PWPW
POLSKA WYTWÓRNIA
PAPIERÓW WARTOŚCIOWYCH

POLITYKA ŚWIADCZENIA USŁUG NIEKWALIFIKOWANYCH CUZ SIGILLUM

Data: 15.04.2025

Status: Aktualna

PWPW S.A.

Wer. 1.5

Spis treści

1. Wstęp

1.1. Słownik pojęć

1) Algorytm RSA – algorytm kryptograficzny określony jednoznacznie przez identyfikator obiektu „{ joint-iso-ccitt(2) ds(5) module(1) algorithm(8) encryptionAlgorithm(1) 1 }”.
2) Algorytm ECDSA – algorytm kryptograficzny służący do realizacji sygnatury z dostarczonych danych. Grupa algorytmów wykorzystujących ECDSA, realizowanych w oparciu o różne funkcje skrótu jest określona przez identyfikator {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4)}
3) Bezpieczne urządzenia do składania podpisu, których zgodność ustalono zgodnie z art. 3 ust. 4 dyrektywy 1999/93/WE, uznaje się za kwalifikowane urządzenia do składania podpisu elektronicznego na mocy Rozporządzenia eIDAS.
4) Certyfikat dostawcy usług zaufania – certyfikat służący do weryfikacji zaawansowanych podpisów elektronicznych lub pieczęci elektronicznych, o których mowa w Załączniku I lit. g, Załączniku III lit. g, Załączniku IV lit. h do Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej nr 910/2014 z dnia 23 lipca 2014r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE oraz certyfikatów służących do weryfikacji innych usług zaufania świadczonych przez kwalifikowanych dostawców usług zaufania.
5) Centrum Usług Zaufania Sigillum – wydzielone organizacyjnie centrum certyfikacji elektronicznej działające w ramach struktur Polskiej Wytwórni Papierów Wartościowych S.A., zwanej dalej „PWPW S.A.” świadczące usługi certyfikacyjne w zakresie objętym niniejszą Polityką, zwane dalej ,,CUZ Sigillum”.
6) Certyfikat klucza publicznego – certyfikat klucza weryfikującego podpis.
7) 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.
8) Certyfikat serwerowy - Niekwalifikowany certyfikat obiektowy służący do uwierzytelnienia oraz zapewnienia poufności w komunikacji z serwerem.
9) Dostawca usług zaufania – oznacza osobę fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania.
10) Identyfikator semantyczny - w kontekście certyfikatów kwalifikowanych odnosi się do unikalnego identyfikatora, który jest przypisany do certyfikatu w celu jednoznacznego określenia jego właściciela oraz powiązanych z nim danych. Jest to kluczowy element w procesie weryfikacji

tożsamości i autentyczności certyfikatu, co zapewnia bezpieczeństwo i zaufanie w transakcjach elektronicznych. Semantyczny identyfikator w certyfikatach kwalifikowanych pomaga w jednoznacznym określeniu tożsamości właściciela certyfikatu poprzez przypisanie znaczenia do określonych danych, na przykład takich jakich niesie w sobie PESEL.

11) Identyfikator niesemantyczny - to unikalny znacznik przypisywany obiektowi, który nie zawiera informacji o znaczeniu lub kontekście tego obiektu. W przeciwieństwie do identyfikatorów semantycznych, które mają przypisane konkretne znaczenie i pomagają w jednoznacznym określeniu tożsamości lub funkcji obiektu, identyfikatory niesemantyczne są zwykle ciągami znaków lub liczb, które służą jedynie do odróżnienia jednego obiektu od innych. Przykładem identyfikatora niesemantycznego może być losowo wygenerowany numer identyfikacyjny przypisany do użytkownika w bazie danych, który nie niesie żadnej dodatkowej informacji o tym użytkowniku. W dalszej części dokumentu dla tego identyfikatora używana będzie nazwa identyfikator własny. Identyfikator niesemantyczny wydawany jest tylko dla certyfikatów zawierających jednocześnie informacje o Organizacji.
12) Klucz – liczba, symbol, ciąg liczb lub symboli jednoznacznie wyznaczający przekształcenie kryptograficzne spośród rodziny przekształceń zdefiniowanej przez algorytm kryptograficzny.
13) Klucz podpisujący – klucz prywatny służący do składania podpisu elektronicznego; klucz podpisujący zawiera dane służące do składania podpisu elektronicznego w rozumieniu Ustawy.
14) Klucz weryfikujący podpis – klucz publiczny służący do weryfikowania podpisu elektronicznego; klucz weryfikujący podpis zawiera dane służące do weryfikacji podpisu elektronicznego lub dane służące do weryfikacji poświadczenia elektronicznego w rozumieniu Ustawy.
15) Klucze infrastruktury – klucze kryptograficzne algorytmów kryptograficznych stosowane do innych celów niż składanie lub weryfikacja bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego, a w szczególności klucze stosowane:
16) do weryfikacji dostępu do urządzeń, oprogramowania weryfikującego lub podpisującego,
17) do zapewnienia podczas transmisji lub przechowywania poufności i integralności zgłoszeń certyfikacyjnych, kluczy użytkowników, rejestrów zdarzeń,
18) w protokołach uzgadniania lub dystrybucji kluczy zapewniających poufność danych.
19) Komponent techniczny – sprzęt stosowany w celu wygenerowania lub użycia danych służących do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego.
20) Kwalifikowane urządzenie do składania podpisu elektronicznego – oznacza urządzenie do składania podpisu elektronicznego, które spełnia wymogi określone w załączniku II Rozporządzenia eiDAS.
21) Kwalifikowane urządzenie do składania pieczęci elektronicznej – oznacza urządzenie do składania pieczęci elektronicznej, które spełnia odpowiednio wymogi określone w załączniku II Rozporządzenia eIDAS.

22) Kwalifikowane usługi certyfikacyjne – usługi certyfikacyjne świadczone przez podmiot posiadający wpis w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne, zgodnie z Polityką odpowiadającą temu wpisowi.
23) Kwalifikowany certyfikat pieczęci elektronicznej – certyfikat pieczęci elektronicznej, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku III do Rozporządzenia nr 910/2014.
24) Kwalifikowany certyfikat podpisu elektronicznego – certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I do Rozporządzenia nr 910/2014.
25) Kwalifikowany elektroniczny znacznik czasu – oznacza elektroniczny znacznik czasu, który spełnia wymogi określone w art. 42 Rozporządzenia.
26) Lista ARL – lista unieważnionych zaświadczeń certyfikacyjnych wystawionych przez dany podmiot świadczący usługi certyfikacyjne, który poświadcza ją w postaci elektronicznej. Podmiot nie musi wystawiać listy ARL, jeśli informacje o unieważnionych zaświadczeniach certyfikacyjnych zawiera już w wystawianej przez siebie liście CRL.
27) 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.
28) Moduł kluczowy – urządzenie współpracujące z komponentem technicznym, przechowujące klucze infrastruktury; dane służące do składania kwalifikowanych podpisów elektronicznych; poświadczeń elektronicznych; klucze chroniące te dane; przechowujące części tych kluczy lub danych.
29) Najwyższa wartość graniczna transakcji – wartość kwotowa określająca ograniczenie najwyższej wartości transakcji, w której Certyfikat może być wykorzystywany, która jest określona przez Zamawiającego/Subskrybenta.
30) Para kluczy algorytmu RSA – dwa klucze (klucz prywatny i klucz publiczny) wyznaczające wzajemnie odwrotne przekształcenia spośród rodziny przekształceń zdefiniowanej przez algorytm RSA.
31) Para kluczy algorytmu EC – dwa klucze (klucz prywatny i klucz publiczny) wyznaczające wzajemnie odwrotne przekształcenia spośród rodziny przekształceń zdefiniowanej przez krzywą np. NIST P-384
32) PKI – Infrastruktura Klucza Publicznego.
33) Polityka – niniejsza polityka usług zaufania CUZ Sigillum.
34) 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: są sporządzone za pomocą podlegających wyłącznej kontroli

podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania poświadczenia elektronicznego; jakakolwiek zmiana danych poświadczonych jest rozpoznawalna.

35) Punkt Rejestracji – jednostka organizacyjna CUZ Sigillum lub inna jednostka organizacyjna działająca w jej imieniu, wykonująca zgodnie z Polityką niektóre funkcje związane ze świadczeniem usług certyfikacyjnych.
36) Punkt zaufania – patrz „Ścieżka certyfikacji klucza weryfikującego podpis".
37) Rada Zatwierdzania Polityk Certyfikacji PWPW S.A. – organ odpowiedzialny za zatwierdzanie Polityk Certyfikacji, zwanym dalej RZPC PWPW S.A.
38) RODO - art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Rozporządzenie 2016/679).
39) Rozporządzenie Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie krajowej infrastruktury zaufania (Dz. U. 2016 poz. 1632), zwane dalej „Rozporządzenie MC".
40) Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, zwane dalej „Rozporządzenie eIDAS".
41) Strona ufająca – osoba fizyczna, prawna lub jednostka organizacyjna nie posiadająca 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 Polityką certyfikat lub zaświadczenie certyfikacyjne.
42) Subskrybent – osoba fizyczna lub prawna, która zawarła z PWPW S.A. umowę o świadczenie usług certyfikacyjnych.
43) Ścieżka certyfikacji klucza weryfikującego podpis - uporządkowany ciąg zaświadczeń certyfikacyjnych lub zaświadczeń certyfikacyjnych i kwalifikowanego 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".

44) System Sigillum (zwany dalej systemem informatycznym) – zespół wzajemnie działających elementów w ramach infrastruktury CUZ Sigillum, w którym zachodzą procesy technologiczne mające na celu przetwarzanie danych w ramach świadczenia usług zaufania.
45) TTP (ang. Trusted Third Party) - patrz: Zaufana Trzecia Strona
46) Usługi certyfikacyjne - szeroka klasa usług dotyczących TTP obejmująca działania polegające na poświadczeniu wybranych informacji przez wygenerowanie podpisanego elektronicznie zaświadczenia certyfikacyjnego, jak certyfikacja kluczy publicznych, certyfikacja istnienia danych elektronicznych w określonym czasie, certyfikacja przedstawienia danych elektronicznych przez określonych użytkowników w określonym czasie.
47) Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej. (Dz. U. 2016 Poz. 1579), zwaną dalej „Ustawa".
48) QSCD - Qualified Signature Creation Device (kwalifikowane urządzenie do składania podpisu elektronicznego) – urządzenie do składania podpisu elektronicznego lub pieczęci elektronicznej, które a) znajduje się na liście, o której mowa w art. 31.2 eIDAS.
49) Zamawiający – osoba prawna lub jednostka organizacyjna nie posiadająca osobowości prawnej, która może finansować usługi certyfikacyjne świadczone na rzecz danego Subskrybenta. Dane Zamawiającego mogą być umieszczone w certyfikacie Subskrybenta. Zamawiający posiada prawo do unieważniania certyfikatu Subskrybenta (art. 21 ust. 2 pkt. 5 Ustawy).
50) 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.
51) Zaufana Trzecia Strona (ang. Trusted Third Party (TTP)) - logiczna strona w modelu PKI posługująca się mechanizmem podpisu elektronicznego i certyfikatu do poświadczania określonej treści, darzona zaufaniem przez pozostałe strony w tym modelu;
52) Zgłoszenie certyfikacyjne - plik w formacie PKCS#10 zawierający między innymi nazwę wyróżniającą Subskrybenta oraz klucz publiczny. Określenia wykorzystywane w Polityce, a niezdefiniowane powyżej należy interpretować zgodnie z definicjami zawartymi w Ustawie i Rozporządzeniu.

1.2. Wprowadzenie

Niniejszy dokument stanowi Politykę certyfikacji PWPW S.A. usług niekwalifikowanych, dla utworzonego w ramach struktur organizacyjnych PWPW S.A. centrum certyfikacji elektronicznej o nazwie Centrum Usług Zaufania „Sigillum" zwane w dalszej części dokumentu CUZ Sigillum, w zakresie świadczenia niekwalifikowanej usługi zaufania polegającej na wystawianiu

niekwalifikowanych certyfikatów podpisu, niekwalifikowanych certyfikatów pieczęci oraz niekwalifikowanych certyfikatów serwerowych (TLS)

CUZ Sigillum w zakresie wydawania certyfikatów niekwalifikowanych zostało zaprojektowane i wdrożone w taki sposób, aby spełnić wymagania nałożone przez krajową Ustawę o Usługach Zaufania i stosowne rozporządzenia, a także wymagania innych, obowiązujących norm prawnych oraz istniejących standardów międzynarodowych w zakresie tworzenia i funkcjonowania systemów PKI, w szczególności z uwzględnieniem zaleceń zawartych w RFC 3647 "Certificate Policy and Certification Practices Framework". Polityka stanowi własność intelektualną PWPW S.A.

We wszystkich aspektach, w których jest to możliwe, świadczenie niekwalifikowanych usług certyfikacyjnych przez CUZ Sigillum podlega podobnym 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, nieobejmowanych ustawową definicją kwalifikowanych certyfikatów. W szczególności mechanizmy i procedury stosowane w celu ochrony klucza prywatnego CUZ Sigillum służącego do wystawiania certyfikatów zgodnie z niniejszą polityką, jak również procedury weryfikacji tożsamości potencjalnego subskrybenta – osoby fizycznej, spełniają wymogi Ustawy.

Aby zapewnić jak najlepszy dostęp do swoich usług osobom niepełnosprawnym CUZ Sigillum oferuje wsparcie techniczne poprzez infolinię, pod numerem +48 22 464-79-79 oraz dojazd i pomoc Inspektora PR w miejsce wskazane przez Klienta po wcześniejszym ustaleniu warunków i terminu.

1.3. Nazwa dokumentu i jego identyfikacja

Identyfikator niniejszego dokumentu Polityki świadczenia usług zaufania.

Nazwa Polityki	POLITYKA ŚWIADCZENIA USŁUG NIEKWALIFIKOWANYCH CUZ SIGILLUM
Wersja Polityki	1.5
Status wersji	Aktualna
Numer referencyjny/OID (ang. Object Identifier)	{iso(1)member-body(2) PL(616) organisation(1) pwpw(113725) id-sigillum(0)id-qtso(1)id-qtsp-doc(0)id-qtsp-doc-version(1)0}
Data wprowadzenia w życie	15.04.2025
Data wygaśnięcia	Do odwołania

Niniejszy dokument Polityki Świadczenia Usług Zaufania jest zbiorem polityk i regulaminów stosowanych przez CUZ Sigillum przy wydawaniu certyfikatów niekwalifikowanych. Każdy niekwalifikowany certyfikat, wydany przez CUZ Sigillum zawiera identyfikator Polityki Certyfikacji zastosowanej do wydania tego certyfikatu.

CUZ Sigillum w wydawanych certyfikatach niekwalifikowanych stosuje własne identyfikatory OID:

- 1.2.616.1.113725.0.1 – CUZ SIGILLUM,
- 1.2.616.1.113725.0.1.0.1.0 - POLITYKA ŚWIADCZENIA USŁUG NIEKWALIFIKOWANYCH CUZ SIGILLUM,
- 1.2.616.1.113725.0.1.1 – Niekwalifikowane certyfikaty podpisu
- 1.2.616.1.113725.0.1.2 – Niekwalifikowany certyfikat pieczęci
- 1.2.616.1.113725.0.1.3 - Niekwalifikowane certyfikaty obiektowe służące do uwierzytelnienia oraz zapewnienia poufności w komunikacji z serwerem tzw. certyfikaty serwerowe (TLS)

1.4. Uczestnicy PKI

W skład systemu PKI obsługiwanego przez CUZ Sigillum, który realizuje swoje usługi na podstawie wpisu do Rejestru Niekwalifikowanych Dostawców Usług Zaufania, wchodzą:

- Urząd certyfikacji;

- Urzędy weryfikacji statusu certyfikatu;
- Punkty rejestracji.

Hierarchia PKI przedstawia się następująco:

Poziom	Parametr	Wartość
Level1 – Root CA	Nazwa DN	CN=CUZ Sigillum Root CA1 O=Polska Wytwórnia Papierów Wartościowych S.A. OU=Centrum Usług Zaufania Sigillum C=PL
	Numer seryjny	2f f5 22 54 e6 15 2f 1c
	Identyfikator klucza	ef 38 00 05 cb 0d 30 68 7e 06 ef dd 47 a1 3b 31 c3 03 54 e8
	Odcisk palca [SHA-1]	a6 cf ac d3 76 e6 09 89 72 4f eb fc a0 bb db fb 17 5a 68 c6
Level2 – Sub CA	Nazwa DN	CN=CUZ Sigillum CA1 O=Polska Wytwórnia Papierów Wartościowych S.A. OU=Centrum Usług Zaufania Sigillum C=PL
	Numer seryjny	30 7b 9d 7a 22 1c e6 97
	Identyfikator klucza	51 35 36 24 16 7a 36 ce fb 76 e0 81 94 64 c8 2e ce d8 de 91
	Odcisk palca [SHA-1]	Cf 2d 07 40 52 07 47 ed e3 db a7 a8 23 b0 19 48 22 1d 1d d0
Level3 – OCSP	Nazwa DN	CN=CUZ Sigillum CA1 OCSP O=Polska Wytwórnia Papierów Wartościowych S.A. OU=Centrum Usług Zaufania Sigillum C=PL
	Numer seryjny	60 c2 7a 48 37 b4 1c 6d
	Identyfikator klucza	e327af89efb05395b662cf0de9b5121d9dcab0c0
	Odcisk palca [SHA-1]	9a421c2f5db67bccfa090a962650a6b35fa7f4c9

Level2 - OCSP	Nazwa DN	CN=CUZ Sigillum Root CA1 OCSP O=Polska Wytwórnia Papierów Wartościowych S.A. OU=Centrum Usług Zaufania Sigillum C=PL
	Numer seryjny	66 a8 6a 29 70 49 e8 72
	Identyfikator klucza	1decc8cef2d14f1e8d592189bbcc8e97bf58a794
	Odcisk palca [SHA-1]	6e814093c5a2b63ea7c356d8842433e427f4dbe7

1.5. Urząd certyfikacji

W ramach Niekwalifikowanego Urzędu Certyfikacji CUZ Sigillum działa jeden urząd nadrzędny RootCA oraz jeden urząd wydający certyfikaty niekwalifikowane:

- CUZ Sigillum CA1 – urząd certyfikacji wydający niekwalifikowane elektroniczne certyfikaty do podpisu, pieczęci oraz serwerowe o strukturze zgodnej z normą X.509 oraz normami ETSI dotyczącymi struktury certyfikatów

Urzędy te działają zgodnie z wymaganiami:

- Ustawy o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz.U.2016r., poz. 1579).
- Normy ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

Urząd ten wydaje certyfikaty podpisu elektronicznego dla osób fizycznych, osób prawnych, certyfikaty serwerowe oraz certyfikaty na potrzeby weryfikacji statusu wydanych certyfikatów (certyfikat usługi OCSP).

1.5.1.Punkty rejestracji

Urząd Certyfikacji CUZ Sigillum współpracuje z Punktami Rejestracji (PR). Reprezentują one urzędy certyfikacji w kontaktach z subskrybentami i posiadają uprawnienia oddelegowane im przez urząd certyfikacji w zakresie potwierdzenia tożsamości podczas rejestracji aktualnego lub przyszłego subskrybenta. CUZ Sigillum ma możliwość potwierdzenia tożsamości osoby ubiegającej się o certyfikat bez jej osobistego stawiennictwa w puncie rejestracji, na podstawie notarialnego potwierdzenia tożsamości. CUZ Sigillum może również wyznaczyć inne osoby potwierdzające w jego imieniu tożsamość

wnioskodawcy oraz uprawnione do przyjmowania wniosków i zawierania umów na świadczenie usług certyfikacyjnych.

Zadania Punktu rejestracji są zapisane:

1) w regulaminie Punktu rejestracji, stanowiącym wewnętrzny dokument CUZ Sigillum jeśli Punkt rejestracji jest jednostką organizacyjną PWPW S.A. lub

2) w umowie pomiędzy PWPW S.A. a podmiotem prowadzącym Punkt rejestracji.

Aktualna lista PR przedstawiona jest na stronie internetowej CUZ Sigillum pod adresem:

https://sigillum.pl

1.6. Obowiązki stron

1.6.1. Obowiązki Subskrybenta

Przed złożeniem wniosku o certyfikat klucza publicznego i podpisaniem umowy o świadczenie usług zaufania, Subskrybent jest zobowiązany do zapoznania się z treścią Polityki oraz Zasadami i warunkami świadczenia usług.

Jeśli Subskrybent posługuje się certyfikatami wystawionymi zgodnie z Polityką, w celu weryfikacji podpisu, oznacza to, że występuje w roli Strony ufającej.

Subskrybent ma obowiązek zachowania poufności kluczy prywatnych związanych z certyfikatami kluczy publicznych wystawionymi zgodnie z Polityką. Subskrybent ponosi pełną odpowiedzialność za bezpieczne przechowywanie swojego klucza prywatnego. W przypadku, gdy klucze przechowywane są w komponentach technicznych lub modułach kluczowych zabezpieczonych hasłami lub kodami PIN, Subskrybent ma obowiązek bezpiecznego przechowywania hasła lub kodu PIN, rozdzielnie z wykorzystywanym komponentem technicznym lub modułem kluczowym.

Subskrybent ma obowiązek zachowania poufności danych uwierzytelniających do swojego indywidulanego konta w systemie Sigillum.

W przypadku utraty klucza prywatnego związanego z certyfikatem klucza publicznego wydanym w ramach Polityki oraz w przypadku ujawnienia tego klucza lub uzasadnionego podejrzenia, że ujawnienie takie mogło nastąpić – Subskrybent jest zobowiązany do niezwłocznego zgłoszenia CUZ Sigillum faktu wystąpienia takiego zdarzenia w celu zawieszenia lub unieważnienia certyfikatów kluczy publicznych związanych z utraconymi lub ujawnionymi kluczami.

Subskrybent jest zobowiązany do podania w umowie o świadczenie usług zaufania i w zgłoszeniu certyfikacyjnym prawdziwych i kompletnych danych w zakresie wymaganych odpowiednio przez umowę lub zgłoszenie certyfikacyjne.

W przypadku wniosku Zamawiającego o zamieszczenie w certyfikacie klucza publicznego Subskrybenta danych Zamawiającego, określa on swoją wolę w stosownym formularzu CUZ Sigillum.

Po otrzymaniu certyfikatu klucza publicznego 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 do CUZ Sigillum celem unieważnienia certyfikatu klucza publicznego i wygenerowania nowego certyfikatu klucza publicznego z prawidłowymi danymi.

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

Subskrybent jest zobowiązany do ponoszenia kosztów świadczenia usług zaufania według cennika obowiązującego w CUZ Sigillum w dniu podpisania umowy o świadczenie usług zaufania – jeśli kosztów tych nie ponosi Zamawiający lub CUZ Sigillum nie jest w stanie uzyskać tych kosztów od Zamawiającego.

1.6.2. Obowiązki Zamawiającego

Zamawiający jest zobowiązany do wyznaczenia odpowiednio umocowanego przedstawiciela/przedstawicieli, odpowiedzialnych za nadzór nad prawidłowością procesu przyznawania i odbierania uprawnień do posługiwania się danymi Zamawiającego w certyfikatach kluczy publicznych wydawanych zgodnie z Polityką.

Zamawiający wydaję pisemną zgodę na umieszczenie danych Zamawiającego w certyfikacie klucza publicznego, wydanego zgodnie z Polityką, poprzez zawarcie z CUZ Sigillum umowy o świadczenie usług zaufania.

Przed wydaniem zgody na umieszczenie danych Zamawiającego w certyfikacie klucza publicznego, przedstawiciel Zamawiającego zobowiązany jest do zapoznania się z Polityką oraz Zasadami i warunkami świadczenia usług, i zaakceptowania zawartych tam postanowień.

W przypadku zmiany danych Zamawiającego zapisanych w certyfikacie klucza publicznego dotyczących Zamawiającego Subskrybent jest zobowiązany do niezwłocznego zgłoszenia tego

faktu do CUZ Sigillum w celu unieważnienia certyfikatu klucza publicznego i ewentualnie wystawienia nowego, zawierającego poprawne dane.

Zamawiający jest zobowiązany do ponoszenia kosztów świadczenia usług zaufania według cennika obowiązującego w CUZ Sigillum, a w dniu podpisania umowy o świadczenie usług zaufania – jeśli zawarł w niej zobowiązanie do poniesienia tych kosztów.

Zamawiający i PWPW S.A. muszą być niezależnymi podmiotami, z wyjątkiem sytuacji, w której PWPW S.A. wystawia certyfikaty niekwalifikowane dla swoich pracowników.

1.6.3. Obowiązki Strony Ufającej

Przy weryfikowaniu ważności podpisu elektronicznego, ważność bada się na podstawie zaświadczenia certyfikacyjnego wystawionego dla urzędu CUZ Sigillum CA1 przez samo podpisany urząd główny CUZ Sigillum Root CA1.

Klucz publiczny stanowiący Punkt zaufania musi być pobrany w sposób zapewniający jego autentyczność i integralność (np. bezpośrednio od właściciela tego klucza lub działającego w jego imieniu Punktu rejestracji lub według procedury zapewniającej weryfikację skrótu kryptograficznego z klucza publicznego).

Strona ufająca ma obowiązek ochrony integralności klucza publicznego stanowiącego Punkt zaufania. W przypadku jakiejkolwiek wątpliwości, co do integralności i autentyczności klucza publicznego, Strona ufająca ma obowiązek ją potwierdzić, na przykład poprzez porównanie kryptograficznego skrótu z posiadanego klucza publicznego ze skrótem klucza publicznego certyfikatu urzędu, dostępnego w repozytorium CUZ Sigillum.

1.7. Zakres stosowania certyfikatów

W ramach Polityki CUZ Sigillum wystawia dla Subskrybentów osobiste certyfikaty niekwalifikowane, które mogą być wykorzystywane do:

- Szyfrowania i podpisywania dokumentów,
- Szyfrowania i podpisywania poczty elektronicznej,
- Uwierzytelniania klienta w protokole SSL/TLS,
- Logowania w usłudze SmartCard Logon.
- Do zapewnienia bezpiecznej komunikacji pomiędzy serwerami

Certyfikaty wystawione zgodnie z niniejszą Polityką mogą być stosowane wyłącznie z aplikacjami, które spełniają następujące wymaganie:

- prawidłowo zarządzają kluczami publicznymi i prywatnymi, ich przesyłaniem oraz używaniem,
- certyfikaty oraz związane z nimi klucze prywatne używają zgodnie z ich deklarowanym przeznaczeniem,
- posiadają wbudowane mechanizmy weryfikacji statusu certyfikatu, budowania ścieżek certyfikacji oraz sprawdzania jego ważności (ważności podpisu, okresu ważności, itp.),
- przekazują użytkownikowi prawidłowe informacje o stanie aplikacji, certyfikatów, itp.

1.7.1. Nierekomendowane zastosowanie certyfikatów

Zabrania się używania certyfikatów wystawionych przez CUZ Sigillum niezgodnie z ich deklarowanym przeznaczeniem oraz w aplikacjach niespełniających wymagań określonych w punkcie 1.6. W szczególności certyfikaty niekwalifikowane wystawione z urzędu CUZ Sigillum CA1 nie mogą być używane jako certyfikaty urzędów certyfikacji.

1.8. Struktura organizacyjna

Centrum Usług Zaufania Sigillum jest to wydzielone organizacyjnie centrum certyfikacji elektronicznej działające w ramach struktur PWPW S.A.

W ramach usług CUZ Sigillum zarząd PWPW S.A. powołał zespół odpowiedzialny za:

- Obsługę systemu,
- Administrowanie systemem,
- Bezpieczeństwo systemu.

Osobą odpowiedzialną za koordynowanie prac zespołu jest Kierownik CUZ Sigillum, który wchodzi również w skład Rady Zatwierdzania Polityk Certyfikacji PWPW S.A. powoływanej przez Zarząd PWPW S.A.

1.9. Dane kontaktowe i rejestrowe

Dane kontaktowe:

Polska Wytwórnia Papierów Wartościowych S.A.

Centrum Usług Zaufania Sigillum

00-222 Warszawa, ul. Sanguszki 1

e-mail: sigillum@pwpw.pl

tel.: (+48) 22 464 79 79

www.sigillum.pl

Dane rejestrowe:

NIP: 525-000-10-90

KRS: 0000062594

Sąd Rejonowy dla m. st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego.

2. Publikowanie i repozytorium

2.1. Repozytorium

W ramach swoich obowiązków CUZ Sigillum prowadzi repozytorium dostępne dla odbiorców usług zaufania.

Repozytorium jest dostępne w sieci Internet za pomocą protokołów LDAP, OCSP via http oraz WWW. W celu zapewnienia wysokiej dostępności usług CUZ Sigillum posiada dwa łącza internetowe od niezależnych dostawców.

Protokołem OCSP na żądanie Strony ufającej udostępniana będzie informacja o statusie certyfikatu. Statusy certyfikatów w aktualnej liście CRL będą w pełni zgodne ze statusami zwracanymi przez usługę OCSP z uwzględnieniem czasu potrzebnego na wygenerowanie i publikację list CRL.

Repozytorium jest dostępne całą dobę, przez wszystkie dni w roku. Ewentualny czas niedostępności repozytorium nie może każdorazowo przekroczyć 2 godzin, zaś minimalna dostępność w skali miesiąca to 99% czasu.

2.2. Publikowanie w postaci elektronicznej

Polityki są publikowane elektronicznie w postaci plików w formacie PDF na stronie internetowej sigillum.pl

W postaci elektronicznej publikowane są następujące dokumenty:

a) Wszystkie wersje Polityki, z podaniem okresu ich obowiązywania,
b) Certyfikaty podpisów elektronicznych klucza publicznego:

i. Urzędu CUZ Sigillum służący do weryfikacji certyfikatów kluczy publicznych wystawionych zgodnie z Polityką,
ii. Pieczęci elektronicznej usługi OCSP,
iii. Użytkowników końcowych wystawione zgodnie z Polityką, o ile Subskrybent, którego dane są umieszczone w certyfikacie wyraził na to zgodę.
iv. Aktualną listę unieważnionych certyfikatów kluczy publicznych i zaświadczeń certyfikacyjnych (CRL), wystawioną zgodnie z Polityką,
v. Cennik.

2.3. Częstotliwość publikacji

Lista unieważnionych certyfikatów jest generowana i publikowana nie rzadziej niż co 24 godziny, niezależnie od tego, czy wystąpiły unieważnienia lub zawieszenia.
W przypadku, gdy od wygenerowania ostatniej listy CRL wystąpiło unieważnienie certyfikatu lub zawieszenie lub też uchylenie zawieszenia certyfikatu, lista CRL jest generowana i publikowana niezwłocznie po wystąpieniu tego zdarzenia. W przypadku wystąpienia zdarzenia unieważnienia certyfikatu na żądanie Subskrybenta, Zamawiającego lub innych upoważnionych lista CRL jest stworzona i opublikowana niezwłocznie, jednak nie później niż w okresie 1 godziny od momentu odebrania żądania unieważnienia.
Nowe wersje Polityk są publikowane niezwłocznie po zatwierdzeniu.
Jeśli Odbiorca certyfikatu i/lub Zamawiający wyraził zgodę na opublikowanie certyfikatu to takie certyfikaty, wystawione zgodnie z Polityką, są publikowane niezwłocznie, nie później niż po upływie 1 doby od momentu wygenerowania certyfikatu.
Certyfikat urzędu lub usługi OCSP – każdorazowo, niezwłocznie, gdy nastąpi wydanie nowego certyfikatu.

2.4. Kontrola dostępu do repozytorium

Repozytorium CUZ Sigillum jest ogólnodostępne w trybie „do odczytu”, w celu pobrania opublikowanych tam danych lub dokumentów.
Realizuje się kontrolę dostępu uniemożliwiającą dokonywanie nieautoryzowanych zmian statusów certyfikatów ani innych dokumentów umieszczonych w repozytorium.
Możliwe będzie ograniczenie dostępu do poszczególnych usług pojedynczym użytkownikom, jeżeli CA będzie w stanie wykazać, że użytkownik nadużywa system.

3. Zasady identyfikacji i uwierzytelnienia

Inspektorzy ds. rejestracji podczas wizyty weryfikują tożsamość oraz uwierzytelniają inne atrybuty wnioskujących o certyfikat, zanim wyślą do CA żądanie o certyfikat. CUZ Sigillum przygotowuje i nadzoruje stosowanie udokumentowanych procedur weryfikacji i uwierzytelniania klientów wnioskujących o certyfikaty.

Wniosek złożony osobiście w PR dotyczący dyspozycji certyfikatem wydanym przez to CA, jest uwierzytelniany przez Inspektora ds. rejestracji zanim zostanie zrealizowany lub w przypadku certyfikatów pieczęci i TLS przez inną upoważnioną przez CUZ Sigillum od tego osobę.

Odbiorcami niekwalifikowanych certyfikatów podpisu elektronicznego mogą być:

- Osoba fizyczna wnioskująca w imieniu własnym,
- Osoba fizyczna reprezentująca osobę prawną, na podstawie zamówienia złożonego przez reprezentanta osoby prawnej,
- Osoba fizyczna będąca upoważnionym przedstawicielem osoby prawnej, na podstawie zamówienia złożonego przez reprezentanta osoby prawnej,
- Osoba fizyczna będąca upoważnionym przedstawicielem osoby prawnej, na podstawie zamówienia złożonego przez osobę fizyczną będącą upoważnionym przedstawicielem osoby prawnej.

Odbiorcami niekwalifikowanych certyfikatów pieczęci elektronicznej oraz certyfikatów TLS mogą być:

- Osoba prawna, na podstawie zamówienia złożonego przez reprezentanta osoby prawnej
- Osoba prawna, na podstawie zamówienia złożonego przez osobę fizyczną będącą upoważnionym przedstawicielem osoby prawnej.

3.1. Zasady nadawania nazw

Certyfikaty wydawane w CUZ Sigillum będą certyfikatami X.509v3, tworzonymi w zgodzie z wymogami zawartymi w RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, z uwzględnieniem wymagań ze standardów europejskich.

3.1.1.Typy nazw

Pole identyfikatora podmiotu ‘subject’ umożliwia zidentyfikowanie podmiotu związanego z kluczem publicznym, umieszczonym w polu klucza publicznego wydanego certyfikatu. Pole ‘subject’ musi zawierać niepustą nazwę wyróżniającą podmiotu. Zawartość pola Odbiorca certyfikatu będzie zgodna z wytycznymi Rekomendacji ITU-T X.520.

3.1.2.Konieczność używania nazw znaczących

Odbiorca certyfikatu może występować pod pseudonimem. W celu zapewnienia możliwości jednoznacznej identyfikacji Odbiorcy certyfikatu, w polu identyfikatora podmiotu ‘subject’ wystąpią co najmniej atrybuty:

- Dla osoby fizycznej
    - countryName
    - do wyboru: (givenName i surname) lub pseudonym
    - commonName
    - serialNumber – może wystąpić, żeby zapewnić unikalność nazwy Odbiorcy w domenie wystawcy certyfikatów Identyfikator ten może przyjąć poniższe wartości:

      Identyfikator semantyczny

      a. Dowód osobisty
      b. Paszport
      c. PESEL
      d. NIP

      Identyfikator niesemantyczny:

      a. identyfikator własny

Dodatkowo, jeżeli osoba fizyczna występuje w powiązaniu z osoba prawną, i w certyfikacie ma być wskazane powiązanie z Zamawiającym, to mogą wystąpić co najmniej atrybuty:

- organizationIdentifier
- organizationName

- Dla osoby prawnej
    - countryName
    - organizationName
    - organizationIdentifier
    - commonName

- Dla certyfikatu serwerowego
    - o countryName
    - o organizationName
    - o organizationIdentifier
    - o commonName

W przypadku wybrania identyfikatora niesemantycznego – identyfikatora własnego CUZ Sigillum oświadcza, a Zamawiający i Subskrybent potwierdzają następujące okoliczności:
- dane zebrane podczas procesu rejestracji będą przechowywane u wystawcy certyfikatu przez okres wynikający z przepisów prawa,
- Zamawiający albo Subskrybent zobowiązani są do zapewnienia rozliczalności działań związanych z wykorzystaniem podpisu elektronicznego weryfikowanego w oparciu o certyfikat w ramach swojej działalności.

3.1.3.Zasady interpretacji różnych postaci nazw

Wystawca certyfikatów jest ostatecznym decydentem w zakresie dopuszczalnej zawartości DN, Subskrybent ma prawo nie wyrazić zgody na zaproponowaną zwartość nazwy DN. Znaczenie poszczególnych atrybutów nazw wyróżniających Odbiorców certyfikatów określone zostało w Polityce.

3.1.4.Stosowanie pseudonimów w nazwie w certyfikat podpisu

Odbiorca certyfikatu może występować pod pseudonimem. Wystawca certyfikatów, w procesie rejestracji, zapewni jednoznaczną weryfikację tożsamości właściciel certyfikatu, w którym występuje pseudonim. Dane zebrane podczas procesu rejestracji będą dostępne u wystawcy certyfikatu przez okres wynikający z przepisów prawa.

3.1.5.Unikalność nazw

CUZ Sigillum zapewnia unikalność nazw w domenie wystawcy certyfikatów, poprzez weryfikację już na poziomie rejestracji użytkowników, że nie zostaną zarejestrowani różni odbiorcy z tym samym zakresem danych w nazwie wyróżniającej certyfikatu (DN). Raz wykorzystana nazwa DN, nie może być wykorzystana przez innego Odbiorcę certyfikatu przez cały okres życia wystawcy certyfikatów.

CUZ Sigillum rozstrzyga spory dotyczące praw do wykorzystywania pseudonimu w identyfikatorze DN zawartym w certyfikatach wystawionych w domenie wystawcy

certyfikatów na korzyść osoby, która już posiada certyfikat zawierający ten pseudonim, wystawiony przez CUZ Sigillum.

W przypadku niekwalifikowanych certyfikatów pieczęci CUZ Sigillum dopuszcza dodanie do certyfikatu dodatkowego pola z unikalnym numerem OID, dostarczonym przez Zamawiającego.

3.1.6. Rozpoznawanie, uwierzytelnianie i rola znaków towarowych

CUZ Sigillum nie weryfikuje praw osób do posługiwania się znakami towarowymi.

3.2. Pierwsza rejestracja

Pojęcie pierwszej rejestracji obejmuje czynności, które są podejmowane przez CUZ Sigillum przed wygenerowaniem certyfikatu dla Subskrybenta mogącego być osobą fizyczną lub osobą prawną, w sytuacji, gdy nie posiada on ważnego certyfikatu wystawionego zgodnie z Polityką.

Przed wystawieniem certyfikatu, CUZ Sigillum przeprowadza weryfikację tożsamości Subskrybenta bądź jego reprezentanta (w przypadku, gdy Subskrybentem jest osoba prawna), co najmniej w zakresie opisanym w podrozdziałach 3.2.2 i 3.2.3, oraz innych atrybutów, które zostaną zebrana w trakcie procesu rejestracji.

W przypadku, gdy Subskrybent jest osobą fizyczną powiązaną z Zamawiającym, który jest osobą prawną, Inspektor ds. rejestracji zweryfikuje prawdziwość danych osoby prawnej, upoważnienie dla Subskrybenta oraz wszelkie inne atrybuty, które są niezbędne w celu uzyskania potwierdzenia powiązań pomiędzy Subskrybentem a osobą prawną. Jeżeli dane osoby prawnej mają wystąpić w atrybutach certyfikatu, obie strony muszą potwierdzić, że wyraziły na to zgodę.

Dopuszcza się 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 CUZ Sigillum.

W procesie rejestracji wniosków o certyfikat bierze udział co najmniej dwóch upoważnionych przedstawicieli CUZ Sigillum.

CA przygotowało i nadzoruje stosowanie udokumentowanych procedur weryfikacji i uwierzytelniania klientów wnioskujących o certyfikaty. Procedury te opisują zakres zbieranych dowodów, który nie wykracza poza dane niezbędne do potwierdzenia prawdziwości danych i atrybutów które zostaną umieszczone w certyfikacie.

W przypadku certyfikatów pieczęci lub TLS zamawiający przedkłada Inspektorowi ds. rejestracji lub innej upoważnionej osobie przez CUZ Sigillum upoważnienie do reprezentowania firmy i złożenia zamówienia w jej imieniu.

3.2.1.Uwierzytelnienie osób prawnych

W celu zidentyfikowania oraz uwierzytelnienia organizacji, która wnioskuje o certyfikat, weryfikowane są co najmniej:

- Dokumenty potwierdzające rejestrację organizacji zgodne z prawem krajowym,
- Dokumenty potwierdzające prawo do reprezentowania organizacji,
- Dokumenty potwierdzające powiązanie pomiędzy Zamawiającym a jednostką organizacyjną, której dane mają się pojawić w certyfikacie.

  Podczas weryfikacji organizacji, następuje również ustalenie i weryfikacja:
- Wszystkich reprezentantów osoby prawnej, na podstawie zapisów w dokumentach założycielskich
- Upoważnionych przedstawicieli osoby prawnej na podstawie dostarczonego upoważnienia oraz wcześniej zweryfikowanych danych o reprezentantach osoby prawnej.

Zweryfikowane zostaną co najmniej następujące dane: pełna nazwa organizacji i numer identyfikacji podatkowej.

3.2.2. Weryfikacja tożsamości osób fizycznych

W celu zidentyfikowania oraz uwierzytelnienia osoby występującej o certyfikat, tożsamość osoby będzie weryfikowana na podstawie dokumentu potwierdzającego tożsamość. Zweryfikowane zostaną co najmniej następujące dane: nazwisko, imiona, data i miejsce urodzenia oraz narodowy unikalny numer identyfikacyjny, o ile w danym kraju występuje, numer i seria dokumentu tożsamości.

W celu przeprowadzenia weryfikacji tożsamości Osoba fizyczna musi stawić się osobiście co najmniej raz w Punkcie Rejestracji lub u notariusza.

Proces uwierzytelnienia przeprowadzany jest przez upoważnione osoby na podstawie przedstawionych dokumentów i polega na weryfikacji tożsamości oraz w przypadku, gdy osoba fizyczna jest powiązana z organizacją, na potwierdzeniu pełnomocnictwa i/lub upoważnienia, oraz na weryfikacji ich zakresu.

CUZ Sigillum przygotował szczegółową procedurę opisującą proces rejestracji. Dokumenty zawierające m. in. tę procedurę są dokumentami wewnętrznymi udostępnianymi tylko określonej grupie pracowników i współpracowników realizujących proces rejestracji.

3.2.3.Zawarcie umowy

Przed wystawieniem certyfikatu podpisu, Subskrybent jest zobligowany do podpisania umowy o świadczenie usług certyfikacyjnych z CUZ Sigillum. Jeżeli w procesie występuje Zamawiający, to także jest zobligowany do podpisania stosownej umowy. Umowa może być podpisana w

formie papierowej bądź elektronicznej przy użyciu kwalifikowanego podpisu elektronicznego. Po stronie PWPW S.A. umowę podpisuje uprawniony Inspektor ds. Rejestracji.

Wzory umów z Subskrybentem i Zamawiającym znajdują się w ogólnodostępnym repozytorium na stronie internetowej sigillum.pl

3.3. Wystawienie kolejnego certyfikatu

Proces wystawienia kolejnego certyfikatu niekwalifikowanego dla klienta przebiega identycznie jak proces wystawienia pierwszego certyfikatu, łącznie z procesem pełnej identyfikacji i uwierzytelniania wnioskodawcy.

3.4. Zawieszenie i unieważnienie certyfikatów

Dyspozycja certyfikatem następuje drogą elektroniczną, telefonicznie lub poprzez osobiste stawienie się Subskrybenta/przedstawiciela Zamawiającego w Punkcie rejestracji po uwierzytelnieniu się danymi ustalonymi Subskrybentem/przedstawicielem Zamawiającego, – jeśli dane takie zostały ustalone. Podanie poprawnych danych uwierzytelniających jest wystarczające do wydania dyspozycji.

Jeżeli danych służących do uwierzytelnienia dyspozycji certyfikatem nie ustalono na etapie rejestracji/ wydawania certyfikatu lub osoba, która chce wydać dyspozycję nie zna tych danych, złożenie dyspozycji możliwe jest tylko osobiście w punkcie rejestracji po uwierzytelnieniu osoby i zweryfikowaniu uprawnień do wydania dyspozycji.

Uwierzytelnienie składającego dyspozycję oraz jego uprawnień następuje na zasadach opisanych w rozdziałach 3.2.1 i 3.2.2.

3.5. Gromadzenie i przetwarzanie danych

Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Rozporządzenie 2016/679) CUZ Sigillum informuje, że:

1. Administratorem, w rozumieniu Rozporządzenia 2016/679 danych osobowych Subskrybenta jest CUZ Sigillum z siedzibą w Warszawie, adres: ul. Sanguszki 1, 00-222 Warszawa.
2. CUZ Sigillum wyznaczyła Inspektora Ochrony Danych, z którym można skontaktować się poprzez adres email iod@pwpw.pl w każdej sprawie dotyczącej przetwarzania danych osobowych Subskrybenta.

3. Podane dane osobowe Subskrybenta będą przetwarzane w celu zawarcia i realizacji umowy, na podstawie art. 6 ust. 1 lit. b) Rozporządzenia 2016/679, zgodnie z którym przetwarzanie danych jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. Dane identyfikacyjne i kontaktowe pozyskane w procesie weryfikacji i uwierzytelniania osób fizycznych i prawnych są gromadzone i przetwarzane zgodnie z obowiązującymi przepisami o ochronie danych osobowych. Kopie i odpisy dokumentów użytych do uwierzytelnienia osób prawnych przechowywane są w archiwum CUZ Sigillum. CUZ Sigillum gromadzi tylko dane niezbędne do potwierdzenia tożsamości i wystawienia certyfikatu.
4. Dane osobowe Subskrybenta mogą być przekazywane:
   a) podmiotom współpracującym z PWPW S.A. realizującym określone zadania w związku z prowadzoną przez PWPW S.A. działalnością, w tym podmiotom przetwarzającym dane osobowe na rzecz PWPW S.A. na podstawie umów powierzenia przetwarzania danych osobowych,
   b) organom uprawnionym do otrzymania osobowych na podstawie przepisów prawa.
5. Dane osobowe Subskrybenta nie będą przekazywane do państwa trzeciego ani organizacji międzynarodowej.
6. Subskrybentowi przysługuje prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania oraz prawo do przenoszenia danych.
7. Subskrybentowi przysługuje prawo wniesienia skargi do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych Osobowych zajmującego się ochroną danych osobowych, w przypadku uznania przez Subskrybenta, że przetwarzanie jego danych osobowych narusza przepisy Rozporządzenia 2016/679.
8. Dane osobowe Subskrybenta nie będą wykorzystane do profilowania lub do zautomatyzowanego podejmowania decyzji.
9. Dane osobowe Subskrybenta będą przetwarzane przez okres niezbędny do realizacji celu, dla którego zostały zebrane.
10. Podanie przez Subskrybenta danych osobowych jest dobrowolnie niemniej jednak konsekwencją niepodania danych osobowych będzie brak możliwości zawarcia i realizacji umowy.”

4. Wymagania dotyczące świadczonych usług

4.1. Zgłoszenie certyfikacyjne

O certyfikat może wnioskować osoba fizyczna, osoba prawna, osoby fizyczna lub prawna zarządzająca sprzętem bądź systemem, dla którego ma zostać wystawiony certyfikat.

4.2. Obsługa zgłoszenia certyfikacyjnego

Każde zgłoszenie certyfikacyjne, które ma zostać zrealizowane przez Centrum Certyfikacji, musi pochodzić z zaufanego kanału rejestracji. Dane rejestracyjne są przekazywane w sposób bezpieczny po wykonaniu uwierzytelnienia dostawcy usługi rejestracji.
Inspektor punktu rejestracji lub inna upoważniona przez CUZ Sigillum do tego osoba identyfikuje Odbiorców i Zamawiających, weryfikuje i uwierzytelnia dostarczone dane i informacje, a następnie rozpoczyna proces generowania certyfikatu.

4.3. Wydanie certyfikatu

Po otrzymaniu żądania certyfikacyjnego, urząd certyfikacji weryfikuje poprawność żądania i na podstawie pozytywnie zweryfikowanych żądań certyfikacyjnych generuje certyfikat dla Subskrybenta certyfikatu lub w przypadku certyfikatów pieczęci i TLS dla upoważnionego reprezentanta firmy.

4.4. Akceptacja certyfikatu

Po odebraniu certyfikatu Subskrybent i Zamawiający mają obowiązek do niezwłocznego sprawdzenia jego zawartości. W przypadku dostrzeżenia jakichkolwiek pomyłek, w szczególności związanych z identyfikacją Odbiorcy certyfikatu, ma on obowiązek do niezwłocznego zgłoszenia tego faktu CUZ Sigillum, celem unieważnienia certyfikatu.

Jeżeli zawartość certyfikatu jest poprawna, Zamawiający potwierdza ten fakt podpisując stosowne oświadczenie.

Kontrola poprawności certyfikatu musi być przeprowadzona przed pierwszym użyciem klucza prywatnego związanego z certyfikatem. W przypadku zaniechania tego obowiązku i posługiwania się kluczem związanym z nieprawidłowym kwalifikowanym certyfikatem, Subskrybenta może narazić się na odpowiedzialność prawną.

4.5. Zasady używania certyfikatu i pary kluczy

Certyfikaty i klucze prywatne powinny być wykorzystywane przez Subskrybenta zgodnie z zasadami w szczególności:

- Algorytm i długość klucza powinny być zgodne z dopuszczonymi przez niniejszą politykę
- Pary kluczy będzie używana tylko zgodnie wymaganiami zakomunikowanymi Zamawiającemu i Subskrybentowi
- Subskrybent będzie unikał nieuprawnionego używania klucza prywatnego
- Klucz prywatny będzie używany tylko pod wyłączną kontrolą Subskrybenta
- Subskrybent i/lub Zamawiający mają obowiązek poinformować Centrum Certyfikacji o przypadkach:
    - Zgubienia, ukradzenia lub podejrzenia kompromitacji klucza prywatnego
    - Utraty kontroli nad kluczem prywatnym z powodu ujawnienia danych aktywacyjnych lub z innych przyczyn
    - Niepoprawności danych w certyfikacje lub o zmianie danych, które zostały zawarte w certyfikacie
- W przypadku kompromitacji klucza prywatnego Subskrybenta, zaniechanie używania klucza prywatnego w celu innym niż odszyfrowanie danych
- Zaniechanie używania klucza prywatnego po otrzymaniu informacji o unieważnieniu certyfikatu Subskrybenta lub certyfikatu urzędu
- Jeżeli certyfikat jest certyfikatem podpisu, klucz prywatny wolno używać tylko do wykonania podpisu

  Strona ufająca zobowiązana jest do weryfikacji statusu certyfikatu klucza publicznego, powiązanego z kluczem prywatnym, którym został podpisany lub opieczętowany otrzymany przez nią dokument elektroniczny, z wykorzystaniem jednej ze wskazanych w Polityce metod weryfikacji statusu certyfikatu.

4.6. Odnowienie certyfikatu

Proces odnowienia certyfikatu jest realizowany w ten sam sposób jak wydanie nowego certyfikatu.

4.7. Odnowienie certyfikatu z wymianą klucza

Proces odnowienia certyfikatu z wymianą klucza jest realizowany w ten sam sposób jak wydanie nowego certyfikatu.

4.8. Modyfikacja zawartości certyfikatu

Proces modyfikacji zawartości certyfikatu jest realizowany w ten sam sposób jak wydanie nowego certyfikatu.

4.9. Zawieszenie, uchylenie zawieszenia i unieważnienie certyfikatu

Zawieszenie certyfikatu następuje z inicjatywy CUZ Sigillum, w przypadku uzasadnionego podejrzenia, że istnieją przesłanki do zawieszenia certyfikatu. W szczególności wystarczającą przesłanką jest odebranie przez CUZ Sigillum informacji telefonicznej, drogą elektroniczną lub poprzez osobiste stawienie się Subskrybenta/przedstawiciela Zamawiającego w Punkcie rejestracji z prośbą, o zawieszenie certyfikatu, uwierzytelnionej danymi ustalonymi z Subskrybentem/Zamawiającym, – jeśli dane takie zostały ustalone.

Uchylenie zawieszenia certyfikatu następuje z inicjatywy CUZ Sigillum, jeśli stwierdzi ustanie przyczyn powodujących zawieszenie. W szczególności, jeśli zawieszenie nastąpiło po otrzymaniu przez CUZ Sigillum informacji od Subskrybenta/przedstawiciela Zamawiającego, uchylenie zawieszenia może nastąpić na prośbę telefoniczną, prośbę przesłaną drogą elektroniczną odpowiednio przez Subskrybenta lub przedstawiciela Zamawiającego, uwierzytelnioną danymi ustalonymi z Subskrybentem lub przedstawicielem Zamawiającego – jeśli dane takie zostały ustalone, lub też poprzez osobiste stawienie się Subskrybenta/przedstawiciela Zamawiającego w Punkcie Rejestracji.

Unieważnienie certyfikatu następuje:

1) na wniosek Subskrybenta,
2) na wniosek Zamawiającego lub innej osoby, której dane zostały zawarte w certyfikacie,
3) na wniosek osób trzecich po uzyskaniu potwierdzenia u Subskrybenta lub Zamawiającego,
4) na wniosek Organu Nadzoru,
5) z inicjatywy CUZ Sigillum.

Unieważnienie certyfikatu na wniosek Subskrybenta następuje na podstawie:

- informacji telefonicznej zawierającej dyspozycję Subskrybenta certyfikatu unieważnienia certyfikatu, uwierzytelnionej danymi ustalonymi z Subskrybentem - jeśli dane takie zostały ustalone, lub
- oryginału dokumentu opatrzonego własnoręcznym podpisem Subskrybenta, złożonym w obecności upoważnionego przedstawiciela CUZ Sigillum, po potwierdzeniu tożsamości na zasadach opisanych w rozdziale 5.1 lub
- dokumentu elektronicznego opatrzonego ważnym kwalifikowanym podpisem elektronicznym złożonym przez Subskrybenta.

Unieważnienie certyfikatu na wniosek Zamawiającego lub innej osoby, której dane zostały zawarte w certyfikacie następuje na podstawie:

- informacji telefonicznej zawierającej dyspozycję Zamawiającego lub innej osoby, której dane zostały zawarte w certyfikacie unieważnienia certyfikatu, uwierzytelnionej danymi ustalonymi z Zamawiającym lub z tą inną osobą - jeśli dane takie zostały ustalone, lub
- oryginału dokumentu opatrzonego własnoręcznym podpisem przedstawiciela Zamawiającego lub innej osoby, której dane zostały zawarte w certyfikacie, złożonym
- w obecności upoważnionego przedstawiciela CUZ Sigillum, po potwierdzeniu tożsamości przedstawiciela Zamawiającego lub tej innej osoby na zasadach opisanych w rozdziale 5.1 oraz po okazaniu oryginału upoważnienia do występowania w imieniu Zamawiającego lub tej innej osoby albo
- dokumentu elektronicznego opatrzonego ważnym kwalifikowanym podpisem elektronicznym złożonym przez przedstawiciela Zamawiającego lub innej osoby, której dane zostały zawarte w certyfikacie, jeśli CUZ Sigillum ma możliwość potwierdzenia upoważnienia do występowania danej osoby w imieniu Zamawiającego lub tej innej osoby na podstawie innych dokumentów (np. z umowy o świadczenie usług zaufania z Zamawiającym).

Unieważnienie certyfikatu na wniosek Osoby trzeciej następuje na podstawie:

- oryginału dokumentu, zawierającego informacje o przyczynie złożenia dyspozycji (np. raport z incydentu wskazującego na możliwość bezprawnego użycia klucza prywatnego), opatrzonego własnoręcznym podpisem Osoby trzeciej, złożonym w obecności upoważnionego przedstawiciela CUZ Sigillum, po potwierdzeniu tożsamości na zasadach opisanych w rozdziale 5.1, lub
- dokumentu elektronicznego, zawierającego informacje o przyczynie złożenia dyspozycji (np. raport z incydentu wskazującego na możliwość bezprawnego użycia klucza prywatnego), opatrzonego ważnym kwalifikowanym podpisem elektronicznym złożonym przez Osobę trzecią, po potwierdzeniu u Dysponenta certyfikatu, że należy zrealizować złożoną dyspozycję.

Unieważnienie certyfikatu na wniosek Organu Nadzoru następuje na podstawie:

- oryginału dokumentu opatrzonego własnoręcznym podpisem ministra właściwego ds. informatyzacji (lub upoważnionego przedstawiciela ministra), albo
- dokumentu elektronicznego opatrzonego ważnym kwalifikowanym podpisem elektronicznym ministra właściwego ds. informatyzacji (lub upoważnionego przedstawiciela ministra).

Niezwłoczne unieważnienie certyfikatu kwalifikowanego przez CUZ Sigillum następuje po upływie 7 dni od momentu zawieszenia w przypadku niemożności wyjaśnienia przyczyn zawieszenia certyfikatu kwalifikowanego. Jako data unieważnienia zostaje użyta pierwotna data zawieszenia. W przypadku wyjaśnienia okoliczności zawieszenia certyfikatu kwalifikowanego, CUZ Sigillum zobowiązane jest do uchylenia zawieszenia.

Jeśli CUZ Sigillum zawrze z Zamawiającym lub tylko z Odbiorcą certyfikatu umowę o świadczenie usług zaufania, może ona przewidywać inne wymagania niż określono powyżej dotyczące sposobu uwierzytelnienia Odbiorcy certyfikatu występującego w imieniu Zamawiającego lub innej osoby, której dane zostały zawarte w certyfikacie przy unieważnianiu, zawieszaniu lub odwoływaniu zawieszenia certyfikatów.

Czas od momentu otrzymania Dyspozycji certyfikatem do podjęcia decyzji i opublikowania nowego statusu certyfikatu wynosi maksymalnie 24 godziny.

Dyspozycja certyfikatem zostanie zrealizowana bez zbędnej zwłoki, najpóźniej w ciągu godziny od podjęcia decyzji o realizacji dyspozycji. Lista CRL zostanie wygenerowana i opublikowana niezwłocznie.

Urząd certyfikacji, wnioskodawca oraz dysponenci certyfikatu zostaną poinformowani zarówno o realizacji Dyspozycji, jak również o odmowie realizacji Dyspozycji wraz z podaniem przyczyny odmowy.

Głównym i zalecanym, stronom ufającym, sposobem weryfikacji statusu certyfikatu, który jest w swoim okresie ważności wskazanym w certyfikacie, jest korzystanie z usługi weryfikacji statusu on-line (OCSP). W przypadku potrzeby zweryfikowania certyfikatu po jego okresie ważności, niezbędne jest skorzystanie z list CRL, na których przechowywane będą informacje o wszystkich unieważnionych certyfikatach wydanych przez ten urząd.

Lista unieważnionych certyfikatów jest generowana i publikowana nie rzadziej niż co 12 godzin, niezależnie od tego, czy wystąpiły unieważnienia lub zawieszenia.

Certyfikatu, który został unieważniony nie można ponownie aktywować.

CUZ Sigillum nie świadczy innej metody weryfikacji statusu certyfikatu niż poprzez usługę OCSP lub weryfikację statusu certyfikatu na liście CRL.

Czas w systemach zaangażowanych w proces realizacji dyspozycji certyfikatem jest synchronizowany z czasem UTC przynajmniej raz dziennie.

4.10. Usługi weryfikacji statusu certyfikatu

CUZ Sigillum świadczy usługę weryfikacji statusu certyfikatu, nieodpłatnie w sposób ciągły.

Status certyfikatu można zweryfikować:

- W usłudze OCSP dostępnej pod adresem wskazanym w certyfikacie,
- Na liście CRL dostępnej pod adresem wskazanym w certyfikacie.

4.11. Zakończenie korzystania z usługi

Odbiorca usług zaufania może zakończyć korzystanie z usługi zaufania poprzez unieważnienie certyfikatu. W momencie osiągniecia końca ważności certyfikatu, w przypadku nieodnowienia certyfikatu, następuje zakończenie korzystania z usługi zaufania przez Odbiorcę.

4.12. Archiwizacja kluczy

CUZ Sigillum nie archiwizuje kluczy prywatny Odbiorców ani nie świadczy usługi depozytu kluczy prywatnych Subskrybentów.

5. Zabezpieczenia fizyczne, organizacyjne i osobowe

W celu zapewnienia maksymalnego poziomu bezpieczeństwa dla świadczonych zaufanych usług CUZ Sigillum stosuje m.in. zabezpieczenia fizyczne, organizacyjne i operacyjne. W rozdziale tym zostały opisane stosowane przez CUZ Sigillum te zabezpieczenia oraz sposoby ich kontrolowania.

Wszystkie zasoby całego systemu teleinformatycznego, służącego do świadczenia usług zaufania, umiejscowione są w wydzielonych pomieszczeniach, z ograniczonym i kontrolowanym dostępem, chronione przed zniszczeniem lub nieuprawnioną modyfikacją. Ponadto podjęte przez CUZ Sigillum działania mają na celu:

- niedopuszczenie do wystąpienia sytuacji awaryjnej, zagrażającej bezpieczeństwu przetwarzanych informacji, a zwłaszcza tych, które dotyczą żywotnych interesów strony ufającej;
- zminimalizowanie skutków ewentualnego zakłócenia pracy systemu.

Cała działalność CUZ Sigillum związana ze świadczeniem usług zaufania jest nadzorowana i kontrolowana. Dotyczy to zarówno działań osób związanych ze świadczonymi usługami, jak i działania całego systemu teleinformatycznego, środowiska pracy (energia, woda, klimatyzacja) oraz dostępu do pomieszczeń i systemu teleinformatycznego.

Na potrzeby prowadzonej przez siebie działalności CUZ Sigillum certyfikowała się w zakresie zarządzania bezpieczeństwem informacji z normy ISO IEC 27001.

5.1. Zabezpieczenia fizyczne

W CUZ Sigillum funkcjonują następujące systemy związane z zabezpieczeniami fizycznymi:

- kontroli dostępu i antywłamaniowy;

- ochrony przeciwpożarowej i automatycznego gaszenia pożaru;
- kontroli środowiska – temperatury, wilgotności i zalania wodą;
- awaryjnego zasilania.

Systemy monitorujące, związane z bezpieczeństwem fizycznym, powiadamiają automatycznie służby ochrony. W razie konieczności powiadamiane są również osoby pełniące odpowiednie role przy świadczeniu usług zaufania w CUZ Sigillum.

W CUZ Sigillum wykorzystywane są również systemy monitorujące pracę osób zatrudnionych przy świadczeniu usług zaufania oraz systemy monitorujące prace urządzeń teleinformatycznych.

Wszystkie systemy monitorujące pracują w sposób ciągły, tzn. 24 godziny na dobę. W celu zapewnienia bezawaryjnej pracy wszystkich systemów monitorujących oraz wspomagających, dokonuje się ich regularnych przeglądów i konserwacji, zgodnie z wymaganiami prawa, umowami serwisowymi i przyjętą w PWPW S.A. polityką.

5.1.1. Miejsce lokalizacji oraz budynek

Jednostka organizacyjna świadcząca zaufane usługi zaufania oznaczone CUZ Sigillum jest umiejscowiona w strefie bezpiecznej na terenie PWPW S.A. Dotyczy to ośrodków podstawowego oraz zapasowego. Ośrodki te znajdują się w lokalizacjach znacznie oddalonych od siebie. Ośrodek zapasowy ma możliwość przejęcia pełnej funkcjonalności ośrodka podstawowego.

Konstrukcje budynków spełniają wymagania dotyczące stref o wysokim poziomie bezpieczeństwa. Pomieszczenia, w których są świadczone usługi zaufania oraz w których znajdują się różne elementy infrastruktury teleinformatycznej wykorzystywanej do świadczenia tych usług, wyposażone są w kontrolę zamknięcia. Ponadto, dla ochrony zasobów związanych z usługami zaufania, CUZ Sigillum stosuje dodatkowe, wydzielone strefy w postaci klatek i sejfów.

Pomieszczenia, w których świadczone są usługi zaufane podzielone są na strefy:

- pomieszczenia administracyjno-operatorskie;
- pomieszczenia systemu teleinformatycznego.

CUZ Sigillum posiada, obok ośrodka podstawowego, ośrodek zapasowy, który podejmuje prace w przypadku, gdy działanie ośrodka podstawowego jest ograniczone lub niemożliwe. Regularnie, w zaplanowanych terminach, odbywają się testy związane z przełączeniem pracy na ośrodek zapasowy oraz poprawnością jego funkcjonowania.

W celu zapewnienia ciągłego świadczenia usług zaufania dostęp do pomieszczeń oraz całego systemu teleinformatycznego CUZ Sigillum zapewniony jest, dla osób pełniących zaufane role w systemie, przez 24 godziny na dobę.

5.1.2. Dostęp fizyczny

Fizyczna kontrola dostępu do CUZ Sigillum jest zapewniona przez standardowe procedury ochrony dostępu obowiązujące na terenie PWPW S.A. oraz przez dodatkowe środki, zapewniające możliwość dostępu do CUZ Sigillum tylko osób uprawnionych. Kontroli podlegają także wszelkie aktywa informacyjne wnoszone i wynoszone na lub poza teren PWPW S.A.

Fizyczny dostęp do pomieszczeń CUZ Sigillum chroniony jest przez służbę ochrony oraz system kontroli dostępu (SKD). Tylko upoważnione osoby mają dostęp fizyczny do bezpiecznych stref, gdzie uwierzytelnienie odbywa się na podstawie elektronicznej karty dostępu oraz numeru PIN. Osoby, które nie posiadają uprawnień w dostępie do pomieszczeń CUZ Sigillum mogą w nich przebywać tylko i wyłącznie pod nadzorem personelu CUZ Sigillum.

5.1.3. Zasilanie i klimatyzacja

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

W przypadku awarii systemu zasilania podstawowego następuje automatyczne przełączenie na zasilanie awaryjne – generator prądu lub UPS.

System klimatyzacyjny zapewnia stabilną temperaturę we wszystkich pomieszczeniach, które są monitorowane pod kątem temperatury i wilgotności. Przekroczenie zadanych wartości progowych powoduje automatyczne powiadomienie personelu CUZ Sigillum.

5.1.4. Ujęcia wody

CUZ Sigillum w obrębie swoich pomieszczeń krytycznych nie posiada ujęć wody. Pomieszczenia CUZ Sigillum są chronione i monitorowane przed zalaniem wodą. Serwerownie w ośrodkach podstawowym i zapasowym monitorowane są czujkami zalania. Pojawienie się wody w tych pomieszczeniach powoduje automatyczne powiadomienie personelu CUZ Sigillum oraz służb ochrony.

5.1.5. Ochrona przeciwpożarowa

Pomieszczenia CUZ Sigillum są chronione i monitorowane pod kątem wystąpieniem pożaru zgodnie z obowiązującymi przepisami. W serwerowniach ośrodka podstawowego i zapasowego zainstalowany jest system automatycznego gaszenia pożaru.

Obok pomieszczeń, w których są świadczone usługi zaufania znajdują są hydranty, a same pomieszczenia wyposażone są w gaśnice umożliwiające gaszenie sprzętu elektronicznego.

Personel CUZ Sigillum jest regularnie szkolony w zakresie ochrony przeciwpożarowej, a w PWPW S.A. odbywają się regularne ćwiczenia personelu związane z tą ochroną.

5.1.6. Użytkowanie nośników danych

Nośniki danych przechowywane przez CUZ Sigillum są zabezpieczone przed wpływem czynników środowiskowych takich jak temperatura, wilgotność i pole magnetyczne. Nośniki danych krytycznych dla świadczenia usług zaufania przechowywane są w sejfach ognioodpornych w pomieszczeniach ośrodka podstawowego. Kopie tych nośników przechowywane są w pomieszczeniach ośrodka zapasowego również w sejfach ognioodpornych.

Tylko autoryzowane nośniki mogą być użyte w systemie teleinformatycznym, użycie nośników jest dozwolone wyłącznie przez autoryzowanych użytkowników.

Wszystkie nośniki, na których utrwalane są informacje związane ze świadczonymi usługami zaufania podlegają ewidencjonowaniu oraz kontroli.

Dostęp do nośników informacji jest ograniczony tylko do osób uprawnionych.

5.1.7. Utylizacja nośników danych

Dokumenty papierowe i nośniki informacji zawierające elementy podlegające ochronie są fizycznie niszczone po okresie przechowywania. Niszczenie to odbywa się pod nadzorem.

Fizyczne niszczenie odbywa się zgodnie z zasadami przyjętymi w PWPW S.A. i potwierdzone jest odpowiednim protokołem zniszczenia.

Po zniszczeniu nośników, zarówno papierowych, jak i elektronicznych, nie ma możliwości odzyskania informacji uprzednio na nich zapisanych.

5.1.8. Przechowywanie kopii zapasowych poza siedzibą CUZ Sigillum

CUZ Sigillum opracowało i wdrożyło procedury zapewniające przechowywanie dwóch jednakowych kompletów kopii zapasowych i archiwalnych: jednego w ośrodku podstawowym, a drugiego w ośrodku zapasowym.

Kopiowaniu i archiwizowaniu podlegają wszystkie wymagane przez Ustawę i Rozporządzenie informacje związane ze świadczonymi przez CUZ Sigillum usługami zaufania.

Zapasowe egzemplarze kluczy kryptograficznych, numerów PIN, haseł itp. przechowywane są w specjalnych strefach (poza siedzibą CUZ Sigillum) o ograniczonym dostępie i chronione przed skutkami różnych katastrof.

5.2. Zabezpieczenia organizacyjne

CUZ Sigillum, obok zabezpieczeń fizycznych, stosuje również zabezpieczenia organizacyjne pozwalające na utrzymanie maksymalnego możliwego poziomu bezpieczeństwa oraz gwarantującego wysoki poziom świadczonych usług zaufania.

Osobom zatrudnionym w CUZ Sigillum, przypisane są odpowiednie role przy świadczeniu usług zaufania. Role i zakres obowiązków pracownika są zapisane w Karcie obowiązków uprawnień i odpowiedzialności lub Umowie świadczenia usług.

5.2.1. Zaufane role

W celu rozdziału odpowiedzialności osób pełniących zaufane role w CUZ Sigillum zdefiniowane są następujące role personelu:

1. Kierownik CUZ Sigillum odpowiada za prawidłowe funkcjonowanie CUZ Sigillum, określa kierunki jej rozwoju oraz wdraża i zarządza Polityką Certyfikacji (KS);
2. Osoby nadzorujące wdrożenie i stosowanie wszystkich procedur bezpiecznej eksploatacji systemów teleinformatycznych wykorzystywanych przy świadczeniu usług zaufania, zwane dalej „Inspektorami ds. Bezpieczeństwa" (IB);
3. Osoby, które potwierdzają tożsamość Subskrybenta oraz zatwierdzają przygotowane zgłoszenia certyfikacyjne, zwane dalej „Inspektorami ds. Rejestracji" (IR);
4. Osoby, które na wniosek uprawnionego podmiotu realizują unieważnienie certyfikatu, zwane dalej „Inspektorami ds. Unieważnienia" (IU);
5. Osoby, które instalują, konfigurują i zarządzają systemem i siecią teleinformatyczną, zwane dalej „Administratorami Systemu" (AS);
6. Osoby, które wykonują stałą obsługę systemu teleinformatycznego, w tym tworzą kopie zapasowe, zwane dalej „Operatorami Systemu" (OS);
7. Osoby, które analizują zapisy rejestrów zdarzeń mających miejsce w systemach teleinformatycznych wykorzystywanych przy świadczeniu usług zaufania, zwane dalej „Inspektorami ds. Audytu" (IA).

Osoby pełniące zaufane role muszą spełniać wymagania określone Ustawą.

5.2.2. Liczba osób wymaganych do zadania

W swoich procedurach bezpieczeństwa związanych ze świadczeniem usług zaufania CUZ Sigillum określa ilości potrzebnych osób do wykonywania poszczególnych czynności. W wielu wypadkach czynności wykonywane przez operatorów (OS) lub administratorów (AS) są nadzorowane przez inspektorów (IB).

Szczególnemu nadzorowi podlegają procesy generowania kluczy używanych przez CUZ Sigillum do podpisywania: certyfikatów, odpowiedzi OCSP, list CRL i znaczników czasu. Przy generowaniu kluczy biorą udział m.in. Inspektor ds. Bezpieczeństwa, Administrator Systemu, Operator Systemu, Inspektor ds. Audytu oraz obserwatorzy.

Ponadto, CUZ Sigillum stosuje zasadę współdzielonego dostępu do wielu czynności lub zasobów systemu pracującego na rzecz świadczenia usług zaufania. Dotyczy to przede wszystkim czynności administracyjnych, sprawdzania rejestrów zdarzeń i wykonywania kopi bezpieczeństwa.

5.2.3. Identyfikacja i uwierzytelnianie każdej roli

Każda osoba zatrudniona przy świadczeniu usług zaufanych, w zależności od piastowanej roli, posiada ściśle określone uprawnienia w dostępie do:

- pomieszczeń, w których świadczone są usługi zaufane lub w których znajduje się sprzęt lub dokumentacja wykorzystywane do świadczenia takich usług;
- systemu teleinformatycznego wykorzystywanego w CUZ Sigillum;
- czynności wykonywanych na oprogramowaniu i danych.

Każda z osób zatrudnionych przy świadczeniu usług zaufania posiada swoje indywidualne konto, które umożliwia ścisłe rozliczanie tej osoby oraz przy pomocy, którego nadawane są ściśle określone uprawnienia. Logowanie do kont umożliwiających bezpośrednie wydawanie certyfikatów, wymaga użycia certyfikatu przechowywanego na karcie kryptograficznej zabezpieczonej PIN'em.

Przegląd kont i uprawnień w CUZ Sigillum odbywa się zgodnie z zasadami przyjętymi w PWPW S.A. Nieużywane konta są niezwłocznie blokowane, a uprawnienia odbierane.

W CUZ Sigillum zainstalowane jest również oprogramowanie nadzorujące pracę poszczególnych osób. Dostęp do tego oprogramowania i informacji przez nie przechowywanych mają tylko te osoby, dla których wynika to z pełnionej roli w systemie świadczenia usług zaufania.

W CUZ Sigillum stosuje się zasadę „minimalnych przywilejów", tzn. osoby wykonujące mające dostęp do pomieszczeń lub systemu teleinformatycznego posiadają tylko te uprawnienia, które są potrzebne do prawidłowego wykonywania swojej pracy. Obowiązki i zakresy odpowiedzialności są rozdzielone na poszczególne komórki organizacyjne w PWPW S.A.

5.2.4. Rozdzielenie obowiązków dla każdej z ról

Nie mogą być ze sobą łączone funkcje, o których mowa w pkt. 1 i 3 oraz w pkt. 1 i 4 Rozdziału 5.2.1. Funkcja, o której mowa w pkt. 5 nie może być łączona z żadną inną z funkcji wymienionych w Rozdziale 5.2.1.

5.3. Zarządzanie personelem

CUZ Sigillum zatrudnia pracowników o wymaganych dla świadczenia usług zaufania kwalifikacjach oraz spełniać określone w Ustawie wymagania. Zatrudnienie odbywa się w oparciu o umowę o pracę lub umowę cywilno-prawną, która określa rolę, jaką osoba będzie pełnić w systemie świadczenia usług zaufania. W ten sposób zapewnione jest zarówno bezpieczeństwo informacji, jak i wysoki poziom świadczonych usług zaufania.

5.3.1. Wymagania związane z kwalifikacjami, doświadczeniem i sprawdzeniem personelu

PWPW S.A. posiada procedury zatrudniania i wyboru personelu uwzględniające przygotowanie, kwalifikacje, doświadczenie zawodowe i wymagania do pracy na danym stanowisku. Stosuje również metody sprawdzenia osoby zatrudnianej na dane stanowisko związane z pełnioną zaufaną rolą.

Każda zatrudniona w PWPW S.A. osoba, niezależnie od formy zatrudnienia, ma ściśle określony zakres obowiązków i uprawnień związanych z rolą, jaką pełni w systemie. Zakres ten musi być podpisany własnoręcznie przez osobę zatrudnioną.

Posiadane przez danego pracownika obowiązki i uprawnienia determinują ściśle zakres dostępu tej osoby do pomieszczeń i systemu teleinformatycznego CUZ Sigillum.

Przed przystąpieniem do wykonywania obowiązków przy świadczeniu usług zaufania, osoba zatrudniona musi odbyć wymagane prawem szkolenia związane z wykonywanymi obowiązkami, w tym w szczególności w z zakresie Ustawy, ochrony danych osobowych i ochrony przeciwpożarowej.

Pracownicy sprawujący kierownicze funkcje posiadają doświadczenie lub wykształcenie w odniesieniu do świadczonej usługi zaufania. Osoby te wykazują się znajomością procedur bezpieczeństwa dla podległego im personelu, są odpowiedzialne za bezpieczeństwo informacji i oceny ryzyka oraz posiadają widzę wystarczającą do wykonywania funkcji zarządzania.

Każdy pracownik, który ma pełnić zaufaną role w CUZ Sigillum musi zostać zaakceptowany przez kierownictwo jednostki organizacyjnej PWPW S.A. właściwej do świadczenie usług zaufania.

5.3.2. Kontrola przygotowania pracownika

Kontrola przygotowania do pracy na danym stanowisku wiążącym się z pełnieniem zaufanej roli jest przeprowadzana w stosunku do każdego nowego pracownika, przed dopuszczeniem go do wykonywania obowiązków oraz w trakcie zatrudnienia. CUZ Sigillum weryfikuje kwalifikacje oraz doświadczenie zawodowe i wymaga oświadczenia o niekaralności.

Szczególny nacisk położony jest na znajomość zagadnień związanych z technologią certyfikatów i świadczenia usług dotyczących podpisu elektronicznego oraz znacznika czasu. Od osób zatrudnionych w CUZ Sigillum wymagane są również wiedza i umiejętności z zakresu obsługi sprzętu i oprogramowania służących do elektronicznego, automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych.

Osoby zatrudnione przy świadczeniu usług zaufania, przed rozpoczęciem pracy, muszą podpisać odpowiednie oświadczenia związane z nieujawnianiem informacji wrażliwych.

Pracownicy nie otrzymują dostępu do pełnienia zaufanych funkcji, dopóki wszelkie, niezbędne kontrole nie zostaną zakończone.

5.3.3. Wymagania szkoleniowe

Wszyscy pracownicy CUZ Sigillum pełniący zaufane role w jej strukturze, są szkoleni w szczególności w zakresie:

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;
5. ustaw i rozporządzeń regulujących pracę CUZ Sigillum;
6. polityk i procedur operacyjnych stosowanych w CUZ Sigillum.

Odbyte szkolenia winny być poświadczone odpowiednymi zaświadczeniami lub certyfikatami.

5.3.4. Wymagania na powtarzanie szkoleń

Dyrektor jednostki organizacyjnej właściwej ds. świadczenia usług zaufania określa plan szkoleń, zapewniający utrzymanie przez personel CUZ Sigillum wysokiego poziomu wiedzy. Plan obejmuje zarówno szkolenia powtarzane, uzupełniające wiedzę, jak i nabywanie nowych umiejętności.

5.3.5. Częstotliwość i sposób rotacji stanowisk

CUZ Sigillum nie realizuje planowej rotacji stanowisk swoich pracowników.

5.3.6. Sankcje za nieuprawnione działania

Z uwagi na fakt, iż wszystkie czynności wykonywane przy świadczeniu usług zaufania są kontrolowanie i dokumentowane możliwe jest wykrycie i udowodnienie ewentualnych nieuprawnionych działań osób zatrudnionych w CUZ Sigillum.

Za nieuprawnione działania CUZ Sigillum może nałożyć na swoich pracowników kary wynikające z Regulaminu Pracy w PWPW S.A., Kodeksu Pracy lub Ustawy.

W przypadku wykonywania przez członków personelu CUZ Sigillum nieuprawnionych działań, mogą się oni narazić również na sankcje wynikające z innych przepisów, w tym m.in. z Ustawy o nieuczciwej konkurencji, Ustawy o ochronie danych osobowych oraz z Kodeksu Karnego.

PWPW S.A. może również dochodzić odszkodowania za poniesione straty na drodze powództwa cywilnego.

5.3.7. Wymagania wobec niezależnych wykonawców

W przypadku wykonywania jakichkolwiek prac na rzecz CUZ Sigillum przez niezależnych kontrahentów, którzy nie są pracownikami CUZ Sigillum wymagane jest:

(1) Podpisanie umowy cywilno-prawnej ściśle określającej:
   (a) zakres wykonywanych prac;
   (b) czas i miejsce ich wykonywania;
   (c) warunki odbioru wykonanych prac (termin odbioru, kryteria jakościowe i ilościowe);
   (d) sankcje za nienależyte lub niewykonanie warunków umowy;
   (e) możliwości audytu i monitorowania personelu kontrahenta;
   (f) odszkodowania za szkody spowodowane działaniami personelu kontrahenta;
   (g) inne zapisu związane z bezpieczeństwem informacji lub jakością świadczonych usług zaufania.

(2) Zobowiązania wykonawcy do spełnienia wymagań bezpieczeństwa obowiązujących w CUZ Sigillum.

(3) Podpisanie przez niezależnego kontrahenta oświadczenia dot. zachowania w poufności wszelkich informacji związanych z wykonywanymi pracami oraz oświadczenia, że wykonawca przyjmuje do wiadomości informacje o sankcjach karnych, jakie grożą za niedotrzymanie klauzuli poufności. Jeżeli na rzecz niezależnego kontrahenta pracuje większa ilość osób, oświadczenia takie musi podpisać każda z tych osób.

Jeżeli będzie zachodziła taka potrzeba CUZ Sigillum przekazuje niezależnemu kontrahentowi zasady dostępu do informacji oraz dopuszczalnego wykorzystania informacji. Wykonawca winien zastać również zapoznany z obowiązującymi w CUZ Sigillum politykami, procedurami czy dokumentami związanymi z bezpieczeństwem informacji oraz świadczonym usługami zaufania. Warunkiem odebrania wykonanych prac przez niezależnego kontrahenta jest podpisaniem bez zastrzeżeń protokołu wykonania i odbioru przez kierownictwo CUZ Sigillum.

5.3.8. Dokumentacja udostępniona personelowi

Personel CUZ Sigillum ma bieżący i bezpośredni dostęp do:

1. wszelkiej odnoszącej się do CUZ Sigillum dokumentacji sprzętu i oprogramowania wykorzystywanego przy świadczeniu usług oznaczonych CUZ Sigillum;
2. Polityki;
3. procedur operacyjnych i zapewniających ciągłość działania obowiązujących w CUZ Sigillum;
4. wzorów umów, wniosków itp. wykorzystywanych przy świadczeniu usług.

Dostęp ten obejmuje zarówno bieżącą, jak i archiwalną dokumentację.

5.4. Procedury kontroli zdarzeń

Wszystkie zdarzenia, istotne z punktu widzenia bezpieczeństwa świadczonych usług zaufania, są przez CUZ Sigillum rejestrowane, przechowywane i audytowane. Zdarzenia objęte procedurą rejestrowania pochodzą zarówno z poszczególnych komponentów samego systemu, jak i czynności wykonywanych przez pracowników CUZ Sigillum.

Rejestry zdarzeń prowadzone są i przechowywane, w szczególności w celu:

1. zapewnienia ciągłości usług;
2. rozliczenia użytkowników i pracowników w zakresie ich działań;
3. kontroli pracowników w zakresie ich działań;
4. dostarczenia dowodów w postępowaniu sądowym. Informacje te są przechowywane w formie elektronicznej.

W CUZ Sigillum wdrożone są procedury w zakresie bezpieczeństwa prowadzonej działalności:

1. monitorowania systemu teleinformatycznego;
2. obsługi rejestrów zdarzeń;
3. postępowania w przypadku naruszenia bezpieczeństwa informacji.

CUZ Sigillum zapewnia poufność zgromadzonych w rejestrach zdarzeń informacji przez stosowanie zabezpieczeń fizycznych, organizacyjnych i proceduralnych.

Rejestry zdarzeń, po okresie wymaganego ich przechowywania, są komisyjnie niszczone, zgodnie z przyjętymi w PWPW S.A. procedurami.

5.4.1. Rodzaje rejestrowanych zdarzeń

Wszystkie istotne elementy infrastruktury CUZ Sigillum prowadzą dzienniki audytu w celu zapewnienia rozliczalności czynności operatorów i administratorów, rejestracji błędów i innych zdarzeń dotyczących bezpieczeństwa informacji w celu wsparcia procesów zarządzania zdarzeniami i incydentami bezpieczeństwa, konfiguracją, pojemnością oraz wykrywania zdarzeń mogących mieć wpływ na dostępność systemów. Dostęp do dzienników zdarzeń podlega kontroli dostępu. Logi i zapisy sesji podlegają ochronie.

Zapisy rejestrów zdarzeń obejmują co najmniej:

1. wszystkie zdarzenia związane z rejestracją, w tym składania wniosków dotyczących uzyskania certyfikatu lub odnowienia certyfikatu;
2. żądania świadczenia usług zaufania normalnie udostępnianych przez system lub usług nie wykonywanych przez system oraz informacji o wykonaniu lub niewykonaniu usługi oraz powód jej niewykonania;
3. istotne zdarzenia związane ze zmianami w środowisku systemu, w tym w podsystemie zarządzania kluczami w szczególności tworzenie kont i rodzaj przydzielanych uprawnień;
4. instalacje nowego oprogramowania lub aktualizacje;
5. rozpoczęcie i przerwanie funkcji rejestrujących zdarzenia;
6. zmiany w konfiguracji funkcji rejestrujących zdarzenia, w tym w szczególności każdą modyfikację lub synchronizację czasu systemowego;
7. czas tworzenia kopii zapasowych;
8. czas archiwizowania rejestrów zdarzeń;
9. zamykanie, otwieranie i ponowne uruchamiania po zamknięciu systemu;
10. nieprzewidziane zdarzenia w działaniu systemu i sprzętu;
11. negatywne wyniki testów;
12. zdarzenia dotyczące komunikacji sieciowej;
13. wszystkie zgłoszenia unieważnienia certyfikatu

Dla poszczególnych zdarzeń zapisywane są przynajmniej:

1. typ zdarzenia;
2. jego identyfikator;
3. datę i czas wystąpienia;
4. informacje związane z powodem wystąpienia zdarzenia;
5. określenie, co do skutków wystąpienia zdarzenia.

Zapisy związane z rejestrowaniem zdarzeń są archiwizowane.

5.4.2. Częstotliwość przeglądania rejestrów zdarzeń

Zdarzenia zapisane w rejestrach są przeglądane przez operatorów (OS) wraz z audytorami (AS) lub inspektorami (IB) co najmniej raz w ciągu doby z wyłączeniem sobót, niedziel oraz dni ustawowo wolnych od pracy. Z fakt dokonania przeglądu jest odnotowywany w dziennikach z przeglądu zdarzeń.

W razie konieczności, np. zaistnienia incydentu, wymagany jest częstszy przegląd rejestrów zdarzeń. Przegląd rejestrów zdarzeń odbywa się głownie pod kątem identyfikacji niepożądanych z punktu widzenia bezpieczeństwa lub jakości świadczonych usług zaufania. Wyniki przeglądu rejestrów zdarzeń odnotowywane są w „Rejestrach przeglądu logów".

Zdarzenia z dzienników systemowych elementów infrastruktury CUZ Sigillum przesyłane są do centralnego systemu, na którym zdefiniowano reguły korelacji zdarzeń z różnych urządzeń. Anomalie w funkcjonowaniu systemu generują powiadomienia do personelu odpowiedzialnego za monitorowanie systemu.

W przypadku zauważenia zdarzeń istotnych z punktu widzenia świadczonych usług, Inspektor Bezpieczeństwa wraz z Operatorem Systemu lub Administratorem Systemu podejmują czynności wyjaśniające to zdarzenia. Jeżeli zauważone zdarzenie związane jest z bezpieczeństwem systemu lub zagraża ciągłości świadczonych usług – dodatkowo sporządzają pisemny „Raport po Incydencie", zgodnie z zasadami obowiązującymi w PWPW S.A..

Inspektor ds. Audytu (IA), po zakończonym miesiącu kalendarzowym, sprawdza kompletność zapisów w „Rejestrach przeglądu logów". Wyniki tego sprawdzenia są dokumentowane w postaci „Raportu Bezpieczeństwa".

Uprawnione osoby dokonują przeglądu rejestru zdarzeń szczególnie pod kątem prób:

1. uniemożliwienia lub zakłócenia działalności CUZ Sigillum w zakresie świadczenia usług zaufania;
2. nieuprawnionego dostępu do systemu teleinformatycznego;
3. nieuprawnionego dostępu do bazy danych;
4. nieuprawnionego dostępu do pomieszczeń CUZ Sigillum.

5.4.3. Okres przechowywania dzienników zdarzeń

Zapisy zdarzeń przechowywane są w miejscu ich powstania przez okres co najmniej dwóch lat i są dostępne w trybie on-line. Po tym czasie rejestry zdarzeń są archiwizowane i udostępniane w trybie off-line.

Zarchiwizowane zdarzenia przechowywane są przez okres min. 3 lat od daty powstania zapisu. Po tym okresie rejestry zdarzeń są niszczone zgodnie z obowiązującymi w CUZ Sigillum procedurami.

5.4.4. Ochrona rejestrów zdarzeń

Rejestry zdarzeń, tak samo jak inne informacje związane z bezpieczeństwem świadczonych usług, podlegają ochronie na takim samym poziomie, jak wszystkie inne związane z działalnością CUZ Sigillum.

W celu ochrony rejestru zdarzeń przed modyfikacją, usunięciem, utratą integralności lub innymi tego typu zdarzeniami w CUZ Sigillum przyjęta zasadę, że żadna z osób wymienionych w Rozdziale 5.2.1 niniejszej Polityki nie może mieć dostępu do rejestru zdarzeń samodzielnie. I tak administratorzy lub operatorzy mają dostęp do rejestrów zdarzeń tylko w obecności jednej z dwóch osób: inspektora lub audytora.

Dostęp do zapisów rejestrów zdarzeń możliwy jest tylko na poziomie ich przeglądania.

5.4.5. Procedury tworzenia kopii zapasowych rejestrów zdarzeń

Procedury bezpieczeństwa dotyczące postępowania z rejestrami zdarzeń wymagają kopiowania zapisów zgodnie z przyjętym harmonogramem – przynajmniej raz w miesiącu. Gdy sytuacja tego wymaga, np. wyłączenia serwera, aktualizacja oprogramowania lub bazy danych, rejestry zdarzeń są zgrywane i kopiowane przed wykonaniem wymaganych czynności.

Przy tworzeniu kopii zapasowych są obecne, co najmniej dwie spośród osób, o których mowa w Rozdziale 5.2.1 niniejszej Polityki.

5.4.6. System zbierania zdarzeń (wewnętrzny i zewnętrzny)

Rejestry zdarzeń ze systemu teleinformatycznego tworzone są automatycznie. Pochodzą z następujących źródeł: system operacyjny, bazy danych oraz wykorzystywane oprogramowanie.

Dodatkowo prowadzone są w formie papierowej dzienniki pracy systemów oraz dzienniki przeglądu rejestrów zdarzeń. Wpisy do tych dokumentów wykonywane są przez odpowiednie, uprawnione osoby.

Wszystkie zapisy związane z prowadzonymi rejestrami są przechowywane w dwóch identycznych egzemplarzach. Jeden egzemplarz znajduje się w ośrodku podstawowym, w którym są świadczone usługi zaufania, drugi poza ośrodkiem podstawowym.

5.4.7. Powiadamianie o zdarzeniach niepożądanych

CUZ Sigillum posiad wdrożony i eksploatowany system monitorowania i powiadamiania o zdarzeniach niepożądanych, mających wpływ na bezpieczeństwo świadczonych usług zaufania. System ten obsługiwany jest przez całą dobę przez Operatorów Systemu. W razie konieczności, w zależności od stopnia krytyczności, powiadamiani są także Administratorzy Systemu oraz Inspektorzy ds. Bezpieczeństwa.

Do zadań powiadomionych osób należy szczegółowe zapoznanie się ze sytuacją, jej analiza i podejmowanie odpowiednich decyzji w celu zapobieżenie skutkom zdarzeń niepożądanych.

5.4.8. Oceny podatności

CUZ Sigillum posiada certyfikat zgodny z normą ISO ICE 27001 na wystawianie i obsługę certyfikatów.

Zgodnie z wymaganiami tej normy CUZ Sigillum przeprowadziło klasyfikację wszystkich swoich aktywów służących do świadczenia usług zaufania. W dalszej kolejności, zgodnie z wymaganiami ww. normy została przeprowadzona analiza podatności aktywów na zagrożenia i oceniono ryzyka z tym związane. Został wdrożony i zaakceptowany przez kierownictwo CUZ Sigillum plan postępowania z ryzykiem.

W PWPW S.A. funkcjonują: komórka audytu wewnętrznego, której zadaniem jest m.in. ocenianie zgodności CUZ Sigillum z wymaganiami normy ISO IEC 27001, a także komórka ds. bezpieczeństwa teleinformatycznego, której zadaniem jest m.in. ocena i analiza podatności oraz reagowanie na incydenty.

5.4.9. Zarządzanie ryzykiem

Zarządzanie ryzykiem to systematyczny i ciągły proces identyfikacji zagrożeń oraz minimalizacji podatności i skutków wystąpienia tych zagrożeń. Zarządzanie ryzykiem ma za zadanie wspieranie procesów decyzyjnych w PWPW S.A., mających na celu dobór środków zmierzających do diagnozowania przyczyn, przeciwdziałania, ograniczenia i sprawnego reagowania na skutki naruszeń, w obszarze zasobów oraz realizowanych procesów CUZ Sigillum.

Raz w roku lub po wprowadzeniu znaczących zmian w procesie (w tym w stosowanej w nim infrastrukturze teleinformatycznej) przeprowadzana jest ocena ryzyka.

Ocena ryzyka wynika z kontekstu organizacji oraz potrzeb biznesowych procesu wystawiania i obsługi certyfikatów, co oznacza, że ryzyka identyfikowane podczas oceny muszą być powiązane z celami biznesowymi procesu.

Lista potencjalnych zagrożeń tworzona jest w oparciu o:

- informacje uzyskane z wcześniejszej sesji analizy ryzyka,
- wyniki audytów wewnętrznych,
- wyniki audytów zewnętrznych,
- raporty z zakresu zgłoszonych incydentów bezpieczeństwa,
- zmiany organizacyjne (np. zmiany struktury organizacyjnej, nowe usługi),
- zmiany techniczne (np. nowe systemy teleinformatyczne, nowy zakres funkcjonalny),
- nowe zagrożenia bezpieczeństwa.

Szczegółowa metodologia wykonania analizy ryzyka oraz sposób postępowania z ryzykiem opisane są w procedurach wewnętrznych PWPW S.A.

5.5. Archiwizacja zapisów

Wszystkie ważne z punku widzenia świadczenia usług zaufania zdarzenia oraz te wymagane przez prawo, są w CUZ Sigillum archiwizowane i kopiowane w dwóch identycznych egzemplarzach na nośniki zewnętrzne.

CUZ Sigillum opracowało i wdrożyło procedury archiwizacji, procedury przechowywania i dostępu do danych archiwalnych.

Archiwum zdarzeń tworzone jest automatycznie, natomiast informacje dotyczące zapisania zdarzeń oraz przeglądu poprawności wykonania kopii prowadzone są przy pomocy tzw. raportów w formie papierowej.

Inspektor ds. audytu zobowiązany jest do przeglądania zapisów związanych z procesem archiwizacji co najmniej raz w miesiącu. Fakt dokonania takiego przeglądu odnotowywany jest w Dzienniku Przeglądu Zdarzeń.

5.5.1. Rodzaje archiwizowanych zapisów

CUZ Sigillum prowadzi archiwum zawierające zapisy związane z:

- działaniami swoich pracowników;
- zdarzeniami mającymi miejsce w systemie teleinformatycznym, które są związane z bezpieczeństwem świadczonych usług zaufania;
- wszystkimi kwalifikowanymi certyfikatami i zaświadczeniami certyfikacyjnymi, których CUZ Sigillum było wystawcą;
- zdarzenia związane z wystawianiem znaczników czasu;
- wszystkimi listami CRL, których CUZ Sigillum było wystawcą;
- umowami o świadczenie usług certyfikacyjnych;
- dokumentami, o których mowa w eIDAS.

Zapisy związane z działaniami pracowników oraz zdarzenia mające miejsce w systemie teleinformatycznym wykonywane są automatycznie.

5.5.2. Okres przechowywania archiwum

Zapisy dzienników zdarzeń i działań pracowników są przechowywane i archiwowane przez okres co najmniej 3 lat. Informacje wymienione w pkt. 5.5.1. są przechowywane przez okres 20 lat od daty utworzenia. Dla certyfikatów CUZ Sigillum i certyfikatów stron ufających okres przechowywania liczony jest od momentu wygaśnięcia tych certyfikatów.

Po okresie przechowywania zarchiwizowane informacje są komisyjnie, w sposób bezpieczny niszczone.

5.5.3. Ochrona archiwum

Nośniki informacji zawierające zarchiwizowane dane są zabezpieczone za pomocą fizycznych i elektronicznych metod kontroli dostępu. Są one również 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.

Dostęp do archiwów mają tyko osoby związane z pełnieniem funkcji zaufania w systemie CUZ Sigillum.

Dostęp do zarchiwizowanych informacji możliwy jest tylko na poziomie ich przeglądania.

5.5.4. Procedury tworzenia kopii zapasowych archiwum

CUZ Sigillum opracowało i wdrożyło procedury tworzenia zasobów archiwalnych i zarządzania tymi zasobami. W szczególności procedury te dotyczą:

1. klasyfikacji zasobów;
2. przetwarzania informacji;
3. zapewnienia bezpieczeństwa dla archiwów.

5.5.5. 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 5.5.1.

5.5.6. System zbierania archiwum (wewnętrzny i zewnętrzny)

Kopie archiwalne są wykonywane przez Operatorów Systemu i zapisywane na zewnętrznych nośnikach danych jednokrotnego zapisu (WORM) w dwóch identycznych egzemplarzach.

Wszystkie zapisy związane z prowadzonymi archiwami są przechowywane w dwóch identycznych egzemplarzach. Jeden egzemplarz znajduje się w ośrodku podstawowym, w którym są świadczone usługi zaufania, drugi poza ośrodkiem podstawowym.

5.5.7. Procedury dostępu i weryfikacji zarchiwizowanych informacji

W celu sprawdzenia poprawności zarchiwizowania informacji na nośnikach zewnętrznych w CUZ Sigillum testowana jest poprawność wykonanych zapisów. Czynność ta wykonywana jest codziennie przez Operatora Systemu pod nadzorem Inspektora ds. Bezpieczeństwa na wybranych losowo obiektach. Informacja o poprawności wykonania zapisu i jego odczytu odnotowywana jest w odpowiednich rejestrach.

Wybrane informacje z archiwum mogą być udostępniane odpowiednim organom jedynie na podstawie art. 15 ust. 4 Ustawy.

5.6. Wymiana kluczy urzędu

Wymiana kluczy w CUZ Sigillum nie jest wykonywana automatycznie. Klucze wygasają zgodnie z terminem ważności certyfikatu dostawcy usług zaufania wystawionego dla CUZ Sigillum przez ministra właściwego ds. informatyzacji.

Klucze są wymieniane odpowiednio wcześnie przed upłynięciem ich terminu ważności, tak, aby okres ważności żadnego z certyfikatów wystawionych przy użyciu tych kluczy nie przekraczał okresu ważności kluczy.

Po wygaśnięciu certyfikatu dostawcy usług zaufania zawierającego stary klucz publiczny CUZ Sigillum, związany z nim klucz prywatny jest niszczony za pomocą przyjętych w CUZ Sigillum odpowiednich procedur.

Po wymianie kluczy CUZ Sigillum używa dla świadczenia usług zaufania tylko i wyłącznie nowego klucza prywatnego.

5.7. Naruszenie bezpieczeństwa kluczy urzędu i procedury odtwarzania po awarii

CUZ Sigillum opracowało i wdrożyło szczegółową procedurę zapewnienia ciągłości funkcjonowania obejmującą sytuację kompromitacji klucza prywatnego CUZ Sigillum, awarie sprzętu, oprogramowania i linii komunikacyjnych oraz naturalne katastrofy takie jak pożar i powódź. Opracowana jest również dokumentacja opisująca podstawową konfigurację sprzętu, systemów operacyjnych, oprogramowania użytkowego, oprogramowania antywirusowego i specyficznego oprogramowania PKI.

CUZ Sigillum posiada również stosowne procedury obsługi kopii zapasowych i archiwalnych oraz procedury przechowywania danych poza swoją siedzibą.

CUZ Sigillum przeprowadza także regularne szkolenia swojego personelu dotyczące procedur postępowania w sytuacjach awaryjnych o negatywnym znaczeniu dla swojej działalności oraz testy przełączenia pracy na ośrodek zapasowy.

Niezależnie od procedur związanych za zachowaniem ciągłości działania, w CUZ Sigillum przygotowane są również procedury powiadamiania organów nadzoru i subskrybentów o takich zdarzeniach.

Wszystkie zdarzenia mogące mieć wpływ na powstanie incydentu, a możliwe do przewidzenia są na bieżąco monitorowane i kontrolowane.

5.7.1. Procedury obsługi incydentów

Procedura obsługi incydentów określa zasady obsługi incydentów związanych z bezpieczeństwem informacji. Obsługa incydentu ma na celu podjęcie niezbędnych działań, które usuną lub zminimalizują skutki zaistnienia incydentu lub przywrócą stan sprzed incydentu. W CUZ Sigillum zostały zidentyfikowane i skatalogowane potencjalne zagrożenia mogące mieć istotny wpływ na ciągłość świadczonych usług zaufania. Są to między innymi:

- kompromitacja kluczy prywatnych urzędu;
- fizyczne lub logiczne uszkodzenie jakiegokolwiek elementu systemu teleinformatycznego służącego do świadczenia usług zaufania;
- utrata zewnętrznych usług sieciowych;
- awaria zasobów obliczeniowych, oprogramowania lub danych;
- utrata zasilania;
- wykrycie desynchronizacji czasu powyżej 1 sekundy względem czasu wzorcowego UTC;
- katastrofy wynikające z przyczyn naturalnych.

Na potrzeby obsługi zagrożeń, incydentów i katastrof w CUZ Sigillum opracowany został plan zapewnienia ciągłości świadczonych usług. Przygotowane są procedury umożliwiające pracę w ośrodku zapasowym dla części lub całości systemu, procedury związane z archiwizacją i kopiowaniem systemu oraz procedury dotyczące odtworzenia systemu po zdarzeniach.

Procedury obsługi incydentów obejmują również tryb ich zgłaszania. Dla potrzeb zgłaszania incydentów uruchomiona jest specjalna linia telefoniczna oraz wewnętrzna strona intranetowa.

5.7.2. Awaria zasobów obliczeniowych, oprogramowania lub danych

CUZ Sigillum 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 CUZ Sigillum.

Aby zminimalizować skutki awarii swoich zasobów teleinformatycznych CUZ Sigillum podjęło następujące działania:

- opracowało i wdrożyło procedurę powiadamiania o zdarzeniach zarówno organów nadzoru, jak i subskrybentów;
- posiada plan pracy w sytuacjach awaryjnych oraz procedury przywracania systemu po katastrofie;
- regularnie tworzy kopie (w dwóch identycznych egzemplarzach) całego systemu, które obejmują oprogramowanie systemowe, użytkowe oraz dane;
- stosuje odpowiednią do potrzeb ilość kluczy, które przechowywane są w różnych miejscach;
- okresowo testuje plany odtworzenia swojej pracy oraz testuje możliwości odtworzenia informacji z kopii zapasowych i archiwalnych;
- wszystkie zmiany w systemie, dotyczące zarówno sprzętu, jak i oprogramowania, są dokumentowane i kontrolowane;
- podpisało stosowne umowy na konserwację sprzętu i oprogramowania z ich dostawcami bądź producentami;
- okresowo i regularnie dokonuje przeglądów systemów wspomagających (zasilani, klimatyzacja itp.).

5.7.3. Procedury w przypadku kompromitacji kluczy prywatnych

W przypadku kompromitacji kluczy prywatnych urzędów świadczących usługi zaufania CUZ Sigillum uruchamia stosowne procedury, które obejmują m.in.:

- wygenerowanie nowych kluczy prywatnych urzędu;
- niezwłoczne powiadomienie wszystkich Subskrybentów o zaistniałym zdarzeniu;
- unieważnienie dotychczasowego certyfikatu dostawcy usług zaufania, związanego ze skompromitowanym kluczem;
- unieważnione zostają wszystkie certyfikaty i certyfikaty dostawcy usług zaufania, znajdujące się na ścieżce certyfikacyjnej związanej ze skompromitowanym urzędem;
- w miejsce unieważnionych certyfikatów i certyfikatów dostawcy usług zaufania zostają wygenerowane nowe, które przesłane zostaną do subskrybentów na koszt CUZ Sigillum.

5.7.4. Zachowanie ciągłości działania

CUZ Sigillum opracowało i wdrożyło plan postępowania obejmujący:

- procedury zapewniające plan ciągłości działania;
- procedury wykonywania kopii zapasowych oraz archiwalnych oraz zasady przechowywania tych kopii poza siedzibą CUZ Sigillum.

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

Klucze prywatne urzędów i usług są zaimportowane do urządzeń kryptograficznych w ośrodku podstawowym i zapasowym, i skojarzone z certyfikatem danej usługi lub urzędu.

Zarówno możliwości odtworzenia informacji z kopii zapasowych, jak i funkcjonowanie ośrodka zapasowego są regularnie testowane.

Po każdym przywróceniu systemu po katastrofie do normalnego stanu, Inspektor ds. Bezpieczeństwa wraz z Administratorem Systemu:

- sprawdzają kompletność i poprawność działania systemu;
- analizują przyczyny i skutki zaistniałej katastrofy;
- informują organ nadzoru i subskrybentów o skutkach katastrofy;
- weryfikują i aktualizują analizę ryzyka związaną ze świadczeniem usług zaufania;
- przeglądają i aktualizują stosowne polityki i procedury pod kątem zapewnienia bezpieczeństwa informacji na przyszłość na wypadek wystąpienia podobnych zdarzeń.

5.8. Zakończenie działalności CUZ Sigillum lub punktów rejestracji

Jeśli wystąpi potrzeba zakończenia działalności CUZ Sigillum lub jednej z oferowanych usług zaufania, powinno się zapewnić minimalizowanie skutków tego faktu dla odbiorców usług certyfikacyjnych, w takim stopniu, w jakim to będzie możliwe.

5.8.1. Czynności przewidziane do wykonania przez CUZ Sigillum

W przypadku planowego zakończenia działalności CUZ Sigillum, CUZ Sigillum niezwłocznie informuje o tym fakcie ministra właściwego ds. informatyzacji oraz Punkty Rejestracji, z wyprzedzeniem co najmniej trzech miesięcy, wraz z przekazaniem informacji o ewentualnym następcy, który mógłby przejąć obsługę Subskrybentów.

Powiadamia wszystkich subskrybentów związanych z urzędem kończącym działalność o zamiarze jej zakończenia. Natomiast tych, którzy posiadają ważne certyfikaty, a wydany przez urząd kończący działalność, z wyprzedzeniem co najmniej trzech miesięcy. W takim przypadku

Punkty Rejestracji mogą proponować Subskrybentom pomoc przy wystąpieniu z wnioskiem o wystawienie certyfikatu do następcy CUZ Sigillum.

CUZ Sigillum, w miarę możliwości, uczyni wszystkiego co możliwe, aby zakończenie działalności w świadczeniu usług spowodowało minimalne szkody w działalności subskrybentów. Jeżeli będzie to możliwe CUZ Sigillum zwraca subskrybentom koszty wydanego certyfikatu, w wysokości proporcjonalnej do pozostałego okresu ważności wydanego certyfikatu.

Zgodnie z wymaganiami Ustawy CUZ Sigillum jest ubezpieczone od odpowiedzialności cywilnej na wypadek wyrządzenia szkód odbiorcom usług zaufanych.

5.8.2. Klucze i certyfikaty subskrybentów

W przypadku zakończenia działalności przez CUZ Sigillum:

1. wszystkie certyfikaty wystawione przez CUZ Sigillum stracą ważność;
2. certyfikat usługi znakowania czasem zostanie unieważniony;
3. zgodnie z obowiązującym prawem, nie będzie możliwości automatycznego „przeniesienia" Subskrybentów do innego Centrum Certyfikacji Elektronicznej.

6. Techniczne środki zabezpieczeń

6.1. Generacja i instalacja par kluczy

Bezpieczeństwo generacji oraz instalacji pary kluczy zapewniają procedury operacyjne stosowane w CUZ Sigillum.

6.1.1. Generacja par kluczy

Pary kluczy wszystkich urzędów CUZ Sigillum generowane są zgodnie z udokumentowaną procedurą generacji, zapewniającą integralność i poufność kluczy. Generacja pary kluczy odbywa się w siedzibie CUZ Sigillum w środowisku bezpiecznym fizycznie, w obecności co najmniej dwóch uprawnionych osób pełniących zaufane role, przy czym jedną z nich musi być Inspektor ds. bezpieczeństwa. Z czynności wykonywanych podczas generacji kluczy sporządzany jest raport, który jest podpisywany przez wszystkich uczestników procedury generacji kluczy. Inspektor ds. bezpieczeństwa zaświadcza swoim podpisem na wspomnianym, że proces generowania kluczy przebiegał zgodnie z udokumentowaną procedurą z zachowaniem poufności i integralności kluczy.

Para kluczy Subskrybenta przeznaczona dla kart kryptograficznych może być generowana jedynie przez Inspektora ds. Rejestracji

Parametry generowanych kluczy muszą spełniać wymagania postawione w normie ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" lub w przepisach krajowych.

Dopuszcza się wydanie certyfikatów pieczęci i TLS na podstawie żądania wygenerowanego przez Zamawiającego .

6.1.2. Dostarczenie klucza prywatnego subskrybentowi

Po wygenerowaniu kluczy w CUZ Sigillum są on dostarczone Subskrybentowi wraz z informacjami pozwalającymi na aktywację klucza prywatnego, Subskrybent ma obowiązek do niezwłocznej zmiany danych pozwalających na aktywację klucza prywatnego.

6.1.3. Dostarczenie klucza publicznego do wydawcy certyfikatu

Klucze publiczne Subskrybentów są dostarczane z Punktu rejestracji w postaci zgłoszenia certyfikacyjnego, podpisanego przez Inspektora ds. rejestracji.

6.1.4. Dostarczenie klucza publicznego CA do podmiotów ufających

Klucz publiczny CUZ Sigillum może być pobrany przez Subskrybenta z Punktu Rejestracji, przy okazji rejestracji Subskrybenta.

6.1.5. Parametry kluczy

Niekwalifikowane urzędy certyfikacji CUZ Sigillum używają kluczy:

- dla urzędu nadrzędnego „CUZ Sigillum Root CA1” - klucz o długości RSA 4096 bitów.
- dla urzędu „CUZ Sigillum CA1” klucz o długości 4096 bitów,
- usługa OCSP – klucz o długości 2048 bitów.

Długość kluczy używanych przez użytkowania końcowego wynosi **RSA 2048 bitów lub EC 384 bity (krzywa NIST P384).**

Klucze prywatne wykorzystywane przez urzędy certyfikacji oraz do świadczenia usług przez CUZ Sigillum są przechowywane w modułach kryptograficznych, których poziom zabezpieczeń jest określony w rozdziale 6.1.19.

Długość kluczy używanych przez Inspektorów ds. rejestracji wynosi **RSA 2048 bitów lub EC 384 bity (krzywa NIST P384).**

O ile przepisy prawa nie stanowią inaczej, algorytmy kryptograficzne stosowane przy generowaniu kluczy powinny spełniać minimalne wymagania określone w dokumencie ETSI TS 119 312 „Electronic Signatures and Infrastructures; Cryptographic Suites”.

6.1.6. Parametry generowania klucza publicznego i kontrola jakości

Klucze publiczne urzędów CUZ Sigillum generowane są za pomocą sprzętowych modułów kryptograficznych, które zapewniają odpowiednią jakość otrzymywanych kluczy.

6.1.7. Zastosowanie kluczy

Sposób użycia klucza zdefiniowany jest w polu *KeyUsage* oraz *ExtendedKeyUsage* rozszerzeń standardowych certyfikatu (X.509 v3). Pole powinno być weryfikowane przez aplikacje korzystające z certyfikatu.

Klucze urzędu są używane wyłącznie do podpisywania certyfikatów Subskrybentów i podpisywania list CRL.

Klucze OCSP są używane wyłącznie do podpisywania odpowiedzi OCSP.

6.1.8. Standardy i kontrola modułu kryptograficznego

W infrastrukturze urzędów CUZ Sigillum stosowany jest sprzętowy moduł kryptograficzny spełniającym wymagania klasy oraz Common Criteria EAL4+. Moduł kryptograficzny został dostarczony do CUZ Sigillum w fabrycznym opakowaniu z plombami w stanie nienaruszonym, a także numerem seryjnym i wersją firmware potwierdzonymi przez producenta. Okresowa kontrola moduły polega na wzrokowym zweryfikowaniu nienaruszalności plomb, kontroli numeru seryjnego oraz komunikatów na wyświetlaczu urządzenia. Przy każdym uruchomieniu modułu kryptograficznego następuje autokontrola urządzenia.

6.1.9. Kontrola klucza prywatnego przez wiele osób

Klucze prywatne wszystkich urzędów CUZ Sigillum są chronione przez podział klucza na części, tak zwane sekrety, zgodnie z wymogami Rozporządzenia. CUZ Sigillum stosuje metodę pośrednią podziału klucza, w której na części dzielony jest klucz symetryczny, którym zaszyfrowano klucz prywatny. Do odtworzenia klucza wymagana jest określona liczba sekretów współdzielonych, tworząc tak zwany próg. Sekrety współdzielone zapisywane są na kartach elektronicznych i chronione są hasłem.

6.1.10. Deponowanie klucza prywatnego

Nie dopuszcza się możliwości składania kluczy prywatnych urzędów CUZ Sigillum, Inspektorów ds. rejestracji, kluczy prywatnych infrastruktury oraz Subskrybentów w depozyt.

6.1.11. Kopia zapasowa klucza prywatnego

CUZ Sigillum tworzy kopie kluczy prywatnych urzędów na wypadek awaryjnej procedury odzyskiwania kluczy. Kopie zapasowe kluczy są przechowywane są w postaci zaszyfrowanej

kluczem symetrycznym, który jest podzielony na sekrety współdzielone. Sekrety przechowywane są w sejfach w bezpiecznych strefach, dostęp do nich posiada wyłącznie upoważniony personel pełniący zaufane role. Dostęp do zapasowych zestawów sekretów wymaga podwójnej kontroli.

CUZ Sigillum nie tworzy kopii zapasowych kluczy prywatnych infrastruktury, Inspektorów ds. rejestracji oraz Subskrybentów.

6.1.12. Archiwizacja klucza prywatnego

Nie dopuszcza się archiwizacji żadnych kluczy prywatnych służących do składania podpisu elektronicznego lub uwierzytelnienia przy wykorzystywaniu kluczy infrastruktury:

1. klucza prywatnego CUZ Sigillum służącego do poświadczania certyfikatów, OCSP, list CRL;
2. kluczy prywatnych Inspektorów ds. rejestracji, służących do podpisywania zgłoszeń certyfikacyjnych;
3. kluczy prywatnych Subskrybentów.

6.1.13. Transfer klucza prywatnego do/z modułu kryptograficznego

Klucz prywatny w postaci jawnej może być przetwarzany wyłącznie w module kryptograficznym. Transfer kluczy prywatnych urzędów CUZ Sigillum do modułu kryptograficznego następuje w procedurze ładowania kluczy. Klucz w postaci jawnej nie jest transferowany poza moduł kryptograficzny.

6.1.14. Przechowywanie klucza prywatnego w module kryptograficznym

Klucz prywatny przechowywany jest w pamięci moduły kryptograficznego w postaci jawnej tylko w czasie trwania sesji aplikacji modułu kryptograficznego.

6.1.15. Sposób aktywacji klucza prywatnego

Materiał kryptograficzny zawierający klucze przechowywany jest w systemie plików w postaci zaszyfrowanej. Aktywacja kluczy prywatnych urzędów CUZ Sigillum wymaga współdziałania dwóch osób pełniących zaufaną rolą, przy czym jedną z nich musi być Inspektor ds. bezpieczeństwa, posiadających współdzielone sekrety na kartach elektronicznych oraz hasła do tych kart.

Aktywacja klucza prywatnego Subskrybenta oraz Inspektora ds. Rejestracji wymaga znajomości kodu PIN do wykorzystywanego przez niego komponentu technicznego. Kod PIN jest przekazywany Subskrybentowi w bezpieczny sposób.

6.1.16. Sposób dezaktywacji klucza prywatnego

Dezaktywacja kluczy prywatnych urzędów CUZ Sigillum następuje pod kontrolą Inspektora ds. bezpieczeństwa. Dezaktywacja klucza prywatnego polega na zakończeniu działania aplikacji modułu kryptograficznego w systemie operacyjnym.

Dezaktywacja klucza prywatnego Subskrybenta oraz Inspektora ds. rejestracji następuje w wyniku zakończenia działania aplikacji korzystającej z klucza.

6.1.17. Sposób zniszczenia klucza prywatnego

Klucze prywatne wszystkich urzędów i usług CUZ Sigillum są niszczone wraz z fizycznym zniszczeniem kart zawierających sekrety współdzielone. Z czynności wykonywanych podczas niszczenia kluczy sporządzany jest raport, który jest podpisywany przez wszystkich uczestników procedury zniszczenia.

Klucz prywatny Subskrybenta oraz Inspektora ds. rejestracji jest niszczony wraz z fizycznym zniszczeniem komponentu technicznego lub modułu kluczowego, na którym się znajduje, lub też poprzez nadpisanie pamięci komponentu technicznego lub modułu kluczowego ciągiem zer.

6.1.18. Poziom zabezpieczeń oferowany przez moduł kryptograficzny

W infrastrukturze urzędów CUZ Sigillum stosowany jest sprzętowy moduł kryptograficzny spełniającym wymagania klasy Common Criteria EAL4+.

6.1.19. Archiwizacja klucza publicznego

Wszystkie klucze publiczne są archiwizowane przez CUZ Sigillum. Certyfikaty, których okres ważności wygasł, są archiwizowane przez okres, co najmniej 20 lat od daty powstania.

6.1.20. Okresy funkcjonowania certyfikatów i okresy funkcjonowania par kluczy

Okresy ważności certyfikatów niekwalifikowanych CUZ Sigillum oraz certyfikatów Subskrybentów, wynoszą nie więcej niż:

- 25 lat dla certyfikatu CUZ Sigillum Root CA1
- 10 lat dla certyfikatów CUZ Sigillum CA1
- 2 lata dla certyfikatów Subskrybentów.

Czas początku ważności certyfikatu CUZ Sigillum oraz certyfikatu Subskrybentów nie może być wcześniejszy niż moment ich wytworzenia.

Okres ważności klucza prywatnego może być krótszy niż okres ważności certyfikatu.

6.1.21. Odnawianie certyfikatów CUZ Sigillum

CUZ Sigillum z odpowiednim wyprzedzeniem czasowym przed wygaśnięciem obecnego certyfikatu usług zaufania urzędu odpowiedzialnego za wystawianie certyfikatów niekwalifikowanych przeprowadza procedurę wygenerowania nowego certyfikatu usług zaufania z poziomu urzędu głównego. Generacja nowego certyfikatu usług zaufania dla urzędu odpowiedzialnego za wystawianie certyfikatów niekwalifikowanych następuje co najmniej 2 lata przed wygaśnięciem obecnego zaświadczenia.

CUZ Sigillum z odpowiednim wyprzedzeniem czasowym przed wygaśnięciem obecnego certyfikatu usług zaufania urzędu głównego przeprowadza procedurę wygenerowania nowego certyfikatu usług zaufania z poziomu urzędu głównego. Generacja nowego certyfikatu usług zaufania dla urzędu głównego następuje co najmniej 10 lat przed wygaśnięciem obecnego zaświadczenia.

6.2. Dane aktywacyjne

Dane aktywujące stosowane są przez Subskrybentów, inspektorów ds. rejestracji oraz przez upoważnione osoby obsługujące urzędy certyfikacji. Dane aktywujące występują w postaci kodów PIN lub haseł i służą do aktywowania kluczy prywatnych.

6.2.1. Generacja i instalowanie danych aktywacyjnych

Dane aktywujące sekrety współdzielone CUZ Sigillum – w postaci kodów haseł – są określane zgodnie z procedurami opracowanymi i wdrożonymi przez CUZ Sigillum.

Dane aktywujące kluczy Subskrybenta są:

1. określane przez Subskrybenta – jeśli to on generuje parę kluczy;
2. określane przez Inspektora ds. rejestracji – jeśli para kluczy jest generowana w Punkcie rejestracji – w takim przypadku dane te najszybciej jak to tylko jest praktyczne i możliwe, powinny być zmienione przez Subskrybenta.
3. określane przez Subskrybenta – jeśli para kluczy generowana jest w procesie prepersonalizacji w bezpiecznym środowisku – w takim przypadku dane do aktywacji, powinny być ustawione przez Subskrybenta na podstawie pinu aktywacyjnego dostarczanego w bezpieczny sposób po zalogowaniu się Subskrybenta do systemu CUZ Sigillum.

6.2.2. Ochrona danych aktywacyjnych

Za ochronę danych aktywujących klucze urzędów CUZ Sigillum odpowiedzialna są osoby uprawnione do posługiwania się tymi danymi.

Subskrybenci i Inspektorzy ds. rejestracji są odpowiedzialni za poziom ochrony swojego hasła aktywacyjnego. Hasło to powinno być przechowywane w miejscu bezpiecznym i niedostępnym dla osób trzecich. Hasło nie może być przekazywane osobom trzecim.

6.2.3. Pozostałe aspekty dotyczące danych aktywacyjnych

Nie dotyczy.

6.3. Zarządzanie bezpieczeństwem systemu informatycznego

W CUZ Sigillum obowiązuje polityka bezpieczeństwa PWPW S.A. Dokument Szczegółowej Polityki Bezpieczeństwa Informacji w PWPW S.A. został zatwierdzony przez Zarząd PWPW S.A., opublikowany i zakomunikowany pracownikom oraz właściwym stronom zewnętrznym poprzez udostępnienie na oficjalnej stronie internetowej PWPW S.A. Wszelkie zmiany w dokumencie polityki są udostępniane zainteresowanym stronom. Przegląd Polityki oraz inwentaryzacja aktywów odbywa się w ramach Zintegrowanego Systemu Zarządzania. Zmiany Polityki wymagają akceptacji Zarządu PWPW S.A.

W systemie teleinformatycznym CUZ Sigillum wykorzystuje się wiarygodne oprogramowanie i sprzęt. Wdrożono zestaw procedur zapewniających bezpieczną eksploatację.

6.3.1. Specjalne wymagania techniczne odnośnie bezpieczeństwa komputerów

Zostały wdrożone techniczne i środowiskowe mechanizmy bezpieczeństwa obejmujące kwestie dotyczące bezpieczeństwa komputerów specyficzne dla działalności CUZ Sigillum. Zabezpieczenia są realizowane w aplikacjach, systemach operacyjnych, sieci teleinformatycznej oraz zabezpieczeniach fizycznych.

6.3.2. Poziom zabezpieczeń komputerów

Zabezpieczenia komputerów stosowane w infrastrukturze CUZ Sigillum spełniają wymagania stawiane systemom eksploatowanym w PWPW S.A.

6.3.3. Zabezpieczenie sieci teleinformatycznej

Sieć teleinformatyczna CUZ Sigillum została podzielona na segmenty przy użyciu zapór sieciowych, na których dodatkowo zostały uruchomione moduły wykrywające włamania. Reguły na zaporach sieciowych pozwalają tylko na zdefiniowany ruch, poprzez listy kontroli dostępu,

pozostałe połączenia są odrzucane. Zapisy zdarzeń sieciowych są regularnie monitorowane przez personel pełniący zaufane role.

Zmiany reguł na zaporach sieciowych wymaga formalnej akceptacji wniosku o zmianę, która odbywa się wedle udokumentowanej procedury zarządzania zmianą. Zarządzanie zaporami sieciowymi odbywa się zgodnie z zasadą czworga oczu (podwójna kontrola). Reguły na zaporach sieciowych są przeglądane przez personel pełniący zaufane role, nie rzadziej niż raz na kwartał lub po wystąpieniu incydentu bezpieczeństwa.

Komunikacja pomiędzy komponentami wchodzącymi w skład CUZ Sigillum jest zabezpieczona za pomocą dwustronnego protokołu SSL/TLS z uwierzytelnieniem klienta.

6.3.4. Uprawnienia użytkowników

Nadanie uprawnień użytkownikom w systemie teleinformatycznym CUZ Sigillum wymaga formalnej akceptacji wniosku zgodnie z udokumentowaną procedurą zarządzania uprawnieniami. Konfiguracja praw dostępu odbywa się w oparciu o zasadę najmniejszych uprawnień oraz podział ról. Konta użytkowników, którzy zmienili stanowisko lub zakończyli zatrudnienie są niezwłocznie modyfikowane lub blokowane.

6.3.5. Zarządzanie zmianami

Wszelkie zmiany w konfiguracji systemów teleinformatycznych oraz oprogramowaniu są identyfikowane, rejestrowane, kategoryzowane, priorytetyzowane, opiniowane, oceniane, zatwierdzane i wdrażane zgodnie z procedurą zarządzania zmianą. Decyzję o wdrożeniu zmiany podejmuje rada ds. zmian (CAB) na podstawie opinii przygotowanych przez przedstawicieli poszczególnych komórek organizacyjnych, w tym komórki ds. bezpieczeństwa IT.

6.3.6. Zabezpieczenie przed szkodliwym oprogramowaniem

Zabezpieczenie przed szkodliwym oprogramowaniem jest realizowane przez zabezpieczenia techniczne (separacja systemów, oprogramowanie antywirusowe oraz uniemożliwienie instalacji aplikacji przez nieupoważnionych użytkowników) i organizacyjne (zwiększanie świadomości użytkowników, wewnętrzne instrukcje opisujące sposób postępowania w przypadku infekcji złośliwym kodem), których zadaniem jest ograniczenie ryzyka infekcji przez złośliwe oprogramowanie.

6.3.7. Zarządzanie aktualizacjami bezpieczeństwa

Systemy teleinformatyczne CUZ Sigillum są regularnie skanowane pod kątem luk bezpieczeństwa przy użyciu skanerów podatności. Dodatkowo systemy przed oddaniem do eksploatacji oraz po znaczących zmianach poddawane są testom penetracyjnym.

Zidentyfikowane podatności podlegają ocenie a następnie podejmowane są odpowiednie środki w celu przeciwdziałania związanemu z nim ryzyku zgodnie z opracowaną i wdrożoną instrukcją zarządzania podatnościami. Czas reakcji na zidentyfikowane krytyczne podatności wynosi maksymalnie 48 godzin.

6.4. Zarządzanie bezpieczeństwem cyklu życia procesu wytwórczego

Zasady kontroli technicznej cyklu życia zostały określone w procedurach operacyjnych stosowanych przez CUZ Sigillum.

Aplikacje Subskrybentów oraz aplikacje CUZ są tworzone w kontrolowanym środowisku stosującym odpowiednie procedury zarządzania jakością, które gwarantują integralność oprogramowania oraz kontrolę ich wersji.

Zgodnie z wymaganiami bezpieczeństwa dla systemu, na każdym etapie prac projektowych bierze udział przedstawiciel działu bezpieczeństwa teleinformatycznego, którego zadaniem jest ocena bezpieczeństwa implementowanego rozwiązania. System przed oddaniem do eksploatacji oraz okresowo jest poddawany niezależnym i wiarygodnym testom penetracyjnym.

7. Profil certyfikatu i list CRL

Profile certyfikatów niekwalifikowanych są zgodne z formatami opisanymi normą ITU-T X.509. oraz ITU-T X.520. Dodatkowo certyfikaty wydawane są zgodnie z profilami certyfikatów zdefiniowanymi w normie **ETSI EN 319 412-1 oraz** ETSI EN 319 412-2 definiujących profile certyfikatów dla osób fizycznych.

7.1. Struktura Certyfikatu

W ramach Polityki CUZ Sigillum wystawia certyfikaty kwalifikowane zawierające następujące elektroniczne struktury danych:

1. Treść certyfikatu (**tbsCertificate**)
2. Informacja o algorytmie użytym do podpisania certyfikatu (**signatureAlgorithm**)
3. Poświadczenie certyfikatu, składane przez organ wydający certyfikat (**signatureValue**)

Opis poszczególnych struktur przedstawiono poniżej.

7.1.1. Treść certyfikatu

Zgodnie ze standardem X.509 na treść certyfikatu składają się pola standardowe i rozszerzone.

Zakres i wartość **pól standardowych** certyfikatów CUZ Sigillum przedstawiono w tabeli:

L.p.	Pole	Opis	Zawartość
1	Version	wersja formatu certyfikatu zgodnie z X.509	V3
2	Serial Number	numer seryjny certyfikatu, unikalny w ramach urzędu wydającego certyfikatu	--
3	Signature	informacja o algorytmie użytym do podpisania certyfikatu	--
4	Issuer	identyfikator (nazwa DN) wydającego certyfikat	Dla urzędu CUZ Sigillum CA1 CN=CUZ Sigillum CA1, O=Polska Wytwórnia Papierów Wartościowych S.A., OU=Centrum Usług Zaufania Sigillum, C=PL
5	Validity	data ważności certyfikatu, określona jako data i czas początku okresu ważności certyfikatu (notBefore) oraz data i czas końca okresu ważności certyfikatu (notAfter)	--
6	Subject	identyfikator (nazwa DN) właściciela certyfikatu	Lista pól wchodzących w skład DN została opisana w rozdziale **Błąd! Nie można odnaleźć źródła odwołania.**
7	SubjectPublicKeyInfo	określenie algorytmu używanego przez właściciela certyfikatu oraz jego klucz publiczny	--

7.1.2.Struktura pola Subject (nazwa DN)

W ramach Polityki CUZ Sigillum wystawia certyfikaty niekwalifikowane dla osób prywatnych, jak również dla osób będących przedstawicielami firm. Pole Subject może zawierać następujące informacje:

1) CN, Common Name

   Pole to jest obowiązkowe i zawiera nazwę użytkownika. Domyślnie zawartość tego pola zawiera następujące informacje:

   a) Imię i nazwisko subskrybenta albo pseudonim
   b) Rolę subskrybenta, jeśli została wprowadzona

2) Serial number

   Pole to jest obowiązkowe i zawiera unikalny identyfikator subskrybenta w formacie zgodnym z normą ETSI 319 412 – 1. Dostępne są następujące identyfikatory:

   Semantyczne

   a) Dowód osobisty
   b) Paszport
   c) PESEL
   d) NIP

   Niesemantyczne:

   a. identyfikator własny

3) Surname

   Pole to jest wypełniane, jeśli wybrano opcję, by certyfikat zawierał imię i nazwisko subskrybenta. Pole zawiera wówczas nazwisko subskrybenta. Pole to nie może występować łącznie z polem pseudonym.

4) Given Name

   Pole to jest wypełniane, jeśli wybrano opcję, by certyfikat zawierał imię i nazwisko subskrybenta. Pole zawiera wówczas imię subskrybenta. Pole to nie może występować łącznie z polem pseudonym.

5) Pseudonym

   Pole to jest wypełniane, jeśli wybrano opcję, by certyfikat zawierał pseudonim subskrybenta. Pole to nie może występować łącznie z polem Surname ani GivenName.

6) Title

   Pole to jest wypełniane, jeśli wybrano opcję, by certyfikat zawierał „Identyfikator certyfikatu". W szczególności może to być informacja o roli subskrybenta.

7) C, Country

Pole to jest obowiązkowe i zawiera dwuliterowy kod kraju związany z lokalizacją subskrybenta zgodny z normą ISO 3166-1

8) L, Locality *

Pole opcjonalne, zawierające informację o miejscowości związanej z lokalizacją subskrybenta lub zamawiającego

9) O, Organization

Pole to jest wypełniane w przypadku certyfikatu dla subskrybenta występującego w kontekście organizacji. Zawiera nazwę organizacji

10) Organization Identifier

Pole to jest wypełniane w przypadku certyfikatu dla subskrybenta występującego w kontekście organizacji. Pole to zawiera identyfikator VAT organizacji.

11) OU, Organizational Unit

12) postalAddress

Pole to jest wypełniane w przypadku certyfikatu dla subskrybenta występującego w kontekście organizacji. Pole to zawiera pełny adres organizacji, tj.:

- kod pocztowy
- miejscowość
- ulica
- numer domu
- numer lokalu

7.1.3. Pola rozszerzone certyfikatu

1. Authority Information Access – niekrytyczne

   Rozszerzenie zawiera wskazanie lokalizacji i metody dostępu do informacji lub usług udostępnianych przez wystawcę certyfikatu, w którym zawarte jest to rozszerzenie. Zawiera dwie informacje:

   - OCSP – adres usługi OCSP
   - CaIssuers – adres, pod jakim dostępny jest certyfikat organu wydającego certyfikat

2. AuthorityKeyIdentifier – niekrytyczne

   Rozszerzenie to identyfikuje certyfikat klucza publiczny organu wydającego certyfikat

3. Basic Constraints – krytyczne

   Określenie, czy właściciel certyfikatu jest użytkownikiem końcowym, czy też podmiotem wydającym certyfikaty.

4. CRL Distribution Points - niekrytyczne

Rozszerzenie to definiuje adres, pod jakim dostępna jest lista CRL pozwalająca na zweryfikowanie statusu certyfikatu

5. Key Usage – krytyczne

   Rozszerzenie definiujące dozwolone użycie klucza

   Dla certyfikatów niekwalifikowanych wystawionych z urzędu CUZ Sigillum CA1 pole to zawiera wartości:

   - Digital Signature
   - Key Encipherment
   - keyAgreement
   - nonRepudiation
   - dataEncipherment

6. Extended Key Usage – niekrytyczne

   Rozszerzenie to określa rozszerzone reguły użycia klucza

   Dla certyfikatów niekwalifikowanych wystawionych z urzędu CUZ Sigillum CA1 pole to zawiera 3 wartości:

   - TLS Web Client
   - E-mail Protection
   - Smartcard Logon

7. Subject Alternative Name – niekrytyczne

   Rozszerzenie to definiuje alternatywną nazwę podmiotu. Dla certyfikatów niekwalifikowanych wystawionych z urzędu CUZ Sigillum CA1 pole to może zawierać 2 wartości:

   - RFC 822 Name – adres poczty elektronicznej subskrybenta
   - User Principal Name – nazwa subskrybenta używana w usłudze SmartCard Logon

8. Subject Directory Attributes - niekrytyczne

   Rozszerzenie to zawiera dodatkowe atrybuty powiązane z subskrybentem i dopełniające informacje zawarte w polu Subject oraz SubjectAlternativeName – rozszerzenie nie jest krytyczne.

   Zawierać może następujące atrybuty:

   - DateOfBirth – zawiera datę urodzenia właściciela certyfikatu
   - PlaceOfBirth – zawiera miejsce urodzenia właściciela certyfikatu
   - Country of Citizenship - obywatelstwo właściciela certyfikatu

9. Subject Key Identifier – niekrytyczne

   Rozszerzenie to identyfikuje klucz publiczny certyfikatu

10. Cerificate Policies – krytyczne

a. Dla urzędu CUZ Sigillum CA1:

- 1.2.616.1.113725.0.1.1 – certyfikat podpisu
- 1.2.616.1.113725.0.1.2 – certyfikat pieczęci
- 1.2.616.1.113725.0.1.3 – certyfikat serwerowy

Rozszerzenia te identyfikują certyfikat klucza publiczny organu wydającego certyfikat

W przypadku **pól krytycznych** od systemu wykorzystującego certyfikat wymagana jest jego poprawna interpretacja. Jeżeli system wykorzystującego certyfikat nie obsługuje pól wskazanych jako krytyczne certyfikat nie może być poprawnie przetwarzany.
Pola niekrytyczne mogą zostać zignorowane, jeżeli system wykorzystujący certyfikat nie potrafi ich poprawnie interpretować.

7.1.4. Algorytm użyty do podpisania certyfikatu

Wartość parametru **signatureAlgorithm** identyfikuje algorytm kryptograficzny wykorzystywany w celu poświadczenia certyfikatu przez jego wydawcę.
Dla urzędu CUZ Sigillum CA1 wykorzystywany jest algorytm sha256WithRSAEncryption
{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }

7.1.5.Poświadczenie certyfikatu

Wartość parametru **signatureValue** tworzona jest poprzez przygotowanie skrótu treści certyfikatu (tbsCertificate), a następnie podpisane tak przygotowanego skrótu kluczem prywatnym wystawcy certyfikatu.

7.2. Struktura listy CRL

Polityka określa strukturę list unieważnionych i zawieszonych certyfikatów (CRL) wystawionych w ramach Polityki. Zawartość i format listy zgodna jest z zapisami normy ITU-T X.509.
Lista CRL certyfikatów jest zbiorem pól, których znaczenie przedstawiono poniżej:

1. Informacja o unieważnionych certyfikatach (**tbsCertList**)
2. Informacja o algorytmie użytym do podpisania listy (**signatureAlgorithm**)
3. Poświadczenie elektroniczne, składane przez organ wydający listę (**signatureValue**)

Certyfikaty unieważnione są publikowane na liście CRL także po okresie ich ważności, natomiast certyfikaty zawieszone są usuwane z listy CRL w momencie ich odwieszenia.
Opis poszczególnych struktur przedstawiono poniżej.

7.2.1.Certyfikaty unieważnione

Zgodnie ze standardem X.509 na treść listy składają się pola standardowe i rozszerzone.

L.p.	Pole	Opis	Zawartość
1.	Version	wersja formatu certyfikatu zgodnie z X.509	2
2.	Signature Algorithm	informacja o algorytmie użytym do podpisania listy CRL	SHA256WithRSA
3.	Issuer	identyfikator urzędu certyfikacji wydającego listę CRL	Dla urzędu CUZ Sigillum CA1 CN=CUZ Sigillum CA1, O=Polska Wytwórnia Papierów Wartościowych S.A., OU=Centrum Usług Zaufania Sigillum, C=PL
4.	ThisUpdate	data/czas wydania listy CRL	--
5.	NextUpdate	data/czas wydania następnej listy CRL (następna lista nie może być wydana później)	--
6.	RevokedCertificates	lista unieważnionych certyfikatów, pojedynczy certyfikat opisany jest następującymi atrybutami: numer seryjny unieważnionego certyfikatu (userCertificate), data unieważnienia certyfikatu (revocationDate), rozszerzenie informacji dla unieważnionego certyfikatu (crlEntryExtensions)	--
7.	CrlExtensions	rozszerzona informacja o liście CRL	--

Poniżej wskazano zakres i wartość pól rozszerzonych list CRL:

- AuthorityKeyIdentifier - niekrytyczne

  Rozszerzenie to identyfikuje certyfikat klucza publiczny organu wydającego listę CRL

- CRLNumber - niekrytyczne

  Zawiera numer listy CRL. Numery są nadawane kolejno, zgodnie z kolejnością wydawania list CRL przez urząd certyfikacji.

7.2.2. Algorytm użyty do podpisania listy

Znaczenie parametru signatureAlgorithm jest identyczne jak w przypadku certyfikatu.

Dla urzędu CUZ Sigillum CA1 wykorzystywany jest algorytm sha256WithRSAEncryption

{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }

7.2.3.Poświadczenie certyfikatu

Znaczenie parametru signatureValue jest identyczne jak w przypadku certyfikatu.

7.2.4.Struktura odpowiedzi OCSP

Urząd certyfikacji udostępnia usługę weryfikacji statusu certyfikatu w trybie online (OCSP). Zawartość i format odpowiedzi OCSP zgodny jest z zapisami normy RFC 6960.

Serwer urzędu wystawiającego poświadczenia o statusie certyfikatu posługuje się dedykowaną parą kluczy, przeznaczoną jedynie dla tej usługi.

Odpowiedź OCSP jest zbiorem pól, których znaczenie przedstawiono poniżej:

1. Informacja o statusie certyfikatu (tbsResponseData)
2. Informacja o algorytmie użytym do podpisania odpowiedzi (signatureAlgorithm)
3. Poświadczenie elektroniczne, składane przez organ wydający odpowiedź (signature)
4. Opcjonalnie certyfikat

7.2.5.Opis poszczególnych struktur przedstawiono poniżej

L.p.	Pole	Opis	Zawartość
1.	Version	wersja formatu usługi zgodna z RFC6990	V1
2.	Responder	identyfikator urzędu certyfikacji dostawcy usługi	--
3.	ProducedAt	Data/czas wygenerowania odpowiedzi	--
4.	Responses	lista aktualnych statusów certyfikatów, pojedynczy certyfikat opisany jest następującymi atrybutami: numer seryjny unieważnionego certyfikatu (certID), status certyfikatu (certStatus), data/czas,	--

		dla której zweryfikowano statusu (thisUpdate), data/czas następnej aktualizacji statusu (nextUpdate), rozszerzenie informacji dla certyfikatu (singleExtensions)	
5.	ResponseExtensions	rozszerzona informacja o odpowiedzi OCSP	--

7.2.6. Algorytm użyty do podpisania odpowiedzi

Dla urzędu CUZ Sigillum CA1 wykorzystywany jest algorytm sha256WithRSAEncryption { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }

8. Opłaty

Za wszystkie usługi świadczone przez CUZ Sigillum pobierane są opłaty. Wysokość oraz rodzaje opłat opublikowane są na stronie pod adresem: www.Sigillum.pl

W przypadku braku uregulowania płatności, CUZ Sigillum ma prawo zawiesić certyfikat Subskrybenta na okres 7 dni po bezskutecznym wezwaniu do uregulowania płatności w terminie 7 dni. Jeżeli w tym czasie płatność zostanie uregulowana, CUZ Sigillum dokona cofnięcia zawieszenia certyfikatu. Jeżeli opłata nie zostanie wniesiona, certyfikat zostanie unieważniony po okresie 7 dni od jego zawieszenia.

9. Ochrona informacji

Wszystkie dane, których nieuprawnione ujawnienie mogłoby narazić na szkodę Centrum Usług Zaufania Sigillum i PWPW S.A. lub Subskrybenta usług zaufania traktowane są jako poufne i podlegają ochronie. Informacje poufne opisane w niniejszym dokumencie nie są tym samym, co informacje poufne w znaczeniu Ustawy o Ochronie Informacji Niejawnych. Słowo „poufne" należy rozumieć jako „dyskrecja, udostępnianie czegoś tylko niewielu osobom".

9.1. Zakres informacji poufnych

Jako poufne traktowane są wszystkie informacje, których nieuprawnione ujawnienie mogłoby narazić na szkodę Centrum Usług Zaufania Sigillum i PWPW S.A. lub Subskrybentów usług zaufania, a szczególności są to:

1) dane służące do składania podpisów elektronicznych lub pieczęci elektronicznych

2) dane do składania poświadczeń elektronicznych

3) wszelkie prywatne klucze infrastruktury

4) dane osobowe Subskrybentów usług zaufania

5) dane osobowe przedstawicieli Zamawiającego

6) umowy podpisane z Punktami rejestracji (jeśli występują)

7) przegląd bezpieczeństwa systemu i ocena ryzyka działalności

8) plan zapewnienia ciągłości funkcjonowania

9) opis konfiguracji podstawowej

10) procedury operacyjne i bezpieczeństwa

Szczegółowy zakres informacji stanowiących tajemnicę przedsiębiorstwa określony jest w dokumentach wewnętrznych PWPW S.A.

9.2. Informacje będące poza zakresem informacji poufnych

Informacje, które nie są traktowane jako poufne:

1) powód unieważnienia certyfikatu

2) informacje zawarte w certyfikatach subskrybenta i listach CRL

3) informacje o opublikowane w repozytorium

4) informacje o naruszeniach przepisów o usługach zaufania przez dostawcę usług zaufania

5) polityki

6) regulaminy

7) inne dokumenty, wymienione w Polityce jako dokumenty znajdujące się w repozytorium.

9.2.1. Odpowiedzialność za ochronę informacji poufnych

Do zachowania tajemnicy obowiązane są:

1) osoby pozostające w stosunku pracy, zlecenia lub innym stosunku prawnym o podobnym charakterze z dostawcą usług zaufania;

2) osoby pozostające w stosunku pracy, zlecenia lub innym stosunku prawnym o podobnym charakterze z podmiotami świadczącymi usługi na rzecz dostawcy usług zaufania.

Obowiązek zachowania tajemnicy trwa przez okres 10 lat od dnia ustania stosunku prawnego.
Okres trwania obowiązku zachowania w tajemnicy danych do składania podpisu elektronicznego lub pieczęci elektronicznej jest nieograniczony w czasie.
Klucze prywatne Subskrybentów związane z certyfikatami powinny być traktowane jako chronione przez Subskrybenta. Wszelkie skutki prawne wynikające z niewłaściwego lub nieuprawnionego użycia tych kluczy po ich przekazaniu Subskrybentowi ponosi Subskrybent.

9.3. Ochrona danych osobowych

Dane osobowe przetwarzane są przez Centrum Usług Zaufania Sigillum i PWPW S.A. zgodnie z Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Rozporządzenie 2016/679)
W tym celu, w PWPW S.A., została opracowana i wdrożona Polityka bezpieczeństwa danych osobowych oraz powołany został Administrator Bezpieczeństwa Informacji, którego zadaniem jest nadzór nad realizacją postanowień tej polityki.

9.4. Plan ochrony prywatności

Zasady gromadzenia, ochrony i wykorzystywania danych osobowych są zgodne z obowiązującym Rozporządzeniem RODO oraz wewnętrznymi dokumentami PWPW S.A.
Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne oraz zabezpieczenia teleinformatyczne. Bezpieczeństwo danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności i rozliczalności.
Zakres danych osobowych gromadzonych i przetwarzanych przez CUZ Sigillum odpowiada celowi, do realizacji którego dane te są potrzebne.

9.5. Informacje uważane za prywatne

Za informacje prywatne uważa się dane osobowe. W rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO)za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka

specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

9.6. Informacje nie uważane za prywatne

W rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO) informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

9.7. Odpowiedzialność za ochronę informacji prywatnych

Do zachowania prywatności danych osobowych obowiązane są:

1) osoby pozostające w stosunku pracy, zlecenia lub innym stosunku prawnym o podobnym charakterze z dostawcą usług zaufania;

2) osoby pozostające w stosunku pracy, zlecenia lub innym stosunku prawnym o podobnym charakterze z podmiotami świadczącymi usługi na rzecz dostawcy usług zaufania.

Obowiązek zachowania tajemnicy trwa przez okres 10 lat od dnia ustania stosunku prawnego.

9.8. Zezwolenie na używanie informacji prywatnych

Zgoda Odbiorcy usług zaufania/przedstawiciela Zamawiającego na przetwarzanie jego danych osobowych w związku ze świadczeniem usług zaufania jest zawarta w umowie o świadczenie usługi i jest obowiązkowa. Na przetwarzanie danych osobowych w celach marketingowych oraz do przesyłania informacji handlowych Odbiorca usług zaufania musi wyrazić dodatkową zgodę.

9.9. Ujawnienie informacji organom administracyjnym

Odstępstwo od zachowania tajemnicy może wynikać jedynie z art. 15 ust. 4 Ustawy.

9.10. Prawo do własności intelektualnej

Wszystkie znaki towarowe, handlowe, graficzne, patenty, licencje i inne używane przez Centrum Zaufania PWPW S.A. stanowią własność intelektualną ich właścicieli.

Wszystkie klucze wystawione przez Centrum Zaufania PWPW S.A. związane z certyfikatem klucza publicznego są własnością podmiotu w przypadku subskrybenta indywidualnego oraz własnością podmiotu reprezentowanego przez subskrybenta w przypadku subskrybenta certyfikatu kwalifikowanego.

9.11. Wyłączenia z gwarancji

PWPW S.A. nie odpowiada wobec odbiorców usług certyfikacyjnych za:

a) Szkody wynikające za użycia certyfikatu klucza publicznego poza zakresem określonym w Polityce, w tym w szczególności, jeśli szkoda wynikła z przekroczenia Najwyższej wartości granicznej transakcji, jeśli wartość taka została określona w certyfikacie klucza publicznego,
b) Szkodę wynikłą z powodu nieprawdziwości zawartych w certyfikacie klucza publicznego danych Zamawiającego

W przypadku, gdy PWPW S.A. działa za pośrednictwem Punktów Rejestracji, odpowiada za działania Punktów Rejestracji tak, jak za działania własne.

9.12. Ograniczenie odpowiedzialności

PWPW S.A. nie odpowiada za jakiekolwiek szkody, które powstały lub mogły powstać dla odbiorców usług zaufania, wynikające z przyczyn innych niż niewykonanie lub nienależyte wykonanie obowiązków przez PWPW S.A. lub upoważnione podmioty działające w jego imieniu. W szczególności PWPW S.A. nie odpowiada za:

a) Skutki nieprawidłowego użycia klucza prywatnego Subskrybenta,
b) Skutki użycia klucza prywatnego Subskrybenta przez nieuprawnioną osobę,
c) Skutki utraty bezpieczeństwa stosowanych przez PWPW S.A. algorytmów kryptograficznych, chyba że użycie tych algorytmów nie jest zgodne z aktualnymi aktami wykonawczymi do Ustawy,
d) Skutki nieprawidłowej, niezgodnej z Polityką, weryfikacji certyfikatów kluczy publicznych wystawionych przez PWPW S.A., w tym skutki wynikające ze stosowania przez Stronę ufającą uproszczonej procedury weryfikacji certyfikatów kluczy publicznych opisanej w Polityce.

9.13. Obowiązywanie i tryb wprowadzania zmian Polityki

Niniejsza Polityka Certyfikacji obowiązuje na czas nieokreślony. PWPW S.A. zastrzega sobie możliwość wprowadzania zmian w każdym czasie. Zmiany mogą wynikać w szczególności:

- Ze zmian przepisów powszechnie obowiązującego prawa – zarówno europejskiego i polskiego,
- Ze zmian wynikających ze sposobu świadczenia przez PWPW S.A. usług, o których mowa w niniejszym dokumencie.
- CUZ Sigillum zastrzega sobie prawo do wprowadzania nowych wersji Polityk w zakresie świadczenia usług zaufania. Miejscem publikacji nowych wersji Polityk jest Repozytorium CUZ Sigillum dostępne pod adresem: https://sigillum.pl
- Zapisy nowych wersji Polityk wchodzą w życie z dniem ich opublikowania w Repozytorium i mają zastosowanie do Certyfikatów wystawionych po tym dniu.

- CUZ Sigillum może zdecydować, w przypadkach uzasadnionych wymogami bezpieczeństwa informacji zabezpieczanych przy użyciu dotychczas wystawionych Certyfikatów, że nowe wersje Polityk będą dotyczyć również Certyfikatów wystawionych przed wejściem w życie nowych wersji Polityk.
- W przypadku wprowadzenia nowych wersji Polityk, które dotyczą Certyfikatów wydanych przed wejściem w życie tychże nowych wersji, CUZ Sigillum niezwłocznie zawiadamia drogą elektroniczną lub pisemnie o wprowadzeniu nowych wersji Polityk Subskrybenta. Jeżeli została zawarta Umowa o świadczeniu usług zaufania z Zamawiającym CUZ Sigillum zawiadamia o wprowadzeniu nowych wersji Polityk również Zamawiającego.
- Jeśli Subskrybent w terminie 30 dni od dnia powiadomienia, w sposób o którym mowa w ust. 4, nie zgłosi zastrzeżeń do nowych wersji Polityk przyjmuje się, iż zapoznał się z ich treścią, akceptuje je oraz zobowiązuje się do przestrzegania postanowień w nich zawartych. W sytuacji zawarcia Umowy o świadczenie usług zaufania z Zamawiającym, prawo wniesienia zastrzeżeń do nowych wersji Polityk oraz wyrażenia akceptacji przysługuje Zamawiającemu.
- W przypadku braku akceptacji nowych wersji Polityk Subskrybent może wypowiedzieć Umowę doręczając pisemne wypowiedzenie zawierające jego oświadczenie woli.
- Każda modyfikacja Polityki musi zostać zatwierdzona przez Radę Zatwierdzania Polityk Certyfikacji PWPW S.A.
- Zmiana Polityki może być dokonywana w sposób planowy lub przyspieszony.
- Procedura przyspieszonej zmiany Polityki zachodzi wtedy, gdy RZPC PWPW S.A. stwierdzi, że posługiwanie się dotychczasową wersją Polityki jest niebezpieczne dla odbiorców usług zaufania. W takim przypadku RZPC PWPW S.A. może wprowadzić zmienioną Politykę w trybie natychmiastowym.
- zmianie Polityki RZPC PWPW S.A. niezwłocznie powiadamia ministra właściwego ds. informatyzacji, nie później niż 7 dni od daty zatwierdzenia zmiany.
- Jeśli zmiany te nie wynikają z przyczyn leżących po stronie PWPW S.A., a są spowodowane np. Wymaganiami prawa lub zmieniającymi się warunkami bezpieczeństwa, w tym bezpieczeństwa algorytmów kryptograficznych, Subskrybentom nie przysługuje prawo do odszkodowania za ewentualne ograniczenia możliwości wykorzystywania certyfikatów.

9.14. Rozstrzyganie sporów

W przypadku powstania sporu pomiędzy CUZ Sigillum a Subskrybentem strony podejmą próbę rozstrzygnięcia sporu w drodze polubownego porozumienia. W przypadku braku porozumienia rozstrzygnięcie sporu zostanie poddane sądowi powszechnemu właściwemu dla siedziby PWPW S.A.

9.15. Prawo właściwe

Umowa, jej wykonanie oraz wszelkie wynikające z niej stosunki prawne, podlegają prawu obowiązującemu na terenie Rzeczpospolitej Polski.

9.16. Zgodność z przepisami prawa

Zapisy polityki oraz zapisy umów o świadczenie usług zaufania podlegają normom prawnym Rzeczpospolitej Polskiej.

10. Rejestr zmian w dokumencie

Opis zmian	Wersja	Data
Stworzenie dokumentu	1.0	29.08.2018
Aktualizacja dokumentu	1.1	14.11.2018
Aktualizacja dokumentu	1.2	01.04.2020
Aktualizacja dokumentu	1.3	15.02.2021
Aktualizacja dokumentu	1.4	04.10.2024
Aktualizacja dokumentu	1.5	28.02.2025

Signature Not Verified
Dokument podpisany przez SYLWESTER SZCZEPANIAK
Data: 2025.03.11 13:02:20 CET

Elektronicznie podpisany przez Rafał Mariusz Jarosz
Data: 2025.03.11 13:26:47 +01'00'

Elektronicznie podpisany przez Anna Weber
Data: 2025.03.11 '13:55:39 +01'00

Anna Weber