PIONIER
INFRASTRUKTURA KLUCZA PUBLICZNEGO

# Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego w PIONIER PKI

**Wdrożenie infrastruktury klucza publicznego (PKI) dla użytkowników sieci PIONIER**

---

| | |
|---|---|
| Plik dokumentu : | **cp-ca-wcss-L2.pdf** |
| Zadanie: | **2b** |
| Partner(zy): | **PCSS, WCSS, UMK, PS** |
| Partner odpowiedzialny: | **WCSS** |
| Klasyfikacja: | **Do użytku publicznego** |
| Data publikacji: | **13 listopada 2010** |

---

Abstrakt: Dokument Polityk Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego opisuje procedury stosowane przez Urząd Certyfikacji PIONIER PKI CA-WCSS-2 podczas certyfikacji klucza publicznego, definiuje uczestników tego procesu oraz określa obszary zastosowań certyfikatów uzyskanych w tym procesie.

PIONIER

## Historia dokumentu

| Wersja | Data | Opis zmian | Autor |
|---|---|---|---|
| 0.1 | 31/10/2009 | Szablon dokumentu | Paweł Wolniewicz |
| 0.5 | 28/02/2010 | Pierwsza wersja dokumentu | Ireneusz Tarnowski |
| 0.6 | 18/03/2010 | Poprawki zespołu | Ireneusz Tarnowski |
| 0.7 | 24/06/2010 | Poprawki zespołu | Ireneusz Tarnowski |
| 0.8 | 16/07/2010 | Poprawki zespołu | Ireneusz Tarnowski |
| 0.9 | 03/08/2010 | Poprawki zespołu | Ireneusz Tarnowski |
| 0.91 | 13/08/2010 | Poprawki struktury i uzupełnienia | Paweł Wolniewicz |
| 0.95 | 06/10/2010 | Poprawki zespołu | Ireneusz Tarnowski |
| 0.96 | 14/10/2010 | Poprawki zespołu | Ireneusz Tarnowski |
| 0.99 | 17/10/2010 | Ostateczna wersja dokumentu | Ireneusz Tarnowski |
| 1.0 | 12/11/2010 | Zaakceptowana wersja dokumentu | Ireneusz Tarnowski |

**Zespół projektu PIONIER PKI opracowujący niniejszą politykę:**

1. Grzegorz Kosicki (WCSS)
2. Adam Osuchowski (CK PŚ)
3. Piotr Strzyżewski (CK PŚ)
4. Ireneusz Tarnowski (WCSS)
5. Maja Wolniewicz (UMK)
6. Paweł Wolniewicz (PCSS)
7. Tomasz Wolniewicz (UMK)

Polityka Certyfikacji
oraz
Kodeks Postępowania Certyfikacyjnego
w

# Urzędzie Certyfikacji PIONIER PKI CA-WCSS-2

wersja dokumentu: 1.0
data publikacji: 12 listopada 2010

# Spis treści

# 1 Wstęp

Urząd Certyfikacji PIONIER PKI CA-WCSS-2 (CA przy Wrocławskim Centrum Sieciowo-Superkomputerowym we Wrocławiu) świadczy usługi certyfikacji użytkowników końcowych w sieci PIONIER (w szczególności użytkowników środowiska akademickiego i naukowo-badawczego).

Dokument jest zgodny z RFC 3647: *„Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”.*

## 1.1 Wprowadzenie

Poniższy dokument opisuje procedury stosowane przez Urząd Certyfikacji PIONIER PKI CA-WCSS-2 podczas certyfikacji klucza publicznego, definiuje uczestników tego procesu oraz określa obszary zastosowań certyfikatów uzyskanych w tym procesie.

Niniejsza polityka jest zgodna z polityką urzędów PIONIER PKI Root-CA i PIONIER PKI Sub-Root-CA-2.

Polityka certyfikacji obowiązuje od dnia uruchomienia Urzędu Certyfikacji PIONIER PKI CA-WCSS-2, tj. od dnia 1 listopada 2010.

Zadaniem Urzędu Certyfikacji PIONIER PKI CA-WCSS-2 jest poświadczanie swoim podpisem elektronicznym:

- kluczy publicznych urzędów rejestracyjnych występujących w imieniu PIONIER PKI,
- kluczy publicznych użytkowników końcowych.

Certyfikaty Urzędu Certyfikacji PIONIER PKI CA-WCSS-2 wydawane są wyłącznie dla osób i instytucji przyłączonych do sieci PIONIER, w szczególności związanych ze środowiskiem naukowo-badawczym i akademickim.

Urząd Certyfikacji PIONIER PKI CA-WCSS-2 (CA przy Wrocławskim Centrum Sieciowo-Superkomputerowym we Wrocławiu) jest prowadzony przez:

```
Wrocławskie Centrum Sieciowo-Superkomputerowe (WCSS)
Politechnika Wrocławska (PWR)
Wybrzeże Wyspiańskiego 27
50-370 Wrocław
Polska (PL)
```

## 1.2 Identyfikator polityki

- Tytuł: `Polityka Certyfikacji` *`Urzędu Certyfikacji PIONIER PKI CA-WCSS-2`*
- Wersja: `0.1`
- Data: `1 listopada 2010`
- OID: `1.3.6.1.4.1.36065.1.5.1.0.1`

Poszczególne komponenty identyfikatora OID to:
1 ISO assigned
3 Organization acknowledged by ISO
6 US Department of Defence
1 Internet
4 Private
1 IANA registered private enterprises
36065 PIONIER
1 PKI
5 *CA-WCSS-2*
1 Polityka Certyfikacji
0 Major version
1 Minor version

## 1.3 Podmioty

### 1.3.1 Urzędy Certyfikacji

Urząd Certyfikacji PIONIER PKI CA-WCSS-2 jest częścią infrastruktury PIONIER PKI.

Certyfikat Urzędu Certyfikacji PIONIER PKI CA-WCSS-2 jest poświadczony przez Urząd Certyfikacji PIONIER PIONIER PKI Sub-Root-CA-2, który z kolei jest poświadczony przez Główny Urząd Certyfikacji PIONIER PKI Root-CA.

Urząd Certyfikacji PIONIER PKI CA-WCSS-2 nie poświadcza certyfikatów innych urzędów.

### 1.3.2 Urzędy Rejestracji

Urząd Certyfikacji występuje jednocześnie jako Urząd Rejestracji. W celu usprawnienia funkcjonowania Urząd Certyfikacji PIONIER PKI CA-WCSS-2 MOŻE powoływać swoje urzędy rejestracji. Rolę urzędu rejestracji powierza się zaufanej osobie, wskazanej przez instytucję. Osoba taka podpisuje umowę z urzędem certyfikacyjnym, w którego imieniu występuje i zobowiązuje się do przestrzegania zasad niniejszego dokumentu.

Lista aktualnie akredytowanych urzędów rejestracji jest dostępna w repozytorium. (Patrz punkt 2.1.)

### 1.3.3 Subskrybenci

Certyfikaty Urzędu Certyfikacji PIONIER PKI CA-WCSS-2 wydawane są wyłącznie dla subskrybentów związanych z instytucjami przyłączonymi do sieci PIONIER, w szczególności związanych ze środowiskiem naukowo-badawczym i akademickim.

Subskrybentami MOGĄ być wyłącznie osoby fizyczne lub osoby reprezentujące systemy komputerowe ubiegające się o certyfikat lub posługujące się certyfikatem, uprawnione do otrzymania certyfikatu (certyfikat osobisty, jak również certyfikat o profilu związanym z usługami systemu komputerowego).

### 1.3.4 Strony ufające

Stroną ufającą jest osoba lub jednostka organizacyjna (lub system komputerowy), która w granicach określonych w Polityce Certyfikacji MOŻE działać w oparciu o certyfikaty wydane przez Urząd Certyfikacji PIONIER PKI CA-WCSS-2.

W szczególności Strona ufająca NIE MUSI być Subskrybentem usług certyfikacyjnych Urzędu Certyfikacji PIONIER PKI CA-WCSS-2, a jej działania ograniczają się wówczas do weryfikacji ważności i interpretacji Certyfikatu Subskrybenta. Na czas wykorzystania certyfikatu Subskrybenta, Strony ufające zobowiązane są do weryfikacji ważności certyfikatu w zgodzie z zapisami Polityki Certyfikacji. Do realizacji procesu weryfikacji ważności certyfikatu Strony ufające posługują się sprzętem i/lub oprogramowaniem do weryfikacji autentyczności i integralności danych zawartych w certyfikacie.

## 1.4 Obszar zastosowania

### 1.4.1 Dozwolone zastosowania

Certyfikaty wystawiane przez PIONIER PKI CA-WCSS-2 MOGĄ być stosowane w różnych aplikacjach internetowych obsługujących certyfikaty X.509 w celu uwierzytelnienia klienta, uwierzytelnienia serwera, uwierzytelnienia i szyfrowania komunikacji, weryfikacji podpisów cyfrowych (między innymi: poczta elektroniczna, dostęp do WWW, dostęp do sieci komputerowej oraz zdalny dostęp do systemów komputerowych).

### 1.4.2 Zabronione zastosowania

Certyfikaty wystawiane przez PIONIER PKI CA-WCSS-2 NIE MOGĄ być używane w żadnych zastosowaniach komercyjnych i finansowych, w zastosowaniach wymagających certyfikatów kwalifikowanych oraz w działalności niezgodnej z prawem.

## 1.5 Zasady administrowania Polityką Certyfikacji

### 1.5.1 Organizacja nadzorująca

Za niniejszą Politykę Certyfikacji odpowiada Zespół d.s. PKI we *Wrocławskim Centrum Sieciowo-Superkomputerowym*:

```
Wrocławskie Centrum Sieciowo-Superkomputerowe
Wybrzeże Wyspiańskiego 27
50-370 Wrocław
tel.:  +48 71 3202456 / +48 71 3203921
fax:  +48 71 3225797

http://ca-2.wcss.pki.pionier.net.pl
e-mail:  ca-2@wcss.pki.pionier.net.pl
```

### 1.5.2 Kontakt

Zespół d.s. PKI we Wrocławskim Centrum Sieciowo-Superkomputerowym:

```
Wrocławskie Centrum Sieciowo-Superkomputerowe
Wybrzeże Wyspiańskiego 27
50-370 Wrocław
tel.:  +48 71 3202456 / +48 71 3203921
fax:  +48 71 3225797

http://ca-2.wcss.pki.pionier.net.pl
e-mail:  ca-2@wcss.pki.pionier.net.pl
```

### 1.5.3 Procedura zatwierdzania polityki certyfikacji

Polityka Certyfikacji jest zatwierdzona przez *Zespół projektu PIONIER PKI* (wskazany przez *Radę Konsorcjum PIONIER*).

Wszelkie zmiany w niniejszej Polityce Certyfikacji MUSZĄ być zatwierdzone przez organ d.s. PIONIER PKI wskazany przez *Radę Konsorcjum PIONIER*.

## 1.6 Definicje i akronimy

**PKI** (ang. *Public Key Infrastructure*) - Infrastruktura Klucza Publicznego - ogół zagadnień technicznych, operacyjnych i organizacyjnych umożliwiających realizację różnych usług ochrony informacji przy zastosowaniu kryptografii klucza publicznego i certyfikatów klucza publicznego

**X.509** - standard definiujący schemat dla certyfikatów kluczy publicznych, unieważnień certyfikatów oraz certyfikatów atrybutu służących do budowania hierarchicznej struktury PKI; aktualna wersja standardu IETF to RFC 5280 (certyfikat klucza publicznego i CRL) oraz RFC 3281 (certyfikat atrybutu)

**Urząd certyfikacji (CA)** (ang. *Certification Authority*) - instytucja (jednostka organizacyjna), która wystawia certyfikaty, listy CRL, certyfikuje inne CA

**Urząd rejestracji (RA)** (ang. *Registration Authority*) - instytucja (jednostka organizacyjna), która zbiera wnioski o wydanie certyfikatu oraz weryfikuje tożsamość subskrybentów

**SubCA** (ang. *Subsidiary Certification Authority*) - pośredni urząd certyfikacji; występujący w rozbudowanej hierarchii PKI urząd podrzędny, posiadający certyfikat klucza publicznego wydany przez urząd nadrzędny; pośredni urząd certyfikacji występuje jako nadrzędny urząd certyfikacji wobec urzędów certyfikacji niższego poziomu

**TTP** (ang. *Trusted Third Party*) - Zaufana Trzecia Strona - wirtualny (logiczny) podmiot w modelu PKI posługujący się mechanizmem podpisu cyfrowego i certyfikatu do poświadczania określonej treści, darzony zaufaniem przez pozostałe strony w tym modelu

**Kodeks Postępowania Certyfikacyjnego (CPS)** (ang. *Certification Practice Statement*) - dokument opisujący od strony operacyjnej proces certyfikacji klucza publicznego uczestników tego procesu (Urzędy Certyfikacji, Urzędy Rejestracji, subskrybentów oraz strony ufające) oraz określający obszary zastosowań uzyskanych w jego wyniku certyfikatów

**Polityka Certyfikacji (CP)** (ang. *Certificate Policy*) - szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki bezpieczeństwa tworzenia i stosowania certyfikatów

**OCSP** (ang. *Online Status Certificate Protocol*) - protokół informowania o statusie ważności certyfikatu w trybie połączeniowym (on-line)

**Lista unieważnionych certyfikatów (CRL)** (ang. *Certificate Revocation List*) - podpisane przez Urząd Certyfikacji chronologiczne zestawienie zawierające listę wszystkich certyfikatów unieważnionych, bądź zawieszonych przez Urząd Certyfikacji

**Wniosek o wystawienie certyfikatu (CSR)** (ang. *Certificate Signing Request*) - zlecenie certyfikacji przygotowane dla podmiotu wnioskującego o certyfikat przy wykorzystaniu jego klucza prywatnego

**Infrastruktura klucza publicznego sieci PIONIER** - PKI działające w ramach infrastruktury sieciowej PIONER na rzecz użytkowników (bezpośrednich oraz pośrednich) sieci PIONIER

**Klucz prywatny** (ang. *Private Key*) - Jeden z dwóch kluczy należących do pary kluczy asymetrycznych, znany tylko jego właścicielowi. W systemie podpisu asymetrycznego klucz prywatny służy do podpisywania. W systemie szyfrowania asymetrycznego klucz prywatny służy do deszyfrowania. Klucz prywatny musi być wyjątkowo starannie chroniony. Klucze prywatne dla certyfikatów o wyższej wiarygodności są zapisane na karcie mikroprocesorowej skąd.

**Klucz publiczny** (ang. *Public Key*) - Jeden z dwóch kluczy należących do pary kluczy asymetrycznych, powszechnie dostępny, którego powiązanie z konkretną osobą (lub firmą) potwierdza certyfikat. W systemie podpisu asymetrycznego klucz publiczny służy do weryfikacji podpisu. W systemie szyfrowania asymetrycznego klucz publiczny służy do szyfrowania.

**Sprzętowy moduł bezpieczeństwa (HSM)** (ang. *Hardware Security Module*) - Zestaw składający się ze sprzętu, oprogramowania, mikrokodu lub ich określonej kombinacji, realizujący operacje lub procesy kryptograficzne, obejmujące szyfrowanie i deszyfrowanie wykonywane w obszarze kryptograficznym tego modułu. Jest to wiarygodna implementacja kryptosystemu, który w bezpieczny sposób wykonuje operacje szyfrowania i deszyfrowania. Operacje kryptograficzne wykonywane są w oparciu o parametry bezpieczeństwa, które są automatycznie usuwane, jeśli urządzenie zostanie otwarte.

**Strona ufająca** (ang. *Trusted Party*) - osoba, jednostka organizacyjna lub system komputerowy, która w granicach określonych w Polityce Certyfikacji może działać w oparciu o certyfikaty

**Użytkownik końcowy** (ang. *End Entity*) - system komputerowy lub osoba ubiegająca się o certyfikat lub posługująca się certyfikatem (subskrybent). Użytkownikiem końcowym jest również strona ufająca w sytuacji, kiedy weryfikuje ważność certyfikatu.

**Subskrybent** (ang. *Subscriber*) - osoba reprezentująca system komputerowy, osoba reprezentująca podmiot (organizację) lub osoba fizyczna ubiegająca się o certyfikat lub posługująca się certyfikatem (uprawniona do posiadania certyfikatu)

**Nazwa wyróżnion (DN)** (ang. Distinguished Name) - zbiór atrybutów tworzących nazwę wyróżnioną podmiotu, odróżniającą go od innych podmiotów tego samego typu.

**Bezpieczna komunikacja sieciowa** - komunikacja sieciowa odbywająca sie w kanale szyfrowanym, z uwierzytelnianiem dwóch stron komunkacji

Słowa **„MUSI”**, **„MOŻE”**, **„POWINIEN”**, **„NIE WOLNO”** i ich odmiana, pisane wielkimi literami (kapitalikami) są używane zgodnie z definicją ich angielskich odpowiedników określonych w RFC 2119, w szczególności słowo „POWINEN” należy rozumieć w taki sposób, że niespełnienie warunku opatrzonego tą klauzulą jest dopuszczalne tylko w szczególnie uzasadnionych przypadkach.

# 2 Zasady dystrybucji i publikacji informacji

## 2.1 Repozytorium

Repozytorium Urzędu Certyfikacji PIONIER CA-WCSS-2 jest dostępne w serwisie WWW pod adresem `http://ca-2.wcss.pki.pionier.net.pl`.

## 2.2 Publikowane informacje

- certyfikaty kluczy publicznych są publikowane pod adresem:
  `http://ca-2.wcss.pki.pionier.net.pl/certs`
- lista odwołanych certyfikatów jest publikowana pod adresem:
  `http://ca-2.wcss.pki.pionier.net.pl/crl`
- Aktualne i archiwalne wersje Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego są publikowane pod adresem:
  `http://ca-2.wcss.pki.pionier.net.pl/cp`
- Lista akredytowanych Urzędów Rejestracji publikowana jest pod adresem:
  `http://ca-2.wcss.pki.pionier.net.pl/ra`

## 2.3 Częstotliwość publikowania informacji

Jeżeli ulega modyfikacji Polityka Certyfikacji lub Kodeks Postępowania Certyfikacyjnego, to aktualne wersje tych dokumentów POWINNY zostać opublikowana najpóźniej z terminem ich wejścia w życie.

Certyfikaty POWINNY być publikowane niezwłocznie po ich wystawieniu.

Lista wycofanych certyfikatów POWINNA być publikowana niezwłocznie po jej aktualizacji.

## 2.4 Dostęp do repozytorium

Wszystkie informacje publikowane w repozytorium są dostępne publicznie i nieodpłatnie.

Nie przewiduje się żadnych niestandardowych metod ochrony dostępu do Polityki Certyfikacji, Kodeksu Postępowania Certyfikacyjnego oraz list odwołanych certyfikatów (CRL).

Urząd Certyfikacji PIONIER PKI CA-WCSS-2 dokłada wszelkich starań by repozytorium dostępne przez całą dobę przez siedem dni w tygodniu.

# 3 Identyfikacja i uwierzytelnianie

## 3.1 Struktura nazewnictwa

### 3.1.1 Typy nazw

Nazwy stosowane w polach *subject name* i *issuer name* MUSZĄ być zgodne z formatem nazw wyróżnionych standardu X.501. Wszystkie elementy nazwy wyróżnionej MUSZĄ być zapisane w formacie `PrintableString` lub `UTF8String` lub `IA5String` (tylko pole e-mail).

Adres e-mail MUSI mieć strukturę zgodną z RFC822 i MUSI być zapisywany w formacie `IA5String`.

Struktura nazwy domenowej MUSI być zgodna z RFC2247.

### 3.1.2 Konieczność używania nazw znaczących

Nazwa wyróżniona stosowana w certyfikacie (z wyjątkiem certyfikatów pseudoanonimowych) MUSI pozwalać na jednoznaczną identyfikację subskrybenta oraz instytucji. Adres e-mail zamieszczony w certyfikacie musi być rzeczywistym adresem poczty elektronicznej, poprzez który można się komunikować z subskrybentem.

### 3.1.3 Anonimowość i pseudoanonimowość

Urząd Certyfikacji PIONIER PKI CA-WCSS-2 nie certyfikuje użytkowników anonimowych. Dopuszczone jest certyfikowanie pseudoanonimowe. Przez „pseudoanonimowość" rozumie się taką sytuację, w której certyfikat nie zawiera danych użytkownika, natomiast zawiera unikatową jego nazwę. Urząd certyfikacji MUSI przechowywać dane umożliwiające powiązanie unikatowej nazwy użytkownika (znajdującej się na certyfikacie) z jego danymi (rzeczywistymi).

Urząd Rejestracji nadzoruje poprawność oraz unikatowość nazw w certyfikatach pseudoanonimowych. Urząd Rejestracji może odmówić poświadczenia wniosku użytkownika, jeżeli unikatowa nazwa użytkownika, wykorzystana we wniosku, może sugerować tożsamość osoby, którą nie jest wnioskodawca. Urząd Rejestracji może również odmówić poświadczenia wniosku użytkownika w każdym innym uzasadnionym przypadku. Urząd Rejestracji informuje wnioskodawcę o przyczynie odrzucenia jego wniosku.

### 3.1.4 Zasady interpretacji nazw

Zasady interpretowania nazw zapisanych w formacie X.501 są zawarte w RFC4514. Zasady interpretowania nazw o strukturze zgodnej z RFC822 są zawarte w RFC2821 i RFC2822.

### 3.1.5 Unikatowość nazw

Nazwa wyróżniona MUSI być unikatowa dla każdej jednostki podmiotu certyfikowanego przez Urząd Certyfikacji PIONIER PKI CA-WCSS-2.

Dwie nazwy uznawane są za identyczne, jeśli różnią się wyłącznie znakami innymi niż litery i cyfry oraz jeśli ich zapis po transkrypcji do znaków zestawu ASCII jest identyczny.

Urząd Certyfikacji może wydać kolejny certyfikat z tą samą nazwą wyróżnioną wyłącznie, jeśli można jednoznacznie stwierdzić, że wnioskujący podmiot jest tym samym, dla którego został wystawiony poprzedni certyfikat.

## 3.2 Identyfikacja i uwierzytelnianie przy pierwszej rejestracji

### 3.2.1 Dowód posiadania klucza prywatnego

Dopuszcza się dwie sytuacje:

1. Subskrybent zleca certyfikację swego klucza publicznego. Subskrybent sam generuje parę kluczy, a następnie przygotowuje zlecenie certyfikacji i podpisuje je. Następnie dostarcza zlecenie certyfikacji oraz wynik działania funkcji skrótu w formie papierowej;
2. Urząd Rejestracji występuje w imieniu subskrybenta i generuje mu parę kluczy oraz zgłasza się do Urzędu Certyfikacji w celu certyfikowania klucza publicznego.

W pierwszej sytuacji zakłada się, że subskrybent jest właścicielem odpowiedniego klucza prywatnego, jeśli zlecenie certyfikacji daje się zweryfikować przy pomocy klucza publicznego zawartego w zleceniu.

Drugi przypadek jest dopuszczalny tylko i wyłącznie w sytuacji, gdy klucz prywatny użytkownika generowany jest na karcie kryptograficznej. Karta krytpograficzna MUSI być zabezpieczona hasłem. Karta kryptograficzna wraz z hasłem MUSI zostać przekazana użytkownikowi w imieniu którego występował Urząd Rejestracji.

### 3.2.2 Uwierzytelnienie instytucji

Urząd Rejestracji MUSI sprawdzić, czy instytucja jest uprawniona do uzyskania certyfikatu z Urzędu Certyfikacji PIONIER PKI CA-WCSS-2.

### 3.2.3 Uwierzytelnienie danych osoby fizycznej

Tożsamość osoby ubiegającej się o certyfikację klucza publicznego MUSI być weryfikowana w czasie osobistego kontaktu z Urzędem Rejestracji na podstawie dokumentu pozwalającego potwierdzić tożsamość osoby.

W przypadku gdy klucz prywatny przechowywany jest ma karcie kryptograficznej, która jednocześnie stanowi dokument tożsamości, tożsamość osoby ubiegającej się o certyfikację klucza publicznego NIE MUSI być weryfikowana w czasie osobistego kontaktu z Urzędem Rejestracji.

Subskrybent zlecający wniosek certyfikacji, zawierając nazwę wyróżnionioną skojarzoną z konkretną instytucją, POWINIEN dostarczyć poświadczenie o przynależności do danej organizacji lub odpowiedni Urząd Rejestracji POWINIEN otrzymać potwierdzenie takiej przynależności.

Subskrybent zlecający wniosek certyfikacji certyfikatu do podpisywania kodu, zawierający nazwę wyróżnioną skojarzoną z nazwa projektu lub oprogramowania, POWINIEN dostarczyć poświadczenie o swoim związku z wymienionym oprogramowaniem.

W uzasadnionych sytuacjach mogą zostać podjęte dodatkowe działania zmierzające do potwierdzenia wiarygodności subskrybenta.

## 3.3 Identyfikacja i uwierzytelnianie przy ponownej rejestracji

Jeżeli wniosek o odnowienie certyfikatu został podpisany przez ważny certyfikat (z taką samą nazwą wyróżnioną), wniosek taki zostaje zaakceptowany bez konieczności wypełnienia nowego wniosku o certyfikat oraz oświadczenia pisemnego. Urząd Certyfikacji zakłada ważność wniosku oraz oświadczenia, które zostało złożone przy występowaniu o certyfikat po raz pierwszy.

Jeśli od ostatniego pisemnego oświadczenia minęło **ponad 5 lat**, uwierzytelnienie użytkownika musi się odbywać zgodnie z procedurą pierwszej rejestracji opisaną w punkcie 3.2.3.

Jeśli certyfikat użytkownika stracił ważność lub został unieważniony, to uwierzytelnienie użytkownika musi się odbywać zgodnie z procedurą pierwszej rejestracji (patrz punkt 3.2.3).

## 3.4 Identyfikacja i uwierzytelnianie żądań odwołania certyfikatów

Za uwierzytelnione jest uważane poświadczenie przekazywanego komunikatu własnym podpisem cyfrowym przy użyciu aktualnego i nie odwołanego certyfikatu. Do sprawdzenia wiarygodności zlecenia POWINNY być stosowane takie same procedury, jakie obowiązują w procesie rejestrowania subskrybenta. Zgłoszenie, które zawiera jednoznaczny dowód naruszenia wiarygodności klucza lub nieaktualności danych nie wymaga dodatkowej weryfikacji.

# 4 Cykl życia certyfikatu - wymagania operacyjne

## 4.1 Zlecenie certyfikacji

### 4.1.1 Podmioty uprawnione do składania wniosków o certyfikat

Certyfikaty osobiste PIONIER PKI CA-WCSS-2 MOGĄ otrzymać użytkownicy sieci PIONIER (użytkownicy związani z organizacją przyłączoną w sposób pośredni lub bezpośredni do sieci PIONIER).

O certyfikat osobisty MOŻE wystąpić inny podmiot (osoba, instytucja, jednostka organizacyjna), niż osoba, której dane są zawarte w certyfikacie.

Certyfikaty infrastruktury PIONIER PKI CA-WCSS-2 MOGĄ zostać wystawione dla infrastruktury, której właścicielem lub użytkownikiem jest organizacja przyłączona w sposób pośredni lub bezpośredni do sieci PIONIER. O certyfikat infrastruktury MUSI wystąpić osoba odpowiedzialna za funkcjonowanie danego elementu infrastruktury.

Certyfikaty do podpisywania kodu PIONIER PKI CA-WCSS-2 MOGĄ otrzymać użytkownicy sieci PIONIER (użytkownicy związani z organizacją przyłączoną w sposób pośredni lub bezpośredni do sieci PIONIER).

### 4.1.2 Zasady składania wniosków o wydanie certyfikatu

Subskrybent musi zapoznać się i zaakceptować Politykę Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego.

Zlecenie certyfikacji może zostać utworzone poprzez formularz na stronie WWW Urzędu Rejestracji lub może być przesłane formacie PKCS10 do właściwego Urzędu Rejestracji.

Gdy klucz prywatny generowany jest na karcie kryptograficznej, zlecenie certyfikacji może pochodzić od innego podmiotu (osoba, instytucja, jednostka organizacyjna), niż osoba, której dane są zawarte w certyfikacie.

## 4.2 Przetwarzanie wniosku o wydanie certyfikatu

### 4.2.1 Weryfikacja tożsamości

W zależności od zastosowania certyfikatu możliwe są 2 rozwiązania.

1. W przypadku certyfikatów dla subskrybentów, którzy są osobami fizycznymi, niezbędna jest pełna weryfikacja tożsamości w Urzędzie Rejestracji w którym składa się wniosek certyfikacyjny.

2. W przypadku certyfikatów dla infrastruktury, niezbędne jest potwierdzenie prawa do domeny.

W przypadku gdy wniosek o certyfikat składany jest w imieniu subskrybenta, to weryfikacja subskrybenta odbywa się w momencie odbierania przez subskrybenta klucza prywatnego. W takim przypadku, klucz prywatny MUSI znajdować się na karcie kryptograficznej. Jeżeli karta kryptograficzna jest kartą spersonalizowaną (zawierjącą informacje o subskrybencie, wystawioną przez jednostkę organizacyjną), ta sama karta kryptograficzna MOŻE być podstawą do pozytywnej weryfikacji subskrybenta.

W przypadku certyfikatów dla subskrybentów, którzy są osobami fizycznymi, tożsamość subskrybenta i przynależność do instytucji MUSZĄ zostać zweryfikowane przez Urząd Certyfikacji lub wspomagający go Urząd Rejestracji zgodnie z punktami 3.2.2 i 3.2.3.

W przypadku wnioskowania o certyfikat infrastruktury, Urząd Rejestracji POWINIEN potwierdzić prawo wnioskodawcy do uzyskania danego certyfikatu.

Jeśli certyfikat ma zawierać adres e-mail, to Urząd Rejestracji POWINIEN potwierdzić, że przy jego pomocy można komunikować się z wnioskodawcą.

### 4.2.2 Zasady akceptacji i odrzucania wniosków o wydanie certyfikatu

Wniosek zostaje zaakceptowany, jeśli parametry techniczne są zgodne z niniejszym dokumentem a wnioskodawca został uwierzytelniony i podpisał oświadczenie o akceptacji Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego. Jeśli wniosek o certyfikat nie spełnia wymagań technicznych, to wnioskodawca jest o tym fakcie informowany i wezwany do poprawienia wniosku. W przypadku gdy uwierzytelnianie i skompletowanie dokumentów trwa dłużej niż 7 dni, wniosek zostaje odrzucony.

Wnioskodawca jest informowany za pomocą poczty elektronicznej o odrzuceniu wniosku i przyczynach odrzucenia.

### 4.2.3 Czas przetwarzania wniosku wydanie certyfikatu

Certyfikat zostaje wystawiony w ciągu **3 dni** roboczych od skompletowania niezbędnych dokumentów (tj. wniosek w postaci elektronicznej oraz podpisane oświadczenie).

## 4.3 Wydanie certyfikatu

### 4.3.1 Postępowanie Urzędu Certyfikacji podczas wydawania certyfikatu

Urząd Certyfikacji wystawia certyfikat zgodnie z polityką zdefiniowaną w niniejszym dokumencie.

W uzasadnionych przypadkach Urząd Certyfikacji ma prawo odmowy realizacji zlecenia certyfikacji.

### 4.3.2 Powiadamianie subskrybenta o wydaniu certyfikatu

Wnioskodawca zostaje powiadomiony o wystawieniu certyfikatu za pomocą poczty elektronicznej. Wystawiony certyfikat jest udostępniony przez interfejs WWW (portal informacyjny Urzędu Certyfikacji lub portal informacyjny PIONIER PKI). Subskrybent odbierający certyfikat MOŻE otrzymać również pełny łańcuch certyfikatów, czyli zestaw wszystkich certyfikatów umożliwiających weryfikację (lista w formacie PKCS#7 zakodowana do postaci PEM lub DER).

## 4.4 Akceptacja certyfikatu

Po otrzymaniu certyfikatu subskrybent ma obowiązek sprawdzenia jego poprawności. W przypadku stwierdzenia jakichkolwiek nieprawidłowości, ma on obowiązek niezwłoczne powiadomić Urząd Certyfikacji, który wydał certyfikat. W przypadku zgłoszenia braku akceptacji wydanego certyfikatu, Urząd Certyfikacji, który wydał certyfikat unieważnia certyfikat. Brak akceptacji certyfikatu, nie odbiera użytkownikowi prawa do złożenia nowego wniosku certyfikacyjnego.

Urząd Certyfikacji ma prawo publikacji każdego wystawionego certyfikatu za pomocą bazy katalogowej LDAP lub w repozytorium.

## 4.5 Zastosowanie certyfikatu i pary kluczy

### 4.5.1 Wykorzystanie pary kluczy i certyfikatu przez użytkownika końcowego

Subskrybenci MUSZĄ wykorzystywać certyfikaty wyłącznie do zastosowań określonych niniejszą polityką i zgodnie z warunkami stosowania określonymi w certyfikacie,

Subskrybenci MOGĄ wykorzystywać certyfikaty, których treść odpowiada stanowi faktycznemu. Jeśli uległy zmianie dane dotyczące subskrybenta, to subskrybent MUSI zlecić Urzędowi Certyfikacji unieważnienie certyfikatu.

Certyfikowany klucz prywatny NIE MOŻE być wykorzystywany przed akceptacją certyfikatu ani po unieważnieniu lub wygaśnięciu certyfikatu.

Certyfikowany klucz prywatny MUSI być wykorzystywany wyłącznie na rzecz podmiotu dla którego został wystawiony certyfikat.

### 4.5.2 Wykorzystanie klucza publicznego i certyfikatu przez stronę ufającą

Strona ufająca certyfikatom POWINNA zapoznać się z niniejszą polityką przed wyciągnięciem jakichkolwiek wniosków dotyczących zaufania certyfikatowi wydanemu zgodnie z niniejszą polityką. Strona ufająca POWINNA:

- wykorzystywać certyfikaty wyłącznie do zastosowań określonych niniejszą polityką i zgodnie z warunkami stosowania określonymi w certyfikacie,
- zweryfikować podpis w certyfikacie subskrybenta przy pomocy ważnego certyfikatu Urzędu Certyfikacji pobranego w bezpieczny sposób,

- akceptować akcje dokonane z użyciem certyfikatu wyłącznie w okresie jego ważności,
- przed podjęciem decyzji sprawdzić status certyfikatu w oparciu o listę CRL pobraną z repozytorium Urzędu Certyfikacji nie dawniej niż 24 godziny.

## 4.6 Odnowienie certyfikatu dla tej samej pary kluczy

### 4.6.1 Zasady odnawiania certyfikatów

Odnowienie certyfikatu w oparciu o te same klucze prywatne jest możliwe wyłącznie dla certyfikatów przechowywanych na karcie kryptograficznej. Jeśli od pierwszej certyfikacji z tym samym kluczem prywatnym minęło więcej niż 6 lat, to kolejne odnowienie certyfikatu w oparciu o te same klucze prywatne nie jest możliwe. W takim wypadku subskrybent MOŻE wystąpić o ponowną certyfikację dla nowej pary kluczy.

Urząd Certyfikacji może wydać kolejny certyfikat z tą samą nazwą wyróżnioną wyłącznie jeśli można jednoznacznie stwierdzić, że wnioskujący podmiot jest tym samym, dla którego został wystawiony poprzedni certyfikat.

### 4.6.2 Podmioty uprawnione do wnioskowania o odnowienia certyfikatu

Zgodnie z punktem 4.1.1.

### 4.6.3 Postępowanie przy odnawianiu certyfikatu

Jak w punkcie 4.2. Uwierzytelnianie podmiotu odbywa się zgodnie z punktem 3.3.

## 4.7 Odnowienie certyfikatu dla nowej pary kluczy

### 4.7.1 Zasady odnawiania certyfikatów

Urząd Certyfikacji może wydać kolejny certyfikat z tą samą nazwą wyróżnioną wyłącznie, jeśli można jednoznacznie stwierdzić, że wnioskujący podmiot jest tym samym, dla którego został wystawiony poprzedni certyfikat.

Certyfikat zostaje odnowiony z datą wystawienia certyfikatu w Urzędzie Certyfikacji, chyba że we wniosku podany jest inny termin. W przypadku podania terminu odnowienia certyfikatu we wniosku, data rozpoczęcia ważności certyfikatu nie może być późniejsza niż **90 dni** od momentu złożenia wniosku.

Czynność ponownej certyfikacji NIE MOŻE zostać zrealizowana, gdy poprzedni certyfikat został odwołany lub uległ już przedawnieniu.

### 4.7.2 Podmioty uprawnione do odnowienia certyfikatu

Zgodnie z punktem 4.1.1.

### 4.7.3 Postępowanie przy odnawianiu certyfikatu

Jak w punkcie 4.2. Uwierzytelnianie podmiotu odbywa się zgodnie z punktem 3.3.

## 4.8 Zmiana danych w certyfikacie

Urząd Certyfikacji PIONIER PKI CA-WCSS-2 nie dopuszcza możliwości zmian danych w certyfikacie. W przypadku zmiany danych, użytkownik ma obowiązek unieważnić certyfikat i wystąpić o nowy certyfikat z prawidłowymi danymi.

## 4.9 Unieważnianie certyfikatu

### 4.9.1 Okoliczności unieważnienia certyfikatu

Urząd Certyfikacji MUSI odwołać certyfikat w następujących przypadkach:

- nastąpiło zgłoszenie żądania unieważnienia przez właściciela certyfikatu lub uprawnionego użytkownika (dotyczy certyfikatów innych niż osobiste),
- uległy zmianie dane dotyczące subskrybenta,
- została naruszona wiarygodność klucza prywatnego subskrybenta lub istnieje takie podejrzenie,
- wiadomo, że subskrybent naruszył swoje zobowiązania.

### 4.9.2 Podmioty uprawnione do zgłaszania żądań unieważnienia certyfikatu

Z wnioskiem o odwołanie certyfikatu MOŻE wystąpić jego właściciel, osoba uprawniona (dotyczy certyfikatów innych niż osobiste), urząd certyfikacji, urząd rejestracji oraz jednostka dostarczająca dowód naruszenia wiarygodności klucza lub nieaktualności danych.

### 4.9.3 Postępowanie przy unieważnianiu certyfikatu

Jednostka żądająca odwołania MUSI zostać uwierzytelniona przez Urząd Certyfikacji lub Urząd Rejestracji zgodnie z punktem 3.4.

Urząd Certyfikacji ma prawo w uzasadnionych przypadkach sam podjąć decyzję o unieważnieniu certyfikatu.

### 4.9.4 Zwłoka występowania o unieważnienie certyfikatu

Podmiot uprawniony do zgłaszania żądań unieważnienia certyfikatu (patrz punkt 4.9.2) powinien wystąpić z takim wnioskiem niezwłocznie po uzyskaniu informacji skutkującej koniecznością unieważnienia certyfikatu (zgodnie z punktem 4.9.1).

### 4.9.5 Czas reakcji na żądanie unieważnienia certyfikatu

Zlecenie odwołania certyfikatu MUSI zostać zrealizowane w ciągu **24 godzin** od jego przyjęcia przed odpowiedni urząd.

### 4.9.6 Obowiązek sprawdzania unieważnień przez strony ufające

Strona ufająca MUSI sprawdzić ważność certyfikatu w oparciu o listę unieważnionych certyfikatów opublikowaną przez Urząd Certyfikacji PIONIER PKI CA-WCSS-2, pobieraną z repozytorium nie rzadziej niż raz dziennie.

### 4.9.7 Częstotliwość publikacji list CRL

Lista unieważnionych certyfikatów jest aktualizowana za każdym razem, gdy ulega odwołaniu certyfikat wystawiony przez ten urząd i nie później niż **7 dni** przed końcem ważności aktualnej listy CRL.

### 4.9.8 Maksymalne opóźnienie publikacji listy unieważnionych certyfikatów (CRL)

Lista unieważnionych certyfikatów jest kopiowana na nośnik danych i przenoszona do repozytorium niezwłocznie po jej sporządzeniu. Lista unieważnionych certyfikatów MUSI być dostępna w repozytorium najpóźniej **1 godzinę** po sporządzeniu.

### 4.9.9 Dostępność weryfikacji unieważnień w trybie online

Urząd Certyfikacji działający w ramach PIONIER PKI udostępnia możliwość sprawdzania unieważnienia, bądź statusu certyfikatu online. Sprawdzenie unieważnienia, bądź statusu certyfikatu online odbywa się w oparciu o protokół OCSP. Dostęp do usługi OCSP odbywa się pod adresem: `http://ocsp.pki.pionier.net.pl`.

### 4.9.10 Obowiązek sprawdzania unieważnień w trybie online

Strona ufająca NIE MUSI weryfikować statusu certyfikatu w trybie online.

### 4.9.11 Warunki zawieszania certyfikatu

Polityka Certyfikacji nie przewiduje możliwości zawieszania i odwieszania wydanych certyfikatów.

## 4.10 Udostępnianie statusu certyfikatów

Urząd Certyfikacji PIONIER PKI CA-WCSS-1 udostępnia status certyfikatów poprzez listy unieważnionych certyfikatów (CRL) oraz przez usługę online opartą o protokół OCSP.

Lista unieważnionych certyfikatów (CRL) jest ważna maksymalnie **30 dni** od daty wystawienia i zawiera certyfikaty, których data ważności jeszcze nie minęła, a które zostały unieważnione.

Najnowsza lista CRL i usługa OCSP są dostępne publicznie. Urząd Certyfikacji PIONIER PKI CA-WCSS-1 dokłada wszelkich starań, by usługi CRL i OCSP były dostępne przez całą dobę przez siedem dni w tygodniu.

# 5 Zabezpieczenia organizacyjne, operacyjne i fizyczne

## 5.1 Zabezpieczenia fizyczne

### 5.1.1 Lokalizacja

Urządzenia działające w ramach Urzędu Certyfikacji znajdują się w budynkach oraz pomieszczeniach należących do instytucji będącej operatorem Urzędu Certyfikacji (Politechnika Wrocławska, Wrocławskie Centrum Sieciowo-Superkomputerowe).

Serwer, którego używa Urząd Certyfikacji, do publikacji informacji w repozytoriach danych, znajduje się w siedzibie Wrocławskiego Centrum Sieciowo-Superkomputerowego, w pomieszczeniu do którego dostęp jest ograniczony.

### 5.1.2 Dostęp fizyczny

Stacje robocze Urzędu Certyfikacji MUSZĄ być umieszczone w pomieszczeniach zabezpieczonych fizycznie. Dostęp do nich mogą mieć wyłącznie osoby posiadające zatwierdzone uprawnienia do wykonywania zadań operatora urzędu. To samo odnosi się do zapasowych stacji roboczych oraz zdeponowanych nośników danych związanych z procesem certyfikacji.

### 5.1.3 Nośniki informacji

W zależności od zastosowania nośnikami informacji powinny być urządzenia (bądź materiały) przeznaczone do zapisu i odczytu, bądź tylko do odczytu.

Nośniki informacji przechowywane są w pomieszczeniu, w którym znajduje się dedykowana stacja robocza Urzędu Certyfikacji.

### 5.1.4 Niszczenie informacji

Zbędne dokumenty papierowe, dokumenty w formie elektronicznej oraz inne nośniki informacji używane przez Urząd Certyfikacji są niszczone w bezpieczny sposób, zgodnie z obowiązującymi przepisami prawa, normami i standardami. Proces niszczenia musi być trwały i uniemożliwić uzyskanie informacji z niszczonego nośnika.

### 5.1.5 Kopia bezpieczeństwa poza siedzibą

Kopia klucza prywatnego oraz podpisany certyfikat Urzędu Certyfikacji zdeponowany jest w bezpiecznym miejscu o ograniczonym dostępie (sejfie). Kopie o których mowa składowane są w formie elektronicznej na nośniku niekasowalnym oraz w formie wydruku na papierze.

## 5.2 Zabezpieczenia proceduralne

### 5.2.1 Zaufane role

W działalności Urzędu Certyfikacji określone są role, które są połączone z funkcją w Urzędzie Certyfikacji. Lista ról Urzędu Certyfikacji:

1. Administrator systemu
   Osoba mająca fizyczny dostęp do urządzeń Urzędu Certyfikacji oraz Urzędu Rejestracji, jak również logiczny dostęp do systemu operacyjnego oraz oprogramowania realizującego funkcjonalność Urzędu Certyfikacji oraz Urzędu Rejestracji.
2. Operator Urzędu Certyfikacji
   Operatorami Urzędów Certyfikacji są osoby posiadające uprawnienia do wystawiania certyfikatów oraz list odwołanych certyfikatów.
3. Operator Urzędu Rejestracji
   Rolę operatora Urzędu Rejestracji powierza się zaufanej osobie, wskazanej przez instytucję, dla której Urząd Rejestracji pełni funkcje rejestracyjne. Osoba taka zobowiązuje się do przestrzegania zasad niniejszego dokumentu.
4. Audytor Systemu
   Osoba mająca uprawnienia do kontroli prawidłowości funkcjonowania Urzędu Certyfikacji oraz Urzędu Rejestracji.

### 5.2.2 Liczba osób wymaganych do zadania

W działalności Urzędu Certyfikacji określona jest liczba osób, pełniących odpowiednie role, do wykonania zadań funkcjonalnych Urzędu Certyfikacji. I tak:

- zmiana kluczy Urzędu Certyfikacji: 2 operatorów
- podpisanie klucza użytkownika końcowego: 1 operator
- unieważnienie certyfikatu użytkownika końcowego: 1 operator
- utworzenie listy unieważnionych certyfikatów (CRL): 1 operator
- przeprowadzenie audytu: 2 operatorów i audytorzy

### 5.2.3 Identyfikacja i uwierzytelnienie osób pełniących zaufane role

Osoby pełniące role muszą zostać zidentyfikowane i uwierzytelnione przed rozpoczęcieciem pracy w ramach Urzędu Certyfikacji lub Urzędu Rejestracji.

## 5.3 Zabezpieczenia osobowe

Urząd Certyfikacji ponosi odpowiedzialność za właściwe przygotowanie i kompetencje swoich oper-atorów, a także gwarantuje operatorom dostęp do wszystkich narzędzi potrzebnych w procesie certyfikacji. Urząd Rejestracji zapewnia poufność i bezpieczeństwo swoich danych. Urząd Certyfikacji zapewnia bezpieczeństwo i poufność procesu komunikacji między Urzędem Certyfikacji, a swoimi Urzędami Rejestracji.

## 5.4 Procedury rejestrowania zdarzeń

### 5.4.1 Rodzaje rejestrowanych informacji

Urząd Certyfikacji rejestruje następujące zdarzenia:

- złożenie wniosku o certyfikację,
- złożenie wniosku o unieważnienie certyfikatu,
- logowanie do dedykowanej stacji roboczej,
- wystawienie certyfikatu,
- unieważnienie certyfikatu,
- utworzenie listy odwołanych certyfikatów.

Każde zdarzenie MUSI zawierać informację czasową (znacznik czasowy) systemu w którym jest rejestrowane oraz identyfikator operatora, który wykonał rejestrowaną czynność lub przyjął wniosek.

### 5.4.2 Częstotliwość przetwarzania rejestrów zdarzeń

Kopia zapasowa rejestrów zdarzeń MUSI być tworzona nie rzadziej niż **1 raz w tygodniu**.

### 5.4.3 Okres przechowywania rejestrów zdarzeń

Rejestry zdarzeń MUSZĄ być przechowywane **5 lat** od zarejestrowanego zdarzenia, mającego miejsce w Urzędzie Certyfikacji PIONIER PKI CA-WCSS-2.

### 5.4.4 Ochrona rejestrów zdarzeń

Rejestry zdarzeń znajdują się w systemie plików na komputerze, którego zdarzenia są rejestrowane.

### 5.4.5 Procedura tworzenia kopii zapasowych rejestrów zdarzeń

Pliki zawierające rejestry zdarzeń MUSZĄ być przechowywane na zewnętrznym nośniku niekasowalnym. Archiwizacja rejestrów zdarzeń na nośnik zewnętrzny MUSI odbywać się nie rzadziej niż **co 1 miesiąc**.

## 5.5 Archiwizacja danych

### 5.5.1 Rodzaje archiwizowanych danych

Urząd Certyfikacji MUSI przechowywać:

- wszystkie informacje otrzymane od Urzędu Rejestracji w procesie rejestracji,
- wszystkie komunikaty wymieniane z Urzędem Rejestracji dotyczące subskrybentów,
- wszystkie komunikaty wymieniane z subskrybentami,
- rejestry zdarzeń (patrz punkt 5.4),
- dokumenty dotyczące ustanowienia Urzędów Rejestracji,
- kopie wszystkich wystawionych certyfikatów,
- kopie wszystkich wystawionych List Unieważnionych Certyfikatów (CRL).

Urząd Rejestracji MUSI przechowywać:

- wszystkie informacje i dokumenty otrzymane od subskrybenta w procesie rejestracji,
- wszystkie komunikaty wymieniane z urzędem certyfikacji dotyczące subskrybentów,
- wszystkie komunikaty wymieniane z subskrybentami.

### 5.5.2 Okres przechowywania archiwizowanych danych

Archiwizowane dane SĄ przechowywane **5 lat** po zakończeniu funkcjonowania Urzędu Certyfikacji PIONIER PKI CA-WCSS-2.

### 5.5.3 Ochrona archiwum

Wszystkie wystawione certyfikaty oraz listy odwołanych certyfikatów są przechowywane w lokalnej bazie danych Urzędu Certyfikacji. To samo dotyczy wszystkich zleceń certyfikacji, dla których wystawiono certyfikaty, komunikatów Urzędów Rejestracji związanych z certyfikacją oraz wszystkich podpisanych umów między urzędami.

Dokumenty w formie papierowej są przechowywane w pomieszczeniu, w którym znajdują się urządzenia Urzędu Certyfikacji (patrz 5.1.1).

### 5.5.4 Procedury tworzenia kopii zapasowych

Dane przechowywane w postaci elektronicznej MUSZĄ być kopiowane na zewnętrzny nośnik danych nie rzadziej niż **1 raz w tygodniu**.

### 5.5.5 Wymagania dotyczące znakowania danych znacznikiem czasu

Wszystkie archiwizowane dane, zarówno w postaci papierowej jak i elektronicznej muszą być oznaczone datą ich sporządzenia lub wpłynięcia do Urzędu Certyfikacji.

### 5.5.6 Procedury dostępu i weryfikacji zarchiwizowanych informacji

Dostęp do archiwum mają wyłącznie uprawnieni pracownicy.

## 5.6 Wymiana pary kluczy certyfikatu Urzędu Certyfikacji

W przypadku zmiany klucza Urzędu Certyfikacji, nowa para kluczy zostanie opublikowana w repozytorium (patrz punkt 2.1). Wszystkie nowe certyfikaty i listy CRL MUSZĄ być podpisywane nowym kluczem.

Informacja o zmianie kluczy jest publikowana na stronie WWW (portal informacyjny Urzędu Certyfikacji oraz portal informacyjny PIONIER PKI) oraz rozpowszechniana przez system zgłaszania problemów w PIONIER PKI (TRS).

## 5.7 Postępowanie po naruszeniu ochrony klucza i awarii

### 5.7.1 Ujawnienie lub podejrzenie ujawnienia kluczy prywatnych urzędu certyfikacji

Jeżeli stwierdzono lub podejrzewa się, iż naruszono wiarygodność klucza prywatnego urzędu certyfikacji, wówczas Urząd Certyfikacji MUSI:

- poinformować swoich subskrybentów oraz strony korzystające z jego certyfikatów,
- zaprzestać korzystania z niewiarygodnego klucza prywatnego podczas świadczenia usługi certyfikacji oraz wystawiania list odwołanych certyfikatów,
- unieważnić wszystkie wystawione certyfikaty,
- zażądać odwołania certyfikatu w nadrzędnym urzędzie certyfikacyjnym.
- wystąpić do nadrzędnego urzędu certyfikacyjnego o podpisanie nowej pary kluczy.

Jeśli certyfikat Urzędu Certyfikacji został unieważniony przez nadrzędny urząd certyfikacji, wtedy Urząd Certyfikacji MUSI poinformować swoich subskrybentów oraz strony korzystające z jego certyfikatów, a następnie albo wystąpić do nadrzędnego urzędu certyfikacyjnego o podpisanie nowej pary kluczy, albo zakończyć działalność.

Po kompromitacji klucza prywatnego Urzędu Certyfikacji, w celu zapewnienia ciągłości działania, dopuszczalne jest użycie dotychczasowych wniosków certyfikacyjnych (CSR) subskrybentów i wystawienie w oparciu o te wnioski nowych certyfikatów.

### 5.7.2 Uszkodzenie sprzętu, oprogramowania i/lub danych

W razie fizycznego uszkodzenia sprzętu uszkodzony komponent jest wymieniany na równoważny, a konfiguracja jest odtwarzana z ostatniej kopii zapasowej.

Pełna funkcjonalność POWINNA być przywrócona w ciągu **3 dni**. Dostęp do repozytorium POWINIEN być przywrócony w ciągu **24 godzin**.

W razie stwierdzenie niespójności lub uszkodzenia danych są one odtwarzane z ostatniej kopii zapasowej. W takim wypadku organizacja prowadząca Urząd Certyfikacji MUSI przeprowadzić inspekcję w celu wyjaśnienia, czy awaria nie jest wynikiem nieuprawnionego dostępu i czy ochrona klucza prywatnego nie została naruszona.

### 5.7.3 Zapewnienie ciągłości działania po katastrofach

W przypadku katastrofy uniemożliwiającej wznowienia działania Urzędu Certyfikacji w dotychczasowej lokalizacji w ciągu **3 dni** decyzję o dalszej działalności (kontynuacji, zaprzestania, przeniesienia) podejmuje organ d.s. PIONIER PKI wskazany przez *Radę Konsorcjum PIONIER*.

## 5.8 Zakończenie działalności Urzędu Certyfikacji i Urzędów Rejestracji

Jeśli Urząd Certyfikacji decyduje się zakończyć świadczenie usług certyfikacji, to POWINIEN poinformować o tym wszystkie zainteresowane strony, zakończyć dystrybucję certyfikatów i list odwołanych certyfikatów. Wszystkie wystawione certyfikaty oraz certyfikaty urzędu kończącego działalność MUSZĄ zostać odwołane.

Subskrybenci informowani są za pośrednictwem poczty elektronicznej, natomiast Strony ufające za pośrednictwem stosownego komunikatu zamieszczonego w Repozytorium oraz na stronach WWW Portalu Informacyjnego. Powiadomienie POWINNO nastąpić przynajmniej z miesięcznym wyprzedzeniem.

Jeśli Urząd Rejestracji kończy działalność to POWINIEN przekazać do Urzędu Certyfikacji wszystkie przechowywane dokumenty i pełne archiwum zgromadzonych danych. Informacje o zakończeniu działalności Urzędu Rejestracji będą zamieszczane w repozytorium oraz na stronach WWW Portalu Informacyjnego.

# 6 Zabezpieczenia techniczne

## 6.1 Tworzenie i przekazywanie pary kluczy

### 6.1.1 Tworzenie par kluczy

Klucz prywatny Urzędu Certyfikacji jest tworzony zgodnie z polityką nadrzędnego Urzędu Certyfikacji.

Użytkownik końcowy samodzielnie tworzy parę kluczy lub możliwe jest utworzenie klucza prywatnego przez Urząd Rejestracji lub Urząd Certyfikacji w imieniu użytkownika. W drugim przypadku Urząd Certyfikacji tworzy klucze przy użyciu sprzętowego modułu (karty kryptograficznej), klucze te przechowywane są na karcie kryptograficznej.

### 6.1.2 Przekazywanie klucza prywatnego użytkownikom końcowym

Klucz prywatny tworzony przez Urząd Certyfikacji lub Urząd Rejestracji zostaje umieszczony na karcie krytpograficznej (typu smartcard) i w takiej postaci przekazany do subskrybenta. Subskrybent odbiera kartę kryptoraficzną oraz identyfikator zastosowany w karcie (hasło/PIN). Dane te (hasło/PIN) mogą również zostać przekazane za pomocą bezpiecznej komunikacji sieciowej.

Urząd Certyfikacji NIE MOŻE przechowywać kluczy prywatnych subskrybentów. Klucz prywatny jest usuwany z wszystkich nośników i urządzeń niezwłocznie po jego przekazaniu subskrybentowi.

### 6.1.3 Dostarczanie klucza publicznego do Urzędu Certyfikacji

Subskrybenci, którzy sami wygenerowali parę kluczy i przygotowali zlecenie certyfikacji przekazują to zlecenie do Urzędu Rejestracji. Urząd Rejestracji przekazuje je Urzędowi Certyfikacji za pomocą bezpiecznej komunikacji sieciowej.

### 6.1.4 Dostarczanie użytkownikom klucza publicznego urzędu certyfikacyjnego

Certyfikat Urzędu Certyfikacji PIONIER PKI CA-WCSS-2 jest dostępny w repozytorium (patrz punkt 2.1).

### 6.1.5 Długość klucza

Klucz prywatny Urzędu Certyfikacji PIONIER PKI CA-WCSS-2 MUSI mieć długość co najmniej **2048 bitów**.

Klucz prywatny użytkownika końcowego POWINIEN mieć długość co najmniej **2048 bitów**. W uzasadnionych przypadkach (np. zastosowanie certyfikatu w aplikacji z ograniczoną długością klucza) Urząd Certyfikacji może podpisać certyfikat dla klucza o długości mniejszej niż 2048 bity.

### 6.1.6 Zastosowanie kluczy zgodnie z rozszerzeniami X.509 v3

Certyfikaty wystawiane przez Urząd Certyfikacji PIONIER PKI CA-WCSS-2 mogą być wykorzystywane zgodnie z wartością ustawianą w polu "KeyUsage" rozszerzenia x.509 v3.

## 6.2 Ochrona klucza prywatnego

Klucz prywatny związany z certyfikatem osobistym NIE MOŻE być udostępniany innym osobom, ani NIE MOŻE być przesyłany i przechowywany w postaci niezaszyfrowanej.

Klucz prywatny związany z certyfikatem infrastruktury NIE MOŻE być używany przez osoby inne niż osoby odpowiedzialne za dany element infrastruktury i MOŻE być przechowywany w systemie plików w postaci niezaszyfrowanej pod warunkiem zapewnienia ograniczenia dostępu tylko dla upoważnionych użytkowników.

### 6.2.1 Standard modułu kryptograficznego

Klucze prywatne Urzędu Certyfikacji PIONIER PKI CA-WCSS-2 SĄ przechowywane w postaci zaszyfrowanej na nośniku typu karta kryptograficzna o standardzie bezpieczeństwa nie niższym niż FIPS 140-2 . Klucz MUSI być chroniony hasłem.

### 6.2.2 Kontrola klucza prywatnego w schemacie N z M

Klucz prywatny Urzędu Certyfikacji PIONIER PKI CA-WCSS-2 nie jest kontrolowany w schemacie N z M. Do użycia klucza prywatnego wystarczy jeden operator.

### 6.2.3 Deponowanie klucza prywatnego

Klucz prywatny Urzędu Certyfikacji PIONIER PKI CA-WCSS-2, ani klucze prywatne subskrybentów, którym urząd których generuje klucze nie podlegają operacji deponowania (ang. key escrow).

### 6.2.4 Kopie bezpieczeństwa klucza prywatnego

Nie przewiduje się przechowywania kopii zapasowych kluczy prywatnych subskrybentów. Kopia zapasowa klucza prywatnego Urzędu Certyfikacji PIONIER PKI CA-WCSS-2 jest zdeponowana w bezpiecznym miejscu o ograniczonym dostępie (sejfie).

Subskrybenci którzy utworzyli parę kluczy w postaci plików MOGĄ tworzyć kopie zapasowe klucza prywatnego. Dopuszczalne jest zapisywanie klucza prywatnego w paczkach PKCS#12 zabezpieczonych odpowiednim hasłem (PIN).

### 6.2.5 Archiwizacja klucza prywatnego

Po utracie ważności certyfikatu Urzędu Certyfikacji klucz prywatny MUSI być archiwizowany przez okres minimum **5 lat**. Klucz jest przechowywany w ten sam sposób jak przed wygaśnięciem, na karcie kryptograficznej.

Urząd Certyfikacji nie archiwizuje kluczy prywatnych subskrybentów.

### 6.2.6 Przechowywanie klucza prywatnego w module kryptograficznym

Klucz prywatny MUSI być przechowywany w postaci zaszyfrowanej.

### 6.2.7 Sposób aktywacji klucza prywatnego

Klucz prywatny Urzędu Certyfikacji aktywowany jest przez włożenie do czytnika kart kryptograficznych i podanie PINu lub hasła.

Aktywacja klucza prywatnego subskrybentów wymaga podania przez właściciela odpowiedniego PINu lub hasła.

Certyfikat infrastruktury (serwera) MOŻE nie wymagać aktywacji przy pomocy hasła.

### 6.2.8 Niszczenie klucza prywatnego

Klucz prywatny MUSI zostać zniszczony w sposób trwały uniemożliwiający jego odtworzenie. Procedura niszczenia klucza prywatnego Urzędu Certyfikacji MUSI być przeprowadzona w sposób komisyjny (w obecności minimum 2 osób mających uprawnienia operatora Urzędu Certyfikacji).

## 6.3 Inne aspekty zarządzania kluczami

### 6.3.1 Archiwizacja kluczy publicznych

Wszystkie klucze publiczne, na podstawie których dokonano certyfikacji są archiwizowane przez Urząd Certyfikacji.

### 6.3.2 Okresy ważności kluczy

Ważność kluczy prywatnych dla wystawianych certyfikatów osobistych NIE MOŻE być dłuższa niż **12 miesięcy**, natomiast dla wystawianych certyfikatów infrastruktury NIE MOŻE być dłuższy niż **36 miesięcy**.

Ważność klucza prywatnego Urzędu Certyfikacji PIONIER PKI CA-WCSS-2 wynosi **6 lat**.

## 6.4 Dane aktywacyjne

### 6.4.1 Generowanie danych aktywujących

Hasła używane do ochrony danych Urzędu Certyfikacji na karcie kryptograficznej POWINNY być definiowane przez Urząd Certyfikacji i MUSZĄ być nie krótsze niż 8 znaków. Hasła używane do ochrony danych Subskrybenta na karcie kryptograficznej POWINNY być definiowane przez Subskrybenta lub Urząd Rejestracji i nie krótsze niż 8 znaków.

Hasło używane do aktywacji klucza, który nie jest przechowywany na karcie kryptograficznej jest tworzone przez Subskrybenta, POWINNO być odporne na ataki brutalne i mieć długość co najmniej 8 znaków.

### 6.4.2 Ochrona danych aktywujących

Hasła MUSZĄ być tak przechowywane, by nie trafiły do osób nieupoważnionych. Hasła NIE MOGĄ być zapisywane i przesyłane w postaci niezaszyfrowanej.

## 6.5 Zabezpieczanie systemów komputerowych

Urząd Certyfikacji MUSI używać stacji roboczej zarezerwowanej do zadań związanych z usługami certyfikacyjnymi w ramach PIONIER PKI. Stacja robocza MUSI być zabezpieczona fizycznie przed nieautoryzowanym dostępem. Stacja robocza NIE MOŻE mieć żadnego połączenia sieciowego z innym komputerem lub urządzeniem (uwzględniając połączenie logiczne oraz fizyczne). Wymiana danych między tą stacją a resztą środowiska biorącego udział w procesie certyfikacji musi odbywać się za pomocą zewnętrznych nośników danych.

Dostęp do stacji roboczej MUSI być zabezpieczony hasłem o długości minimum 8 znaków lub systemem haseł jednorazowych.

Funkcjonalność systemu operacyjnego oraz uruchomione oprogramowanie MUSZĄ być ograniczone do niezbędnego do realizacji zadań Urzędu Certyfikacji.

Stacja robocza jest monitorowana, rejestrowana jest aktywność w systemie oraz próby nieautoryzowanego dostępu.

## 6.6 Kontrola techniczna

Instalacja, konfiguracja i wymiana sprzętu, jak również instalacja, aktualizacja oraz konfiguracja systemu operacyjnego i oprogramowania MUSI być dokonywana przez operatorów Urzędu Certyfikacji PIONIER PKI CA-WCSS-1 lub pod ich bezpośrednim nadzorem.

## 6.7 Kontrola bezpieczeństwa sieci

Stacja robocza Urzędu Certyfikacji dedykowana do realizacji zadań podpisywania certyfikatów (w której znajduje się klucz prywatny Urzędu Certyfikacji) NIE MOŻE mieć żadnego połączenia

sieciowego z innym komputerem lub urządzeniem (uwzględniając połączenie logiczne oraz fizyczne).

Publiczny serwer Urzędu Certyfikacji podłączony jest do sieci publicznej chronionej zaporą sieciową. Dozwolone są połączenia z sieci publicznej do stacji z repozytorium danych oraz stacji realizującej funkcjonalność OCSP w celu pobrania udostępnianych danych.

# 7 Profile certyfikatów i list CRL

## 7.1 Profil certyfikatów

### 7.1.1 Numer wersji

Wszystkie certyfikaty wystawiane przez Urząd Certyfikacji PIONIER PKI CA-WCSS-2 muszą być zgodne ze standardem X.509 v3.

### 7.1.2 Pola rozszerzeń

#### Certyfikat urzędu certyfikacji

| | |
|---|---|
| Key Usage | keyCertSign, cRLSign<br>**Rozszerzenie krytyczne.** |
| Basic Constraints | CA=true<br>**Rozszerzenie krytyczne.** |
| Authority Key Identifier | sygnatura klucza prywatnego<br>**Rozszerzenie niekrytyczne.** |
| Subject Key Identifier | sygnatura klucza prywatnego<br>**Rozszerzenie niekrytyczne.** |
| CRL Distribution Points | Adres URL listy CRL<br>**Rozszerzenie niekrytyczne.** |
| Certification Policy | Identyfikator OID Polityki Certyfikacji<br>**Rozszerzenie niekrytyczne.** |

#### Certyfikaty osobiste

| | |
|---|---|
| Key Usage | digitalSignature, keyEncipherment<br>**Rozszerzenie krytyczne.** |
| Basic Constraints | CA=false<br>**Rozszerzenie krytyczne.** |
| Authority Key Identifier | sygnatura klucza Urzędu Certyfikacji<br>**Rozszerzenie niekrytyczne.** |
| Subject Key Identifier | sygnatura klucza prywatnego<br>**Rozszerzenie niekrytyczne.** |
| CRL Distribution Points | Adres URL listy CRL<br>**Rozszerzenie niekrytyczne.** |
| Certification Policy | Identyfikator OID Polityki Certyfikacji<br>**Rozszerzenie niekrytyczne.** |
| Extended Key Usage | clientAuth<br>**Rozszerzenie niekrytyczne.** |

#### Certyfikaty poczty elektronicznej

| | |
|---|---|
| Key Usage | digitalSignature, nonRepudiation, keyEncipherment<br>**Rozszerzenie krytyczne.** |

| | |
|---|---|
| Basic Constraints | CA=false<br>**Rozszerzenie krytyczne.** |
| Authority Key Identifier | sygnatura klucza Urzędu Certyfikacji<br>**Rozszerzenie niekrytyczne.** |
| Subject Key Identifier | sygnatura klucza prywatnego<br>**Rozszerzenie niekrytyczne.** |
| CRL Distribution Points | Adres URL listy CRL<br>**Rozszerzenie niekrytyczne.** |
| Certification Policy | Identyfikator OID Polityki Certyfikacji<br>**Rozszerzenie niekrytyczne.** |
| Subject Alternative Name | Jeden lub więcej adresów e-mail, osoby posługującej się danym certyfikatem.<br>**Rozszerzenie niekrytyczne.** |
| Extended Key Usage | clientAuth, emailProtection<br>**Rozszerzenie niekrytyczne.** |

### Certyfikaty serwerów

| | |
|---|---|
| Key Usage | digitalSignature, keyEncipherment<br>**Rozszerzenie krytyczne.** |
| Basic Constraints | CA=false<br>**Rozszerzenie krytyczne.** |
| Authority Key Identifier | sygnatura klucza Urzędu Certyfikacji<br>**Rozszerzenie niekrytyczne.** |
| Subject Key Identifier | sygnatura klucza prywatnego<br>**Rozszerzenie niekrytyczne.** |
| CRL Distribution Points | Adres URL listy CRL<br>**Rozszerzenie niekrytyczne.** |
| Certification Policy | Identyfikator OID Polityki Certyfikacji<br>**Rozszerzenie niekrytyczne.** |
| Subject Alternative Name | Jedna lub więcej pełnych nazw domenowych serwera, posługującego się danym certyfikatem.<br>**Rozszerzenie niekrytyczne.** |
| Extended Key Usage | serverAuth<br>**Rozszerzenie niekrytyczne.** |

### Certyfikatów dla usług i aplikacji

| | |
|---|---|
| Key Usage | digitalSignature, keyEncipherment<br>**Rozszerzenie krytyczne.** |
| Basic Constraints | CA=false<br>**Rozszerzenie krytyczne.** |
| Authority Key Identifier | sygnatura klucza Urzędu Certyfikacji<br>**Rozszerzenie niekrytyczne.** |
| Subject Key Identifier | sygnatura klucza prywatnego<br>**Rozszerzenie niekrytyczne.** |
| CRL Distribution Points | Adres URL listy CRL<br>**Rozszerzenie niekrytyczne.** |
| Certification Policy | Identyfikator OID Polityki Certyfikacji<br>**Rozszerzenie niekrytyczne.** |
| Subject Alternative Name | Jedna lub więcej pełnych nazw domenowych serwera, posługującego się danym certyfikatem.<br>**Rozszerzenie niekrytyczne.** |

| | |
|---|---|
| Extended Key Usage | serverAuth, clientAuth<br>**Rozszerzenie niekrytyczne.** |

**Certyfikaty do podpisywania kodów**

| | |
|---|---|
| Key Usage | digitalSignature<br>**Rozszerzenie krytyczne.** |
| Basic Constraints | CA=false<br>**Rozszerzenie krytyczne.** |
| Authority Key Identifier | sygnatura klucza Urzędu Certyfikacji<br>**Rozszerzenie niekrytyczne.** |
| Subject Key Identifier | sygnatura klucza prywatnego<br>**Rozszerzenie niekrytyczne.** |
| CRL Distribution Points | Adres URL listy CRL<br>**Rozszerzenie niekrytyczne.** |
| Certification Policy | Identyfikator OID Polityki Certyfikacji<br>**Rozszerzenie niekrytyczne.** |
| Subject Alternative Name | Adres e-mail<br>**Rozszerzenie niekrytyczne.** |
| Extended Key Usage | codeSigning<br>**Rozszerzenie niekrytyczne.** |

### 7.1.3 Stosowane algorytmy

W certyfikatach wystawianych przez Urząd Certyfikacji PIONIER PKI CA-WCSS-1 stosowane są algorytmy:

- rsaEncryption (OID 1.2.840.113549.1.1.4)
- sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5)

Inne algorytmy NIE POWINNY być stosowane. W szczególności NIE MOGĄ być stosowane algorytmy md5WithRSA i DSAWithSHA1.

### 7.1.4 Postać nazw

Certyfikat Urzędu Certyfikacji PIONIER PKI CA-WCSS-2 ma nazwę wyróżnioną postaci: *C=PL, O=PIONIER, O=WCSS, CN=Urzad Certyfikacji PIONIER PKI CA-WCSS-2*

Nazwy wyróżnione w certyfikatach subskrybentów mają następującą strukturę:

- C=PL
- ST: lokalizacja województwo - pole opcjonalne, niezalecane
- L: lokalizacja miasto - pole opcjonalne, niezalecane
- O=PIONIER
- O: nazwa instytucji - pole obowiązkowe

- OU: nazwa jednostki organizacyjnej w ramach instytucji - pole opcjonalnie, może wystąpić kilkukrotnie
- CN: nazwa podmiotu
- CN: dodatkowa nazwa rozróżniająca nadawana przez Urząd Certyfikacji
- Email: adres e-mail subskrybenta - pole opcjonalne, niezalecane

### 7.1.5 Ograniczenia nazw

Nazwa instytucji w polu O musi być zgodna z umową zawartą pomiędzy Urzędem Certyfikacji a daną instytucją. Nazwa w polu "O" MUSI być pełną nazwą instytucji lub jej powszechnie używanym skrótem i MUSI być zapisana przy użyciu liter języka polskiego lub być transliteracją do zestawu znaków ASCII.

Każda instytucja może zdefiniować hierarchię stosowanych pól. Właściwy Urząd Rejestracji POWINIEN zapewnić spójność stosowanych nazw.

W certyfikatach dla osób fizycznych pole "CN" w nazwie wyróżnionej MUSI zawierać imię i nazwisko zgodnie z przedstawionym dokumentem tożsamości. Imię i nazwisko MUSI być zapisane zgodnie z zapisem w dokumencie tożsamości lub za pomocą transkrypcji do znaków zestawu ASCII. Pole "CN" MOŻE zawierać drugie imię lub inicjał.

W certyfikatach pseudoanonimowych nazwa podmiotu w polu "CN" MUSI być poprzedzona tekstem *„alias: "* W certyfikatach infrastruktury pole "CN" w nazwie wyróżnionej MUSI zawierać pełną nazwę domenową. Opcjonalnie nazwa domenowa może być poprzedzona nazwą usługi i ukośnikiem "/".

Urząd Certyfikacji ma decydujący głos w spornych sprawach dotyczących nazwy wyróżnionej subskrybenta.

### 7.1.6 Identyfikator Polityki Certyfikacji

Identyfikator Polityki Certyfikacji zgodnie z którą certyfikat został wydany. jest zawarty w certyfikatach subskrybentów w polu rozszerzenia `certificatePolicies`.

## 7.2 Profil list CRL

### 7.2.1 Numer wersji

Urząd Certyfikacji PIONIER PKI CA-WCSS-2 wystawia listy CRL w formacie X.509 wersja 2.

### 7.2.2 Pola listy CRL

Lista CRL (Certificate Revocation List) zawiera następujące pola:

- Version: `2 (0x1)`

- Signature Algorithm: `sha1WithRSAEncryption`
- Issuer: `C=PL, O=PIONIER, O=WCSS, CN=Urzad Certyfikacji PIONIER PKI CA-WCSS-2`
- LastUpdate: ... *Data ostatniej aktualizacji*
- NextUpdate: ... *Data następnej aktualizacji*
- Revoked Certificates
  - Serial Number: ... *Numer seryjny odwołanego certyfikatu*
  - Revocation Date: ... *Data odwołania certyfikatu*

# 8 Audyty

## 8.1 Audyt zgodności

### 8.1.1 Częstotliwość audytu

Urząd Certyfikacji PIONIER PKI CA-WCSS-2 nie rzadziej niż **1 raz w roku** MUSI przeprowadzić wewnętrzną kontrolę usług i zgodności funkcjonowania z Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego. W ramach kontroli Urząd Certyfikacji MUSI przeprowadzić kontrolę wszystkich aktualnie ustanowionych Urzędów Rejestracji.

Zewnętrzny audyt może być przeprowadzony na wniosek organizacji prowadzącej nadrzędny Urząd Certyfikacji lub organu d.s. PIONIER PKI wskazanego przez *Radę Konsorcjum PIONIER*.

Zewnętrzny audyt może być również przeprowadzony na wniosek organizacji zarządzającej polityką certyfikacji (ang. Policy Management Authority), której członkiem jest Urząd Certyfikacji PIONIER PKI CA-WCSS-2.

Koszt audytu jest w całości ponoszony przez organizację wnioskującą.

### 8.1.2 Tożsamość/kwalifikacje audytora

Audytor MUSI posiadać

- wystarczające, potwierdzone kwalifikacje,
- kompletne informacje o jednostce organizacyjnej, która administruje audytowanym Urzędem Certyfikacji,
- kompletne informacje o audytowanym Urzędzie Certyfikacji (w szczególności znać politykę certyfikacji).

### 8.1.3 Związek audytora z audytowaną jednostką

Audyt wewnętrzny jest przeprowadzony przez pracowników jednostki prowadzącej Urzędu Certyfikacji PIONIER PKI CA-WCSS-2.

Audyt zewnętrzny jest przeprowadzany przez osoby wskazane przez wnioskodawcę.

### 8.1.4 Zagadnienia obejmowane przez audyt

W ramach audytu sprawdzana jest zgodność procedur stosowanych prze Urząd Certyfikacji i Urzędy Rejestracji z procedurami zdefiniowanymi w niniejszym dokumencie.

### 8.1.5 Działania podejmowane w celu usunięcia usterek wykrytych podczas audytu

W przypadku wykrycia niezgodności między stosowanymi procedurami a procedurami zdefiniowanymi w niniejszym dokumencie, Urząd Certyfikacji MUSI przygotować raport zawierający sposoby usunięcia niezgodności i planowany czas ich wdrożenia.

### 8.1.6 Informowanie o wynikach audytu

O wynikach audytu informowani są:

1. Administrator systemu.
2. Operator Urzędu Certyfikacji PIONIER PKI CA-WCSS-2.
3. Operator nadrzędnego urzędu certyfikacji dla Urzędu Certyfikacji PIONIER PKI CA-WCSS-2.
4. Organ d.s. PIONIER PKI wskazany przez *Radę Konsorcjum PIONIER*.
5. Organ zlecający audyt.

# 9 Inne postanowienia

## 9.1 Opłaty

Nie przewiduje się pobierania opłat za świadczenie usług certyfikacyjnych.

## 9.2 Odpowiedzialność finansowa

Urząd Certyfikacji nie ponosi odpowiedzialności finansowej za certyfikaty wystawione w ramach niniejszej Polityki Certyfikacji.

## 9.3 Informacje poufne

Urząd Certyfikacji PIONIER PKI CA-WCSS-2 traktuje jako informacje poufne wszystkie informacje związane z realizowanymi przez siebie usługami poza informacjami dostępnymi publicznie w repozytorium.

Pracownicy Urzędu Certyfikacji i Urzędów Rejestracji zobowiązani są do zachowania w tajemnicy informacji poufnych uzyskanych w związku z pełnioną funkcją.

Urząd Certyfikacji ujawnia informacje poufne organom administracyjnym i sądowym zgodnie z istniejącymi uregulowaniami prawnymi.

## 9.4 Ochrona danych osobowych

Urząd Certyfikacji PIONIER PKI CA-WCSS-2 traktuje jako dane osobowe wszystkie informacje o subskrybentach uzyskane w związku z realizowanymi przez siebie usługami, poza informacjami zawartymi w certyfikatach i listach odwołanych certyfikatów. Dane osobowe są przetwarzane zgodnie Ustawą o ochronie danych osobowych. Urząd Certyfikacji przy podpisywaniu umowy MUSI informować subskrybentów o przetwarzaniu ich danych osobowych przez Urząd Certyfikacji PIONIER PKI CA-WCSS-2 oraz o przysługujących im w związku z tym prawach.

Urząd Certyfikacji ujawnia dane osobowe organom administracyjnym i sądowym zgodnie z istniejącymi uregulowaniami prawnymi.

## 9.5 Ochrona praw autorskich

Urząd Certyfikacji NIE MOŻE rościć sobie jakichkolwiek praw własności intelektualnej do wydanych certyfikatów.

Prawa autorskie do niniejszej polityki posiada Konsorcjum PIONIER.

Niniejsza polityka może być kopiowana, drukowana i rozpowszechniana pod warunkiem zachowania jej w całości oraz podania źródła informacji.

## 9.6 Udzielane gwarancje

Urząd Certyfikacji PIONIER PKI CA-WCSS-2 gwarantuje przestrzeganie procedur opisanych w niniejszym dokumencie.

## 9.7 Zwolnienia z domyślnie udzielanych gwarancji

Urząd Certyfikacji PIONIER PKI CA-WCSS-2 działa z dochowaniem należytej staranności, w oparciu o fakty uznane za wiarygodne, jednak nie gwarantuje, że są one w pełni dokładne, kompletne i aktualne.

## 9.8 Ograniczenia odpowiedzialności

Urząd Certyfikacji PIONIER PKI CA-WCSS-2 nie ponosi odpowiedzialności za szkody poniesione w wyniku decyzji podjętych na podstawie działań Urzędu Certyfikacji PIONIER PKI CA-WCSS-2 i podległych Urzędów Rejestracji, na podstawie informacji przez nie dostarczonych ani na podstawie wystawionych certyfikatów i list unieważnionych certyfikatów.

## 9.9 Przepisy przejściowe i okres obowiązywania polityki certyfikacji

Polityka Certyfikacji obowiązuje do odwołania lub zmiany.

## 9.10 Określanie trybu komunikacji z odbiorcami

Urząd Certyfikacji PIONIER PKI CA-WCSS-2 będzie komunikował się z odbiorcami poprzez:

- portal informacyjny PIONIER PKI `www.pki.pionier.net.pl`,
- korespondencję e-mail,
- osobiście.

## 9.11 Zmiany w polityce certyfikacji

Dopuszcza się realizację zmian typu edytorskiego w niniejszej polityce. Aktualizacje dotyczących aspektów technicznych lub proceduralnych POWINNY być publikowanie w portalu informacyjnym z **30 dniowym** uprzedzeniem.

Wszelkie zmiany w dokumencie polityki certyfikacji, z wyjątkiem drobnych zmian edycyjnych, wymagają nadania nowego identyfikatora OID.

## 9.12 Obowiązujące prawo

Działalność Urzędu Certyfikacji PIONIER PKI CA-WCSS-2 opisanego niniejszą polityką podlega prawu polskiemu.

W rozumieniu prawa polskiego, tj. ustawy o podpisie elektronicznym, Dziennik Ustaw 130 z dnia 15.11.2001r., Urząd Certyfikacji PIONIER PKI CA-WCSS-2 nie jest kwalifikowanym podmiotem świadczącym usługi certyfikacyjne.

## 9.13 Procedura rozstrzygania sporów

W kwestiach spornych, wynikających z korzystania z usług certyfikacyjnych i interpretacji Polityki Certyfikacji wiążące interpretacje wydaje **Organ d.s. PIONIER PKI wskazany przez *Radę Konsorcjum PIONIER***, będący organem nadzorującym prace Urzędu Certyfikacji PIONIER PKI CA-WCSS-2.

Przy braku polubownego rozwiązania sporu, może on zostać skierowany do sądu powszechnego właściwego dla siedziby Urzędu Certyfikacji PIONIER PKI CA-WCSS-2.

Powyższy dokument został zatwierdzony 12 listopada 2010 roku przez **Zespół projektu PIONIER PKI wskazany przez *Radę Konsorcjum PIONIER***.