POLSKIE CENTRUM CERTYFIKACJI ELEKTRONICZNEJ
Sigillum
POLSKA WYTWÓRNIA PAPIERÓW WARTOŚCIOWYCH S.A.

REGULAMIN PCCE DLA KWALIFIKOWANYCH ZNACZNIKÓW CZASU

Symbol dokumentu: P5.083
Data: 29 03 2005r
Wersja: 1.1

ROK ZAŁOŻENIA 1919

POLSKA WYTWÓRNIA PAPIERÓW WARTOŚCIOWYCH S.A.

Spis treści

1 Słownik ... 7

2 Wprowadzenie ... 10

2.1 Usługi certyfikacyjne Sigillum PCCE ... 10
2.2 Wprowadzanie zmian ... 10
2.3 Normy i Zalecenia ... 10
2.4 Hierarchia identyfikatorów obiektów X.500 ... 10
2.5 Struktura operacyjna systemu PKI obsługiwanego przez Sigillum PCCE ... 11
2.5.1 Domena produkcji certyfikatów ... 11
2.5.2 Domena odbiorców ... 12
2.6 Filozofia ochrony ... 12
2.7 Polityka kadrowa ... 12
2.8 Zarządzanie politykami certyfikacji ... 12
2.9 Podmioty systemu PKI zarządzanego przez Sigillum PCCE ... 13
2.9.1 Sigillum PCCE ... 13
2.9.2 Subskrybenci i odbiorcy usług certyfikacyjnych ... 14
2.10 Dane teleadresowe ... 14

3 Postanowienia ogólne ... 15

3.1 Obowiązki ... 15
3.1.1 Obowiązki Sigillum PCCE ... 15
3.1.2 Obowiązki subskrybenta ... 15
3.1.3 Obowiązki strony ufającej ... 15
3.1.4 Obowiązki repozytorium ... 15
3.2 Odpowiedzialność Sigillum PCCE ... 15
3.3 Zakres odpowiedzialności finansowej ... 15
3.4 Interpretacja i określenie prawa właściwego dla regulaminu ... 16
3.5 Opłaty ... 16
3.5.1 Opłaty za wystawienie znacznika czasu ... 16
3.5.2 Opłaty za inne usługi ... 16
3.5.3 Zwrot opłat ... 16
3.6 Publikowanie i repozytorium ... 16
3.6.1 Publikowanie informacji o funkcjonowaniu Sigillum PCCE ... 16
3.6.2 Częstotliwość publikacji ... 16
3.6.3 Kontrola dostępu ... 17
3.6.4 Repozytorium ... 17
3.7 Audyt ... 17
3.8 Poufność informacji ... 17

3.8.1 Rodzaje informacji uważanych za poufne 17
3.8.2 Rodzaje informacji, które nie są uważane za poufne 17
3.9 Prawa własności intelektualnej 18

4 Reguły dotyczące identyfikacji i uwierzytelniania podmiotów 19
4.1 Żądanie wystawienia znacznika czasu 19

5 Procedury operacyjne 20
5.1 Żądanie wystawienia znacznika czasu 20
5.2 Wystawianie znacznika czasu 20
5.3 Procedury audytu zabezpieczeń 20
5.3.1 Rodzaje rejestrowanych zdarzeń 20
5.3.2 Częstotliwość przeglądania dzienników zdarzeń 21
5.3.3 Okres przechowywania dzienników zdarzeń dla celów audytu 21
5.3.4 Zabezpieczenia dzienników zdarzeń dla celów audytu 21
5.3.5 Procedury wykonywania kopii zapasowych dzienników zdarzeń dla celów audytu 21
5.3.6 Prowadzenie dzienników zdarzeń 21
5.3.7 Powiadamianie o naruszeniach bezpieczeństwa 21
5.3.8 Ocena podatności na zagrożenia 21
5.4 Archiwizacja zapisów 22
5.4.1 Zabezpieczenie archiwów 22
5.4.2 Procedury archiwizacji 22
5.4.3 Wymagania na datowanie zapisów 22
5.5 Wymiana kluczy 22
5.6 Postępowanie po kompromitacji klucza lub innym zdarzeniu o potencjalnie dużym negatywnym znaczeniu dla działalności 22
5.6.1 Awaria zasobów obliczeniowych, oprogramowania lub danych23
5.6.2 Unieważnienie zaświadczenia certyfikacyjnego Sigillum PCCE23
5.6.3 Wykreślenie Sigillum PCCE z rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne 23
5.6.4 Zapewnienie możliwości przywrócenia funkcjonowania po katastrofie naturalnej lub innym zdarzeniu o potencjalnie dużym negatywnym znaczeniu dla działalności 24
5.7 Zakończenie działalności Sigillum PCCE 24
5.7.1 Uwagi 24
5.7.2 Przechowywanie archiwów 24

6 Fizyczne, proceduralne i osobowe środki zabezpieczenia 25
6.1 Zabezpieczenia fizyczne 25
6.1.1 Lokalizacja Centrum 25
6.1.2 Fizyczna kontrola dostępu 25
6.1.3 Zasilanie i klimatyzacja 25
6.1.4 Ochrona przed zalaniem wodą 25

6.1.5 Zapobieganie pożarom i ochrona przed ich skutkami 25
6.1.6 Przechowywanie nośników danych 25
6.1.7 Usuwanie niepotrzebnych nośników i danych 25
6.1.8 Kopia awaryjna poza siedzibą Sigillum PCCE 26
6.2 Kontrola proceduralna 26
6.2.1 Zaufane role 26
6.2.2 Dopuszczenie do pełnienia zaufanej roli 26
6.3 Nadzór osobowy 26
6.3.1 Wymagania dotyczące przygotowania, kwalifikacji, doświadczenia i sprawdzenia personelu 26
6.3.2 Kontrola przygotowania pracownika 26
6.3.3 Wymagania szkoleniowe 27
6.3.4 Wymagania na powtarzanie szkoleń 27
6.3.5 Częstotliwość i sposób rotacji stanowisk 27
6.3.6 Sankcje za nieuprawnione działania 27
6.3.7 Dokumentacja udostępniona personelowi 27

7 Techniczne środki zabezpieczeń 28
7.1 Generowanie i instalowanie par kluczy 28
7.1.1 Generowanie pary kluczy 28
7.1.2 Dostarczanie klucza publicznego Sigillum PCCE do odbiorców usług certyfikacyjnych 28
7.2 Ochrona klucza prywatnego 28
7.2.1 Standardy dotyczące modułu kryptograficznego 28
7.2.2 Podział klucza 28
7.2.3 Depozyt klucza prywatnego 28
7.2.4 Kopia zapasowa klucza prywatnego 28
7.2.5 Archiwizacja klucza prywatnego 28
7.2.6 Umieszczanie klucza prywatnego w module kryptograficznym 29
7.2.7 Metody aktywacji klucza prywatnego 29
7.2.8 Metody deaktywacji klucza prywatnego 29
7.2.9 Metody zniszczenia klucza prywatnego 29
7.3 Dane aktywujące klucze 29
7.3.1 Generowanie i instalowanie danych aktywujących klucze 29
7.3.2 Ochrona danych aktywujących klucze 29
7.4 Zarządzanie bezpieczeństwem komputerów 29
7.4.1 Specyfikacja wymagań technicznych na bezpieczeństwo komputerów 29
7.5 Zarządzanie cyklem życia elementów technicznch 29
7.5.1 Zarządzanie rozwojem systemu 30
7.5.2 Kontrola bezpieczeństwa zarządzania 30
7.6 Zarządzanie bezpieczeństwem sieciowym 30

8 Profil znacznika czasu i żądania znacznika czasu 31

8.1.1 Profil nieuwierzytelnionego żądania znacznika czasu (na podstawie RFC 3161) 31

8.1.2 Profil uwierzytelnionego żądania znacznika czasu 32

8.1.3 Profil odpowiedzi serwera znacznika czasu 33

9 Zarządzanie politykami i regulaminem certyfikacji 37

10 Załącznik A: Polityki certyfikacji wspierane przez niniejszy regulamin certyfikacji 38

1 Słownik

1) Ustawa - Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450)
2) Rozporządzenie - Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094)
3) Regulamin – niniejszy regulamin certyfikacji.
4) Polityka – polityka certyfikacji wspierana przez Regulamin.
5) Polska Wytwórnia Papierów Wartościowych S.A. - Sigillum PCCE – Polskie Centrum Certyfikacji Elektronicznej „Sigillum" – podmiot świadczący usługi certyfikacyjne w zakresie objętym niniejszym regulaminem nazywany dalej Sigillum PCCE.

   Sigillum PCCE świadczy także inne usługi certyfikacyjne, w tym kwalifikowane oraz niekwalifikowane usługi certyfikacyjne polegające na wystawianiu certyfikatów, jednak działalność Sigillum PCCE w tym zakresie nie jest uregulowana niniejszym regulaminem certyfikacji.
6) Algorytm RSA – algorytm kryptograficzny określony jednoznacznie przez identyfikator obiektu „{ joint-iso-ccitt(2) ds(5) module(1) algorithm(8) encryptionAlgorithm(1) 1 }"
7) Klucz – liczba, symbol lub ciąg liczb lub symboli jednoznacznie wyznaczający przekształcenie kryptograficzne spośród rodziny przekształceń zdefiniowanej przez algorytm kryptograficzny
8) Para kluczy algorytmu RSA – dwa klucze (*klucz prywatny* i *klucz publiczny*) wyznaczające wzajemnie odwrotne przekształcenia spośród rodziny przekształceń zdefiniowanej przez algorytm RSA
9) Klucz podpisujący – klucz prywatny służący do składania podpisu elektronicznego; klucz podpisujący stanowi dane służące do składania podpisu elektronicznego w rozumieniu Ustawy
10) 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
11) 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; certyfikat klucza weryfikującego podpis jest certyfikatem w rozumieniu Ustawy

12) Kwalifikowany certyfikat – certyfikat spełniający warunki określone w Ustawie, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne, spełniający wymogi określone w Ustawie

13) 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 organy wydającego zaświadczenia certyfikacyjne bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania poświadczenia elektronicznego
    b. jakakolwiek zmiana danych poświadczonych jest rozpoznawalna

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

15) Ścieżka certyfikacji znacznika czasu - uporządkowany ciąg zaświadczeń certyfikacyjnych 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 poświadczenie elektroniczne zawarte w jednym z nich zostało sporządzone przy pomocy danych służących do składania poświadczenia elektronicznego związanych z drugim z nich; ścieżka certyfikacji znacznika czasu zawiera zaświadczenie certyfikacyjne, o którym mowa w art. 23 ust. 2. Ustawy (zaświadczenie certyfikacyjne wystawiane kwalifikowanemu podmiotowi przez ministra właściwego ds. gospodarki lub podmiot przez niego upoważniony)

16) Lista ARL – lista unieważnionionych zaświadczeń certyfikacyjnych wystawionych przez dany podmiot świadczący usługi certyfikacyjne lub przez ministra właściwego ds. gospodarki lub podmiot przez niego upoważniony

17) Subskrybent usług certyfikacyjnych – osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która przysłała żądanie wystawienia znacznika czasu.

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

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

20) Kwalifikowane usługi certyfikacyjne – usługi certyfikacyjne świadczone przez podmiot posiadający wpis w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne, zgodnie z polityką odpowiadającą temu wpisowi
21) Komponent techniczny - sprzęt stosowany w celu wygenerowania lub użycia danych służących do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego.
22) 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
23) Znacznik czasu - jednostka danych oznaczająca moment, w którym zaszło określone zdarzenie względem ustalonego czasu odniesienia.
24) UTC - Coordinated Universal Time- rozwiązania zapewniające synchronizację z Międzynarodowym Wzorcem Czasu z dokładnością do 1 sekundy
25) Bezpieczne urządzenie służące do weryfikacji podpisu elektronicznego – urządzenie służące do weryfikacji podpisu elektronicznego spełniające wymagania określone w Ustawie i Rozporządzeniach

Określenia wykorzystywane w niniejszej regulaminie, a niezdefiniowane powyżej należy interpretować zgodnie z definicjami zawartymi w Ustawie i Rozporządzeniu.

2 Wprowadzenie

Niniejszy Regulamin Certyfikacji został opracowany w celu wspierania wykorzystywania znaczników czasu wystawianych przez Sigillum PCCE zgodnie z politykami certyfikacji określonymi w załączniku A.

Niniejszy Regulamin należy rozpatrywać łącznie z odpowiadającą polityką certyfikacji, opracowaną i opublikowaną przez Sigillum PCCE.

Niniejszy Regulamin stanowi własność intelektualną PWPW SA. Podmioty inne niż Sigillum PCCE nie mają prawa do wystawiania znaczników czasu zawierających oznaczenia zgodności z niniejszym Regulaminem bez uprzedniej zgody Sigillum PCCE.

Niniejszy regulamin zawiera opis procedur obowiązujących przy świadczeniu usług certyfikacyjnych przez Sigillum PCCE w ramach polityk wspieranych przez regulamin oraz sposób wykorzystywania istotnych dla bezpieczeństwa zasobów przy realizacji tych procedur.

2.1 Usługi certyfikacyjne Sigillum PCCE

PWPW S.A. -Sigillum PCCE jest kwalifikowanym podmiotem świadczącym usługi certyfikacyjne polegające na wystawianiu znaczników czasu, zgodnie z Ustawą i Rozporządzeniem.

2.2 Wprowadzanie zmian

Regulamin podlega standardowym procedurom przeprowadzanym przez Radę Zatwierdzania Polityk Certyfikacji Sigillum PCCE zgodnie ze statutem Rady.

Rada Zatwierdzania Polityk Certyfikacji Sigillum PCCE jest również podmiotem uprawnionym do wprowadzania i zatwierdzania zmian w Regulaminie. Nowe wersje Regulaminu otrzymują nowy, unikalny numer wersji.

O zmianie regulaminu certyfikacji Sigillum PCCE powiadamia ministra właściwego ds. gospodarki niezwłocznie, nie później niż w terminie 7 dni od daty zatwierdzenia zmiany przez Zarząd PWPW S.A. i dostarczenia Kierownikowi Sigillum PCCE decyzji o zmianie regulaminu wraz z dokumentem potwierdzającym akceptację zmiany przez Zarząd PWPW S.A.

2.3 Normy i Zalecenia

Struktura regulaminu certyfikacji opiera się na dokumencie “Internet X.509 Public Key Infrastructure Certificate policy and Certification Practices Framework”i została dostosowana do potrzeb Sigillum PCCE.

2.4 Hierarchia identyfikatorów obiektów X.500

Identyfikatory obiektów X.500 (OID) występujących w systemie PKI obsługiwanym przez Sigillum PCCE zostały określone w dokumencie , opracowanym przez Sigillum PCCE.

Przydzielono identyfikatory OID Sigillum PCCE, jako kwalifikowanemu podmiotowi świadczącemu usługi certyfikacyjne (OID: : { iso(1) member-body(2) PL(616) organisation(1) 113560 }) oraz politykom certyfikacji wspieranych przez Regulamin.

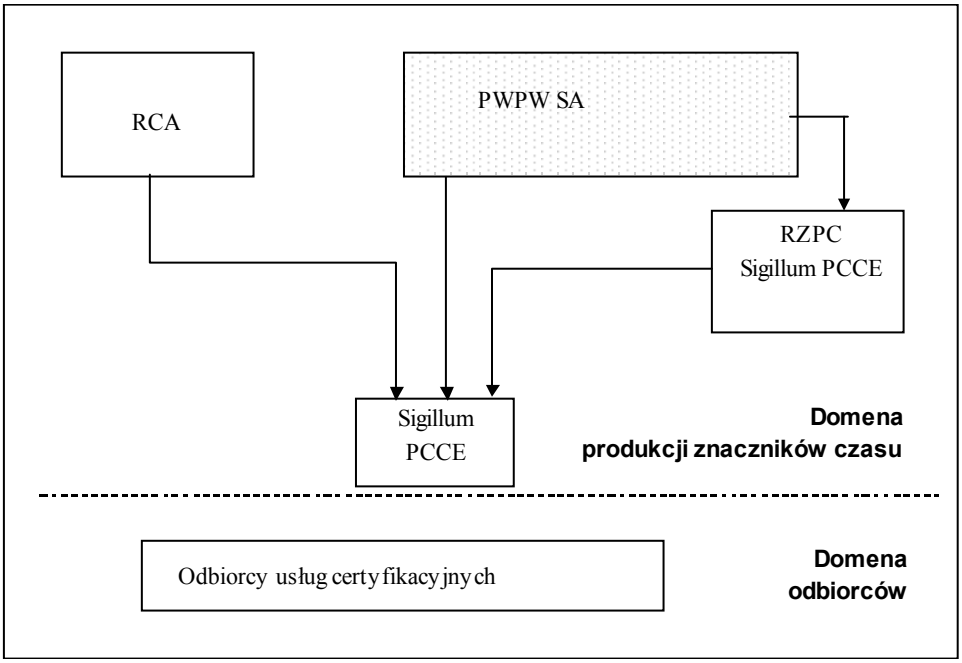
Nie przydziela się identyfikatorów OID regulaminom certyfikacji.

Numery OID przydzielone politykom certyfikacji są określone w tych politykach.

2.5 Struktura operacyjna systemu PKI obsługiwanego przez Sigillum PCCE

Struktura operacyjna systemu PKI obsługiwanego przez Sigillum PCCE oraz usytuowanie tego systemu zostały określone na rysunku poniżej.

Wyjaśnienie poszczególnych punktów zamieszczono w kolejnych podrozdziałach.



Rysunek 3 Struktura operacyjna systemu PKI obsługiwanego przez Sigillum PCCE oraz jego usytuowanie

2.5.1 Domena produkcji certyfikatów

W skład domeny produkcji certyfikatów wchodzi:

1) RCA (ang. *RootCA*), czyli działający na podstawie Ustawy minister ds. gospodarki lub podmiot upoważniony na podstawie art. 23 ust. 4 lub 5 Ustawy;
2) PWPW SA, jako firma świadcząca usługi certyfikacyjne;
3) RZPC Sigillum PCCE, czyli utworzona przez PWPW SA Rada Zatwierdzania Polityk Certyfikacji;
4) Sigillum PCCE (Polskie Centrum Certyfikacji Elektronicznej Sigillum), jako jednostka organizacyjna PWPW SA utworzona w celu świadczenia usług certyfikacyjnych.

2.5.2 Domena odbiorców

Domena odbiorców składa się z odbiorców usług certyfikacyjnych świadczonych przez Sigillum PCCE zgodnie z polityką wspieraną przez niniejszy regulamin. Do odbiorców usług certyfikacyjnych zaliczają się również subskrybenci Sigillum PCCE.

2.6 Filozofia ochrony

Celem procedur i mechanizmów ochrony działalności Sigillum PCCE jest zapewnienie:

1) Poufności danych, które mają pozostać poufne (w tym szczególnie klucza prywatnego Sigillum PCCE).
2) Pewności co do oznaczenia wystawianych znaczników właściwym, rzetelnym i dokładnym czasem.
3) Bezpieczeństwa związku pomiędzy zawartymi w znaczniku: czasem i kryptograficznym skrótem oznaczanego dokumentu.
4) Wysokiego poziomu dostępności usług świadczonych przez Sigillum PCCE.

Filozofia ochrony w Sigillum PCCE polega między innymi na stałym monitorowaniu zagrożeń i reagowaniu na nie oraz stosowaniu najnowszych technologii i wiedzy, przede wszystkim zawartych w normach krajowych i międzynarodowych.

2.7 Polityka kadrowa

Sigillum PCCE opracowało i stosuje procedury związane z zatrudnianiem personelu zapewniające jego wysoki profesjonalizm.

Personel Sigillum PCCE wykonujący zadania związane z działalnością certyfikacyjną prowadzoną przez Sigillum PCCE spełnia wymagania określone w Ustawie.

2.8 Zarządzanie politykami certyfikacji

PWPW S.A. utworzyła jednostkę organizacyjną zwaną „Radą Zatwierdzania Polityk Certyfikacji”, mającą uprawnienia i odpowiedzialną za zarządzanie politykami certyfikacji funkcjonującymi w Sigillum PCCE.

Do głównych obowiązków Rady Zatwierdzania Polityk Certyfikacji należy:

1) zatwierdzanie polityk i regulaminów certyfikacji,
2) zatwierdzanie zmian w politykach i regulaminach certyfikacji,
3) zarządzanie numerami OID polityk certyfikacji obowiązujących w Sigillum PCCE,
4) powoływanie Zespołów Tworzących Polityki Certyfikacji opracowujących nowe polityki oraz regulaminy certyfikacji, na podstawie założeń opracowanych przez Radę Zatwierdzania Polityk Certyfikacji – jeśli wystąpi potrzeba opracowania nowych polityk lub regulaminów certyfikacji, lub potrzeba modyfikacji istniejących polityk lub regulaminów,
5) utrzymywanie i okresowa ocena funkcjonujących polityk i regulaminów certyfikacji,
6) zapewnienie właściwego udostępniania polityk i regulaminów certyfikacji.

O zmianach w politykach certyfikacji Sigillum PCCE powiadamia ministra właściwego ds. gospodarki niezwłocznie, nie później niż w terminie 7 dni od daty zatwierdzenia zmiany przez Zarząd PWPW S.A.

2.9 Podmioty systemu PKI zarządzanego przez Sigillum PCCE

2.9.1 Sigillum PCCE

Sigillum PCCE świadczy usługi certyfikacyjne polegające na wystawianiu znaczników czasu, zgodnie z Ustawą oraz przyjętą przez Sigillum PCCE polityką certyfikacji.

Sigillum PCCE używa do podpisywania znaczników algorytmu RSA, z kluczem o długości 2048 bitów.

Sigillum PCCE wykonuje następujące zadania:

1) generuje własne klucze;
2) dostarcza zgłoszenie certyfikacyjne dotyczące własnych kluczy do ministra właściwego ds. gospodarki lub podmiotu przez niego wskazanego;
3) publikuje politykę i regulamin certyfikacji, w oparciu o które działa, oraz inne dane wymienione jako zawartość repozytorium w polityce certyfikacji;
4) generuje znaczniki czasu, po weryfikacji uprawnień potencjalnego subskrybenta do otrzymania znacznika;
5) przeprowadza regularne audyty swojej działalności.

2.9.2 Subskrybenci i odbiorcy usług certyfikacyjnych

Subskrybentami i odbiorcami usług certyfikacyjnych mogą być osoby fizyczne, prawne lub organizacje nieposiadające osobowości prawnej.

2.10 Dane teleadresowe

Zapytania skargi oraz inne sprawy związane z niniejszym regulaminem powinny być kierowane do:

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 25 34

adres serwera znacznika czasu:

193.178.164.5:80 lub uzc.sigillum.pl:80

3 Postanowienia ogólne

3.1 Obowiązki

3.1.1 Obowiązki Sigillum PCCE

Sigillum PCCE jest zobowiązane do:

1) utrzymywania infrastruktury operacyjnej systemu PKI w zakresie określonym w niniejszym regulaminie;
2) prowadzenia działalności w sposób efektywny i wiarygodny w zgodzie z:
   a. Ustawą i aktami wykonawczymi,
   b. obowiązującą polityką i regulaminem certyfikacji,
   c. wewnętrznymi procedurami obowiązującymi w Sigillum PCCE.
3) uzyskania zaświadczenia certyfikacyjnego ministra właściwego ds. gospodarki;
4) wystawiania znaczników czasu po spełnieniu przez subskrybenta wymogów wynikających z polityki certyfikacji;
5) publikowania w repozytorium danych określonych w polityce certyfikacji;
6) archiwizacji danych związanych ze świadczeniem usług certyfikacyjnych.

3.1.2 Obowiązki subskrybenta

Obowiązki subskrybenta usług certyfikacyjnych są określone w polityce certyfikacji, według której wystawiono certyfikat.

3.1.3 Obowiązki strony ufającej

Obowiązki strony ufającej są określone w polityce certyfikacji, według której wystawiono certyfikat.

3.1.4 Obowiązki repozytorium

Sigillum PCCE prowadzi repozytorium dostępne przez protokoły HTTP.

Zawartość repozytorium oraz wymagania dotyczące jego dostępności określono w polityce certyfikacji.

3.2 Odpowiedzialność Sigillum PCCE

Zasady odpowiedzialności Sigillum PCCE zostały określone w polityce certyfikacji, według której wystawiono dany certyfikat.

3.3 Zakres odpowiedzialności finansowej

Zakres odpowiedzialności PWPW S.A. określony jest w polityce certyfikacji, zgodnie z którą został wystawiony znacznik czasu.

3.4 Interpretacja i określenie prawa właściwego dla regulaminu

Niniejszy regulamin podlega prawodawstwu obowiązującemu w Rzeczpospolitej Polskiej.

3.5 Opłaty

3.5.1 Opłaty za wystawienie znacznika czasu

Sigillum PCCE pobiera opłaty za wystawienie znacznika czasu, zgodnie z cennikiem opłat opublikowanym w repozytorium.

3.5.2 Opłaty za inne usługi

Nie pobiera się opłat za udostępnienie polityki oraz regulaminu certyfikacji za pośrednictwem repozytorium.

3.5.3 Zwrot opłat

Nie przewiduje się zwrotu opłat za wygenerowanie znaczników czasu, w szczególności w przypadku utraty ważności przez te znaczniki.

3.6 Publikowanie i repozytorium

3.6.1 Publikowanie informacji o funkcjonowaniu Sigillum PCCE

3.6.1.1 Publikowanie w postaci elektronicznej

Niniejszy regulamin i polityki certyfikacji są publikowane elektronicznie w postaci plików w repozytorium Sigillum PCCE i są dostępne pod adresem: www.sigillum.pl/repozytorium

Oprócz powyższych dokumentów, w postaci elektronicznej publikowany jest aktualny cennik.

3.6.1.2 Publikacje drukowane

Nie przewiduje się rozpowszechniania papierowych wersji dokumentów.

3.6.2 Częstotliwość publikacji

Nowe wersje polityk oraz regulaminów certyfikacji są publikowane niezwłocznie po zatwierdzeniu.

3.6.3 Kontrola dostępu

Nie realizuje się kontroli dostępu w trybie "do odczytu" do repozytorium Sigillum PCCE, w celu pobrania opublikowanych tam danych lub dokumentów.

Realizuje się kontrolę dostępu uniemożliwiającą dokonywanie nieautoryzowanych zmian w repozytorium.

3.6.4 Repozytorium

Sigillum PCCE prowadzi repozytorium dostępne za pomocą protokołów HTTP.

Repozytorium nie zawiera żadnych informacji o poufnym charakterze.

Szczegóły umożliwiające dostęp do repozytorium oraz szczegóły określające dostępność do repozytorium zostały zamieszczone w polityce certyfikacji.

3.7 Audyt

Sigillum PCCE podlega audytom na zasadach określonych w Ustawie.

3.8 Poufność informacji

3.8.1 Rodzaje informacji uważanych za poufne

Wszystkie dane, których nieuprawnione ujawnienie mogłoby narazić na szkodę podmiot świadczący usługi certyfikacyjne lub odbiorcę usług certyfikacyjnych, a w szczególności dane służące do składania poświadczeń elektronicznych, są objęte tajemnicą. Odstępstwo od zachowania tajemnicy może wynikać jedynie z art. 12 ust. 3 Ustawy.

Tajemnicą są objęte również dane osobowe subskrybentów.

3.8.1.1 Gromadzenie i wykorzystywanie danych osobowych

Zasady gromadzenia i wykorzystywania danych osobowych zgodne są z obowiązującą Ustawą o ochronie danych osobowych.

Dane osobowe nie są wykorzystywane do celów innych niż obsługa subskrybenta w zakresie usług certyfikacyjnych.

3.8.2 Rodzaje informacji, które nie są uważane za poufne

3.8.2.1 Dokumentacja Sigillum PCCE

Następujące dokumenty Sigillum PCCE są uważane za dokumenty, które mogą być publicznie dostępne:

1) polityki certyfikacji,

2) regulaminy certyfikacji,
3) inne dokumenty, wymienione w polityce certyfikacji jako dokumenty znajdujące się w repozytorium.

3.9 Prawa własności intelektualnej

Sigillum PCCE oświadcza, że jest w posiadaniu urządzeń oraz licencji na oprogramowanie wykorzystywane przy realizacji niniejszego regulaminu.

Sigillum PCCE gwarantuje, że wykorzystywanie niniejszego regulaminu nie narusza praw autorskich stron trzecich.

Sigillum PCCE wyklucza swoją odpowiedzialność za wszelkie inne ewentualne naruszenia praw autorskich.

Wszystkie prawa własności intelektualnej, włączając prawa do wszystkich dokumentów tworzonych przez PWPW SA na potrzeby tej polityki (w postaci elektronicznej lub innej), należą do PWPW SA i pozostają jej własnością.

4 Reguły dotyczące identyfikacji i uwierzytelniania podmiotów

4.1 Żądanie wystawienia znacznika czasu

Reguły uwierzytelnienia podmiotu przy żądaniu wystawienia znacznika czasu określone są przez politykę certyfikacji.

5 Procedury operacyjne

5.1 Żądanie wystawienia znacznika czasu

Żądanie wystawienia znacznika czasu jest przysyłane przez subskrybenta za pomocą protokołu HTTP, na adres serwera znacznika czasu określony w rozdziale 2.10.

Żądanie powinno być podpisane elektronicznie przez subskrybenta oraz zawierać certyfikat klucza weryfikującego podpis.

Dla wybranych grup klientów, identyfikowanych innymi sposobami (w szczególności dla wewnętrznych podmiotów systemu Sigillum PCCE), może być dopuszczona możliwość przyjmowania niepodpisanych żądań wystawienia znacznika czasu.

5.2 Wystawianie znacznika czasu

Po otrzymaniu wniosku o wystawienie znacznika czasu, Sigillum PCCE:

1) weryfikuje podpis elektroniczny pod wnioskiem,
2) sprawdza uprawnienia potencjalnego subskrybenta do otrzymania znacznika (tzn. sprawdza, czy subskrybent posługuje się certyfikatem wydanym przez upoważnione centrum certyfikacji oraz czy nie zostały mu odebrane prawa do otrzymywania znaczników czasu),
3) jeśli weryfikacja uprawnień przebiegła pomyślnie – wystawia i wysyła znacznik (w ramach tej samej sesji sieciowej).

Strona ufająca może otrzymać potrzebny jej znacznik czasu od subskrybenta.

Sigillum PCCE nie magazynuje wystawionych znaczników czasu i nie prowadzi usługi udostępniania wcześniej wystawionych znaczników.

Dla wybranych grup klientów, identyfikowanych innymi sposobami (w szczególności dla wewnętrznych podmiotów systemu Sigillum PCCE), punkty 1) i 2) powyżej pomija się.

5.3 Procedury audytu zabezpieczeń

Sigillum PCCE prowadzi dzienniki zdarzeń związanych ze świadczeniem usług certyfikacyjnych.

5.3.1 Rodzaje rejestrowanych zdarzeń

Zapisy dzienników zdarzeń obejmują co najmniej:

1) żądania świadczenia usług certyfikacyjnych normalnie udostępnianych przez system lub usług nie wykonywanych przez system oraz informacji o wykonaniu lub niewykonaniu usługi oraz powód jej niewykonania,

2) istotne zdarzenia związane ze zmianami w środowisku systemu, w tym w podsystemie zarządzania kluczami, w szczególności tworzenie kont i rodzaj przydzielanych uprawnień,
3) instalacje nowego oprogramowania lub aktualizacje,
4) rozpoczęcie i przerwanie funkcji rejestrujących zdarzenia,
5) czas tworzenia kopii zapasowych,
6) czas archiwizowania rejestrów zdarzeń,
7) zamykanie, otwieranie i ponowne uruchamiania po zamknięciu systemu,
8) negatywne wyniki testów, o których mowa w § 15 ust. 8 Rozporządzenia,
9) rejestrowanie błędów w działaniach źródła czasu.

Wszystkie zapisy dzienników zdarzeń oznaczone są czasem z dokładnością do jednej sekundy.

5.3.2 Częstotliwość przeglądania dzienników zdarzeń

Zapisy dzienników zdarzeń są przeglądane przez administratora systemu i inspektora do spraw audytu przynajmniej raz w każdym dniu roboczym.

5.3.3 Okres przechowywania dzienników zdarzeń dla celów audytu

Zapisy zdarzeń są przechowywane przez okres co najmniej 3 lat od powstania zapisu.

5.3.4 Zabezpieczenia dzienników zdarzeń dla celów audytu

Zapisy zdarzeń są przechowywane w formie gwarantującej integralność.

5.3.5 Procedury wykonywania kopii zapasowych dzienników zdarzeń dla celów audytu

Sigillum PCCE opracowało i przestrzega procedur wykonywania kopii zapasowych dzienników zdarzeń, z zachowaniem integralności danych.

5.3.6 Prowadzenie dzienników zdarzeń

Dzienniki zdarzeń prowadzone są przez Sigillum PCCE w postaci elektronicznej (z zapisem automatycznym i ręcznym) oraz w postaci papierowej (z zapisem ręcznym). Wszędzie, gdzie to tylko możliwe, zastosowano zapis automatyczny.

5.3.7 Powiadamianie o naruszeniach bezpieczeństwa

W przypadku wystąpienia krytycznego błędu związanego z bezpieczeństwem lub naruszenia bezpieczeństwa powiadamiany jest inspektor bezpieczeństwa.

5.3.8 Ocena podatności na zagrożenia

Sigillum PCCE opracowało ocenę ryzyka związanego z bezpieczeństwem funkcjonowania systemu.

5.4 Archiwizacja zapisów

Sigillum PCCE prowadzi archiwum zawierające zapisy określone w niniejszym regulaminie.

Zapisy dzienników zdarzeń są przechowywane przez okres co najmniej 3 lat.

5.4.1 Zabezpieczenie archiwów

Nośniki informacji zawierające zarchiwizowane dane są zabezpieczone za pomocą fizycznych metod kontroli dostępu. Są one zabezpieczone ponadto przed wpływem czynników środowiskowych takich jak temperatura, wilgotność i pole magnetyczne.

Integralność archiwów jest zapewniona przy użyciu podpisów elektronicznych wykonywanych za pomocą kluczy infrastruktury.

5.4.2 Procedury archiwizacji

Sigillum PCCE opracowało i wdrożyło procedury archiwizacji, procedury przechowywania i dostępu do danych archiwalnych (dokument „Procedury audytu i archiwizacji").

5.4.3 Wymagania na datowanie zapisów

Nie określa się wymagań co do konieczności datowania zapisów archiwum. Nie narusza to obowiązku zapisania daty każdego zdarzenia, w sposób określony w rozdziale 5.3.1.

5.5 Wymiana kluczy

Wymiana kluczy Sigillum PCCE nie jest wykonywana automatycznie. Klucze wygasają zgodnie z terminem ważności zaświadczenia certyfikacyjnego wystawionego Sigillum PCCE przez ministra właściwego ds. gospodarki lub podmiot przez niego upoważniony.

Klucze powinny być wymienione odpowiednio wcześnie przed upłynięciem ich terminu ważności, tak aby okres ważności wystawianych znaczników czasu był odpowiednio długi.

Istnieje konieczność otrzymania nowego zaświadczenia certyfikacyjnego od ministra właściwego ds. gospodarki lub podmiotu przez niego wskazanego.

Po wygaśnięciu zaświadczenia certyfikacyjnego zawierającego stary klucz publiczny Sigillum PCCE, związany z nim klucz prywatny jest niszczony za pomocą procedur określonych w rozdziale 7.2.9.

5.6 Postępowanie po kompromitacji klucza lub innym zdarzeniu o potencjalnie dużym negatywnym znaczeniu dla działalności

Sigillum PCCE:

1) opracowało i wdrożyło szczegółową dokumentację zawierającą:

a. plan zapewnienia ciągłości funkcjonowania, obejmujący sytuację kompromitacji klucza prywatnego Sigillum PCCE, awarie sprzętu, oprogramowania i linii komunikacyjnych oraz naturalne katastrofy takie jak pożar i powódź;

b. dokument opisujący podstawową konfigurację, dotyczący między innymi systemów operacyjnych, oprogramowania antywirusowego i specyficznego oprogramowania PKI;

c. procedury tworzenia kopii zapasowych i archiwalnych oraz procedury przechowywania danych poza siedzibą Sigillum PCCE.

2) przedstawia powyższą dokumentację na żądanie ministra właściwego ds. gospodarki lub podmiotu przez niego wskazanego;

3) przeprowadza szkolenia swojego personelu dotyczące procedur postępowania w sytuacjach awaryjnych o potencjalnie dużym negatywnym znaczeniu dla działalności Sigillum PCCE;

5.6.1 Awaria zasobów obliczeniowych, oprogramowania lub danych

Sigillum PCCE opracowało i wdrożyło dokument opisujący podstawową konfigurację oraz procedury wykonywania kopii zapasowych i archiwalnych. Postępowanie w przypadku wystąpienia awarii zasobów obliczeniowych lub oprogramowania określają procedury wynikające z umów serwisowych zawartych przez Sigillum PCCE.

5.6.2 Unieważnienie zaświadczenia certyfikacyjnego Sigillum PCCE

Sigillum PCCE opracowało i wdrożyło plan zapewnienia ciągłości funkcjonowania, obejmujący sytuację unieważnienia zaświadczenia certyfikacyjnego wystawionego Sigillum PCCE przez ministra właściwego ds. gospodarki lub podmiot przez niego upoważniony

Plan ten zawiera obowiązek niezwłocznego zniszczenia klucza prywatnego związanego z unieważnionym zaświadczeniem certyfikacyjnym za pomocą procedur określonych w rozdziale 7.2.9.

5.6.3 Wykreślenie Sigillum PCCE z rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne

Sigillum PCCE opracowało i wdrożyło plan zapewnienia ciągłości funkcjonowania, obejmujący sytuację wykreślenia Sigillum PCCE z rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

Plan ten zawiera obowiązek zaprzestania świadczenia usług certyfikacyjnych po otrzymaniu decyzji o wykreśleniu Sigillum PCCE z rejestru, w zakresie polityki certyfikacji, której dotyczy decyzja.

5.6.4 Zapewnienie możliwości przywrócenia funkcjonowania po katastrofie naturalnej lub innym zdarzeniu o potencjalnie dużym negatywnym znaczeniu dla działalności

Sigillum PCCE opracowało i wdrożyło plan postępowania obejmujący procedury wykonywania kopii zapasowych oraz archiwalnych oraz zasady przechowywania tych kopii poza siedzibą Sigillum PCCE.

Sigillum PCCE zorganizowało i utrzymuje ośrodek zapasowy, zdolny do przejęcia funkcji ośrodka podstawowego w sytuacjach awaryjnych.

5.7 Zakończenie działalności Sigillum PCCE

Jeśli wystąpi potrzeba zakończenia działalności Sigillum PCCE, zapewni ono zminimalizowanie skutków tego faktu dla odbiorców usług certyfikacyjnych, w takim stopniu w jakim to będzie możliwe.

5.7.1 Uwagi

W przypadku planowego zakończenia działalności Sigillum PCCE, Sigillum PCCE informuje niezwłocznie o tym fakcie ministra właściwego ds. gospodarki, oraz publikuje stosowną informację w repozytorium, z wyprzedzeniem co najmniej trzech miesięcy. Informacja taka będzie również opublikowana w dzienniku o zasięgu ogólnopolskim.

Opublikowana informacja będzie pouczała użytkowników o konieczności powtórnego oznakowania czasem dokumentów oznaczonych przez Sigillum PCCE, pod rygorem utraty ważności znaczników czasu.

W przypadku awaryjnego zakończenia działalności Sigillum PCCE, na przykład w wyniku kompromitacji klucza prywatnego, Sigillum PCCE niezwłocznie poinformuje niezwłocznie, nie później niż w terminie 7 dni, o sytuacji ministra właściwego ds. gospodarki. Sigillum PCCE dostarczy w takim przypadku odbiorcom usług certyfikacyjnych tak wiele informacji, jak tylko będzie to w danych okolicznościach praktyczne i rozsądne.

Wszystkie znaczniki czasu wystawione przez Sigillum PCCE weryfikowane przy użyciu zaświadczenia certyfikacyjnego Sigillum PCCE wystawionego przez ministra właściwego ds. gospodarki lub podmiot przez niego wyznaczony, po unieważnieniu tego zaświadczenia stracą ważność.

5.7.2 Przechowywanie archiwów

Po zakończeniu działalności, archiwa danych związanych ze świadczeniem usług certyfikacyjnych są przekazywane ministrowi właściwemu ds. gospodarki, na podstawie art. 13 ust. 3 Ustawy.

6 Fizyczne, proceduralne i osobowe środki zabezpieczenia

6.1 Zabezpieczenia fizyczne

6.1.1 Lokalizacja Centrum

Sigillum PCCE jest umiejscowione w bezpiecznym środowisku na terenie PWPW SA.

6.1.2 Fizyczna kontrola dostępu

Sigillum PCCE jest wydzieloną jednostką PWPW SA. Fizyczna kontrola dostępu do Sigillum PCCE jest zapewniona przez standardowe procedury ochrony dostępu obowiązujące na terenie PWPW SA oraz przez dodatkowe środki, zapewniające możliwość dostępu do CCE tylko osób uprawnionych.

6.1.3 Zasilanie i klimatyzacja

Pomieszczenia Sigillum PCCE, w których umieszczone są elementy techniczne, są wyposażone w awaryjne systemy zasilania oraz w systemy klimatyzacyjne.

6.1.4 Ochrona przed zalaniem wodą

Pomieszczenia Sigillum PCCE są chronione przez zalaniem wodą.

6.1.5 Zapobieganie pożarom i ochrona przed ich skutkami

Pomieszczenia Sigillum PCCE są chronione przez wystąpieniem pożaru, zgodnie z obowiązującymi przepisami.

6.1.6 Przechowywanie nośników danych

Nośniki dane przechowywane przez Sigillum PCCE są zabezpieczone przed wpływem czynników środowiskowych takich jak temperatura, wilgotność i pole magnetyczne.

6.1.7 Usuwanie niepotrzebnych nośników i danych

Dokumenty papierowe i nośniki magnetyczne zawierające elementy podlegające ochronie są niszczone poprzez:

1) w przypadku nośników magnetycznych:
    a. fizyczne zniszczenie nośnika,
2) w przypadku dokumentów papierowych:
    a. zniszczenie w niszczarce do papieru;

6.1.8 Kopia awaryjna poza siedzibą Sigillum PCCE

Sigillum PCCE opracowało i wdrożyło procedury zapewniające przechowywanie dwóch jednakowych kompletów kopii zapasowych i archiwalnych:
1) jednego w ośrodku podstawowym,
2) drugiego w ośrodku zapasowym.

6.2 Kontrola proceduralna

6.2.1 Zaufane role

W celu rozdziału odpowiedzialności osób pełniących zaufane role w Sigillum PCCE, zgodnie z aktami wykonawczymi do Ustawy, CCE definiuje następujące role personelu:

1) osoby nadzorujące wdrożenie i stosowanie wszystkich procedur bezpiecznej eksploatacji systemów teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych, zwane dalej „Inspektorami Bezpieczeństwa”,
2) osoby, które instalują, konfigurują i zarządzają systemem i siecią teleinformatyczną zwane dalej „Administratorami Systemu”,
3) osoby, które wykonują stałą obsługę systemu teleinformatycznego, w tym tworzące kopie zapasowe, zwane dalej „Operatorami Systemu”,
4) osoby, które analizują zapisy rejestrów zdarzeń mających miejsce w systemach teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych, zwane dalej „Inspektorami ds. Audytu”.

Nie mogą być ze sobą łączone funkcje, o których mowa w pkt 1 i 2 oraz w pkt 1 i 3. Funkcja, o której mowa w pkt. 4 nie może być łączona z żadną inną z funkcji wymienionych powyżej.

6.2.2 Dopuszczenie do pełnienia zaufanej roli

Osoby pełniące zaufane role musza się cieszyć zaufaniem kierownictwa Sigillum PCCE oraz spełniać wymagania określone Ustawą.

6.3 Nadzór osobowy

6.3.1 Wymagania dotyczące przygotowania, kwalifikacji, doświadczenia i sprawdzenia personelu

Procedury zatrudniania i wyboru personelu powinny uwzględniać przygotowanie, kwalifikacje, doświadczenie i wymagania co do metod sprawdzenia osoby zatrudnianej na dane stanowisko.

6.3.2 Kontrola przygotowania pracownika

Kontrola przygotowania do pracy na danym stanowisku wiążącym się z pełnieniem zaufanej roli w Sigillum PCCE jest przeprowadzana w stosunku do każdego nowego pracownika, przed dopuszczeniem go do wykonywania obowiązków.

6.3.3 Wymagania szkoleniowe

Wszyscy pracownicy Sigillum PCCE, pełniący zaufane role w CCE, są szkoleni w szczególności z następujących dziedzin:

1) automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych,
2) mechanizmów zabezpieczania sieci i systemów teleinformatycznych,
3) kryptografii, podpisów elektronicznych i infrastruktury klucza publicznego,
4) sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych.

6.3.4 Wymagania na powtarzanie szkoleń

Kierownik Sigillum PCCE określa plan szkoleń, zapewniający utrzymanie przez personel Sigillum PCCE wysokiego poziomu wiedzy.

6.3.5 Częstotliwość i sposób rotacji stanowisk

Sigillum PCCE nie realizuje planowej rotacji stanowisk swoich pracowników.

6.3.6 Sankcje za nieuprawnione działania

Sigillum PCCE może nałożyć na swoich pracowników, za nieuprawnione działania, kary wynikające z Kodeksu Pracy.

W przypadku wykonywania przez członków personelu Sigillum PCCE nieuprawnionych działań, mogą się oni narazić również na sankcje wynikające z innych przepisów, w tym z Ustawy, z ustawy o nieuczciwej konkurencji oraz z kodeksu karnego.

6.3.7 Dokumentacja udostępniona personelowi

Personel Sigillum PCCE ma dostęp do:

1) wszelkiej odnoszącej się do CCE dokumentacji sprzętu i oprogramowania wykorzystywanego przez CCE;
2) polityk i regulaminów certyfikacji;
3) procedur operacyjnych obowiązujących w Sigillum PCCE.

7 Techniczne środki zabezpieczeń

7.1 Generowanie i instalowanie par kluczy

7.1.1 Generowanie pary kluczy

Para kluczy Sigillum PCCE jest generowana w bezpiecznym urządzeniu, w obecności co najmniej dwóch uprawnionych osób, przy czym jedną z nich musi być inspektor ds. audytu.

7.1.2 Dostarczanie klucza publicznego Sigillum PCCE do odbiorców usług certyfikacyjnych

Klucz publiczny Sigillum PCCE – w postaci zaświadczenia certyfikacyjnego, może być pobrany przez subskrybenta z repozytorium Sigillum PCCE.

7.2 Ochrona klucza prywatnego

7.2.1 Standardy dotyczące modułu kryptograficznego

Moduł kryptograficzny wykorzystywany przez Sigillum PCCE do przetwarzania klucza prywatnego Sigillum PCCE, posiada certyfikat ITSEC E3 z „wysoką” siłą mechanizmów.

7.2.2 Podział klucza

Klucz prywatny Sigillum PCCE jest podzielony na 8 fragmentów.

7.2.3 Depozyt klucza prywatnego

Nie dopuszcza się możliwości składania klucza prywatnego w depozyt.

7.2.4 Kopia zapasowa klucza prywatnego

Mechanizm zapewnienia kopii zapasowej klucza prywatnego Sigillum PCCE jest zrealizowany dzięki podziałowi klucza na fragmenty w liczbie większej niż jest wymagana do odtworzenia klucza.

7.2.5 Archiwizacja klucza prywatnego

Nie dopuszcza się archiwizacji żadnych kluczy prywatnych służących do składania podpisu elektronicznego lub uwierzytelnienia, to jest w szczególności klucza prywatnego Sigillum PCCE służącego do poświadczania znaczników czasu.

Dopuszcza się archiwizację przez subskrybenta, w bezpieczny sposób, jego klucza prywatnego służącego do deszyfrowania danych lub kluczy.

7.2.6 Umieszczanie klucza prywatnego w module kryptograficznym

Klucz prywatny może być przetwarzany wyłącznie w komponencie technicznym. Klucz może być wynoszony poza komponent techniczny jedynie na zabezpieczonych modułach kluczowych, w postaci podzielonej na fragmenty.

7.2.7 Metody aktywacji klucza prywatnego

Aktywacja klucza prywatnego Sigillum PCCE wymaga współdziałania dwóch osób posiadających karty z fragmentami klucza oraz kody PIN do tych kart.

7.2.8 Metody deaktywacji klucza prywatnego

Deaktywacja klucza prywatnego Sigillum PCCE następuje w wyniku wyjęcia z czytnika komponentu technicznego przynajmniej jednej z dwóch kart zawierających fragmenty klucza.

7.2.9 Metody zniszczenia klucza prywatnego

Klucz prywatny Sigillum PCCE jest niszczony wraz z fizycznym zniszczeniem wszystkich modułów kluczowych, które zawierają fragmenty tego klucza.

7.3 Dane aktywujące klucze

7.3.1 Generowanie i instalowanie danych aktywujących klucze

Dane aktywujące fragmenty klucza prywatnego Sigillum PCCE – w postaci kodów PIN – są określane zgodnie z procedurami opisanymi w dokumencie „Procedury operacyjne i bezpieczeństwa”.

7.3.2 Ochrona danych aktywujących klucze

Za ochronę danych aktywujących klucze odpowiedzialna jest osoba uprawniona do posługiwania się tymi danymi.

7.4 Zarządzanie bezpieczeństwem komputerów

7.4.1 Specyfikacja wymagań technicznych na bezpieczeństwo komputerów

Sigillum PCCE opracowało i wdrożyło dokument „Bezpieczeństwo techniczne i środowiskowe”, zawierający wymagania na bezpieczeństwo komputerów specyficzne dla działalności Sigillum PCCE.

7.5 Zarządzanie cyklem życia elementów technicznch

7.5.1 Zarządzanie rozwojem systemu

Aplikacje Sigillum PCCE są tworzone w kontrolowanym środowisku stosującym odpowiednie procedury zarządzania jakością.

7.5.2 Kontrola bezpieczeństwa zarządzania

Bezpieczeństwo zarządzania systemem jest kontrolowane poprzez system uprawnień zapewnianych przez system operacyjny oraz poprzez system ról pełnionych przez personel, opisany w rozdziale 6.2.1.

7.6 Zarządzanie bezpieczeństwem sieciowym

Sigillum PCCE opracowało i wdrożyło system oceny ryzyka działalności, który określa wszystkie znaczące zagrożenia wiążące się z bezpieczeństwem sieciowym. Procedury operacyjne przez Sigillum PCCE uwzględniają występowanie zidentyfikowanych obszarów ryzyka.

8 Profil znacznika czasu i żądania znacznika czasu

8.1.1 Profil nieuwierzytelnionego żądania znacznika czasu (na podstawie RFC 3161)

Pole	Opis/wartość
version	„1”.
messageImprint	Skrót z wiadomości, która ma zostać oznaczona czasem.
hashAlgorithm	Identyfikator OID algorytmu skrótu SHA-1: { iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26 }
hashedMessage	Ciąg bajtów reprezentujący skrót z wiadomości.
reqPolicy	Pole opcjonalne, jeśli występuje oznacza żądanie wystawienia znacznika czasu zgodnie z podaną polityką. Jeśli pole występuje – powinno zawierać identyfikator „{ 2 5 29 32 0}” (any policy) lub identyfikator polityki (OID) {1 2 616 1 113560 10 2 1 0}
nonce	Liczba generowana przez klienta. Pole opcjonalne.
certReq	Pole opcjonalne o wartości “1” lub „0”. Jeśli występuje i jest równe „1”, oznacza, że serwer powinien do odpowiedzi dołączyć zaświadczenie certyfikacyjne służące do weryfikacji znacznika.
extensions	Rozszerzenia wg RFC 3161. Pole nie może wystąpić. Jeśli wystąpi – żądanie jest przez serwer odrzucane.

Możliwość zastosowania nieuwierzytelnionego żądania znacznika czasu, zgodnego z profilem powyżej, może być dopuszczona dla wybranych grup klientów, identyfikowanych innymi sposobami (w szczególności dla wewnętrznych podmiotów systemu Sigillum PCCE).

Dla pozostałych subskrybentów obowiązuje *Profil uwierzytelnionego żądania znacznika czasu*.

8.1.2 Profil uwierzytelnionego żądania znacznika czasu

Pole	Opis/wartość
version	„1”
digestAlgorithms	Lista identyfikatorów algorytmów skrótu. Lista powinna zawierać algorytm użyty do stworzenia skrótu z podpisywanego żądania znacznika czasu.
contentInfo	Pole zawiera właściwe żądanie znacznika czasu
contentType	Identyfikator OID id-signedData { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 2 }
content	Zakodowane w ASN1 (DER) nieuwierzytelnione żądanie znacznika czasu – zgodne z profilem określonym w rozdziale 8.1.1
certificates	Lista certyfikatów. Lista powinna zawierać certyfikat (X509v3) klucza, którym zostało podpisane żądanie oznaczenia czasem (i tylko ten certyfikat)
crls	Lista list CRL. Lista może być pusta - nie jest przetwarzana przez serwer znacznika czasu (listy CRL pobierane są z innego źródła).
signerInfos	Lista podpisów Lista musi zawierać dokładnie jeden podpis
version	„1”
singerIdentifier	Informacje o certyfikacie osoby podpisującej żądanie
issuerAndSerialNumber	
issuer	Identyfikator wyróżniający (DN) wystawcy certyfikatu

serialNumber	Numer seryjny certyfikatu
digestAlgorithm	Identyfikator OID algorytmu skrótu SHA-1: { iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26 }
signedAttrs	Pole opcjonalne. Jego zawartość nie jest przetwarzana przez serwer znacznika czasu.
signatureAlgorithm	Algorytm podpisu: SHA1WithRSAEncryption { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 5 }
signature	Wartość podpisu.
unsignedAttrs	Pole opcjonalne. Jego zawartość nie jest przetwarzana przez serwer znacznika czasu.

8.1.3 Profil odpowiedzi serwera znacznika czasu

Pole	Opis/wartość
status	Informacje o stanie przetworzenia żądania wystawienia znacznika czasu.
status	Pole przyjmuje jedną z następujących wartości: 0, 2, 3, 4. Jeśli pole jest równe 0, to oznacza, że znacznik został poprawnie wystawiony. Każda inna wartość z powyżej wymienionych oznacza niewystawienie znacznika (zgodnie z RFC 3161).
statusString	Tekstowy opis przyczyn odrzucenia żądania wystawienia znacznika czasu.
failInfo	Powód odrzucenia żądania wystawienia znacznika czasu - jeden z poniższych kodów liczbowych (zgodnie z RFC 3161): 0, 2, 5, 14, 15, 16, 17, 25.
timeStampToken	

contentType	id-signedData { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 2 }
content	
version	„1”
digestAlgorithms	Lista identyfikatorów algorytmów skrótu. Lista zawiera identyfikator SHA-1 { iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26 }
contentInfo	
contentType	id-ct-TSTInfo { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 4}
content	Zakodowana wartość znacznika czasu.
version	„1”
policy	Identyfikator polityki wystawiania znaczników czasu przez Sigillum PCCE identyfikator polityki (OID) {1 2 616 1 113560 10 2 1 0}
messageImprint	Skrót z wiadomości oznaczanej czasem.
hashAlgorithm	Identyfikator OID algorytmu funkcji skrótu: SHA-1 { iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26 }
hashedMessage	Ciąg bajtów reprezentujący skrót z wiadomości.
serialNumber	20 bajtowy numer seryjny znacznika czasu.
genTime	Czas UTC w którym został utworzony znacznik czasu.
accuracy	Dokładność z jaką wyznaczono wartość GenTime.

seconds	„1”
nonce	Wartość Nonce przepisana z żądania znacznika czasu (jeśli wystąpi)
certificates	Lista certyfikatów. Jeśli w żądaniu wartość CertReq była równa „1”, to pole to zawiera zaświadczenie certyfikacyjne Sigillum PCCE służące do weryfikacji znacznika czasu.
crls	Pusta lista CRL.
signerInfos	Lista podpisów. Zawiera poświadczenie elektroniczne Sigillum PCCE.
version	„1”
singerIdentifier	Informacje o zaświadczeniu certyfikacyjnym Sigillum PCCE, wystawionym przez ministra właściwego ds. gospodarki lub podmiot przez niego upoważniony
issuerAndSerialNumber	
issuer	Identyfikator wyróżniający (DN) wystawcy zaświadczenia certyfikacyjnego Sigillum PCCE
serialNumber	Numer seryjny zaświadczenia certyfikacyjnego Sigillum PCCE
digestAlgorithm	Identyfikator OID algorytmu skrótu: SHA-1 { iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26 }
signedAttrs	Zbiór podpisanych atrybutów zawierający: 1) Skrót z zaświadczenia certyfikacyjnego Sigillum PCCE 2) Skrót ze znacznika czasu
signatureAlgorithm	Algorytm poświadczenia elektronicznego: SHA1WithRSAEncryption { iso(1) member-body(2) us(840)

	rsadsi(113549) pkcs(1) 1 5 }
signature	Wartość poświadczenia elektronicznego pola signedAttrs (w tym znacznika czasu).
unsignedAttrs	Pusty zbiór atrybutów.

9 Zarządzanie politykami i regulaminem certyfikacji

PWPW S.A. ustanawia Radę Zatwierdzania Polityk Certyfikacji, która jest zobowiązana do zarządzania politykami i regulaminami certyfikacji w ramach struktury Sigillum PCCE.

O każdej zmianie polityki lub regulaminu niezwłocznie powiadamiany jest minister właściwy do spraw gospodarki nie później niż w ciągu 7 dni od daty zatwierdzenia zmian.

Aktualna wersja polityk i regulaminów jak również wszystkie wersje obowiązujące wcześniej są publikowane w repozytorium.

Wszystkie dokumenty związane ze świadczeniem usług certyfikacyjnych przechowywane są przez PWPW S.A. zgodnie z wewnętrznymi procedurami bezpieczeństwa.

10 Załącznik A: Polityki certyfikacji wspierane przez niniejszy regulamin certyfikacji

Niniejszy regulamin wspiera zastosowanie „Polityki PCCE dla kwalifikowanych znaczników czasu”.