ Object Signing CA	NIE

6.7.2 Profil listy CRL

lista CRL

Pole	**Opis/wartość**
TbsCertList	Poświadczona elektronicznie treść Listy CRL
SignatureAlgorithm	Sha-1WithRSAEncryption: { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
SignatureValue	Wartość poświadczenia elektronicznego

Poświadczona elektronicznie treść Listy CRL

Pole	**Opis/wartość**	**Krytyczne**
Version	„1” (X.509 v2)	TAK
Signature	Sha-1WithRSAEncryption: { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }	TAK
Issuer	identyfikator wystawcy listy CRL, zgodny z identyfikatorem określonym w profilu certyfikatów	TAK
ThisUpdate	data wydania listy CRL	NIE
NextUpdate	data wydania następnej listy CRL (następna lista nie może być wydana później)	TAK
revokedCertificates		NIE
userCertificate	numer seryjny zawieszonego lub unieważnionego certyfikatu lub unieważnionego zaświadczenia certyfikacyjnego	NIE

revocationDate	data zawieszenia bądź unieważnienia certyfikatu lub unieważnienia zaświadczenia certyfikacyjnego	TAK
crlEntryExtensions	rozszerzenia listy CRL (dotyczą każdego z certyfikatów lub zaświadczeń certyfikacyjnych z osobna)	NIE
cRLReason	kod przyczyny unieważnienia lub wskazanie, że certyfikat został zawieszony	NIE
CrlExtensions	rozszerzenia listy CRL (dotyczą całej listy)	NIE
authorityKeyIdentifier	skrót SHA-1 z klucza publicznego w polu keyIdentifier	NIE
cRLNumber	numer kolejny listy CRL	NIE

Listy CRL wydawane przez PCCE Sigillum zawierają dane o unieważnionych lub zawieszonych certyfikatach oraz dane o unieważnionych zaświadczeniach certyfikacyjnych. Nie będą wydawane listy ARL.

Przyjął do archiwum (data i podpis): ……..

Zatwierdził (data i podpis): ……..

Nadzorował (data i podpis): ……..

Opracował (data i podpis): ……..

Nazwa pliku: **P3032 wer1.5_27_06_2008r_Polit_certyf_Sigillum.doc**

osoba odpowiedzialna (nadzorował): **Jacek Biernacki 33 292 96**

Rejestr zmian w dokumencie:

Wersja	Data	Opracował	Opis nowelizacji
0.2	2003-01-30	Grazyna Kowalska	Zakończenie prac przez Wykonawcę
1.00	Luty 2003r		Ustalenie wersji dokumentu
1.1	27-05-2003	Artur Miękina Paweł Sałek	Zmiana nazwy dokumentu i inne zmiany
1.2	1-11-2003	Artur Miękina Paweł Sałek	Słownik, treść dokumentu - poprawki redakcyjne Rozdział 3 i 4.1 – dopisanie klas do certyfikatów, dopisanie certyfikatów dla weryfikacji poczty elektronicznej, dopisanie certyfikatu szkolno- testowego Rozdział 4.2.1. – wyłączenie prawdziwości danych w certyfikatach szkoleniowo-testowe Rozdział 6.1 pt. 2 – dopisane 2 atrybuty Rozdział 6.1 dopisany okres ważności certyfikatu szkolno-testowego Rozdział 6.4 uwzględnienie certyfikatu szkolno- testowego Rozdział 6.7.1 - uzupełnienie tabel z profilem certyfikatu, dopisanie atrybutów, Rozdział 6.7.1.1 – uzupełnienie tabeli: rozszerzeń standardowych i niestandardowych Rozdział 6.7.2 poprawki w tabeli elektroniczna treść listy CRL
1.3	15.05.2004	Artur Miękina Paweł Sałek	Rozszerzenie okresu ważności certyfikatu do 2 lat Dodanie w profilu certyfikacyjnym

			pola CRL Distribution Point Możliwość dostarczenia komponentów wraz z certyfikatami drogą pocztową oraz korespondencyjne podpisanie umów.
1.4	1.07.2005	Artur Miękina, Adam Mazurek Paweł Sałek, Michał Złonkiewicz, Franciszek Wołowski	• Usunięcie wzmianki o certyfikatach testowych • Dodanie informacji o nowych certyfikatach • Rozszerzenie przeznaczenia certyfikatu do zapewniania poufności danych • Zmiana definicji sponsora • Usunięcie możliwości zawieszenia/unieważnienia certyfikatu faksem • Dodanie wskazania adresu email ze strony do unieważniania certyfikatów • Dodanie zapisu mówiącego o zasadach weryfikacji przez Sponsora tożsamości jego subskrybentów • Zmiany w profilu certyfikatu
1.5	27.06.2008	Zespół Tworzenia Polityk Certyfikacji	• Dodanie zapisów odnośnie weryfikacji tożsamości przez notariuszy • Zmiana sum gwarancyjnych dla poszczególnych certyfikatów
1.6	04.01.2017	Zespół Tworzenia Polityk Certyfikacji	• Zmiany w rozdziale „Profil certyfikacji”

Data następnej nowelizacji dokumentu:……