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-root-ca.pdf**
Zadanie:	**2b**
Partner(zy):	**PCSS, WCSS, UMK, PS**
Partner odpowiedzialny:	**WCSS**
Klasyfikacja:	**Do użytku publicznego**
Data publikacji:	**26 listopada 2010**

Abstrakt: Dokument Polityk Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego opisuje procedury stosowane przez Główny Urząd Certyfikacji PIONIER PKI Root-CA 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	28/10/2010	Pierwsza wersja dokumentu	Ireneusz Tarnowski
0.2	04/11/2010	Zmiany zespołu	Ireneusz Tarnowski
0.3	09/11/2010	Ostateczna wersja dokumentu	Ireneusz Tarnowski
1.0	12/11/2010	Zaakceptowana wersja dokumentu	Ireneusz Tarnowski

Zespół projektu PIONIER PKI zatwierdzający niniejszą politykę:

1. Adam Osuchowski (CK PŚ)
2. Grzegorz Kosicki (WCSS)
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

Głównym Urzędzie Certyfikacji PIONIER PKI Root-CA

wersja dokumentu: 1.0
data publikacji: 23 listopada 2010

Spis treści

1 Wstęp

Urząd Certyfikacji **PIONIER PKI Root-CA** jest głównym urzędem certyfikacji w hierarchii PIONIER PKI i świadczy usługi certyfikacji dla pośrednich urzędów certyfikacji w sieci PIONIER.

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 Główny Urząd Certyfikacji PIONIER PKI Root-CA podczas certyfikacji klucza publicznego, definiuje uczestników tego procesu oraz określa obszary zastosowań certyfikatów uzyskanych w tym procesie.

Polityka certyfikacji obowiązuje od dnia uruchomienia Głównego Urzędu Certyfikacji PIONIER PKI Root-CA, tj. od dnia 23 listopada 2010.

Zadaniem Głównego Urzędu Certyfikacji PIONIER PKI Root-CA jest poświadczanie swoim podpisem elektronicznym kluczy publicznych pośrednich urzędów certyfikacji w infrastrukturze PIONIER PKI.

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

Główny Urząd Certyfikacji PIONIER PKI Root-CA 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 Root-CA`***
- Wersja: `0.1`
- Data: `1 listopada 2010`

- OID: `1.3.6.1.4.1.36065.1.0.1.0.1`

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
0 *Root-CA*
1 Polityka Certyfikacji
0 Major version
1 Minor version

1.3 Podmioty

1.3.1 Urzędy Certyfikacji

Główny Urząd Certyfikacji PIONIER PKI Root-CA jest częścią infrastruktury PIONIER PKI.

Główny Urząd Certyfikacji PIONIER PKI Root-CA poświadcza wyłącznie certyfikaty innych urzędów certyfikacji.

1.3.2 Urzędy Rejestracji

Urząd Certyfikacji występuje jednocześnie jako Urząd Rejestracji.

1.3.3 Subskrybenci

Certyfikaty Urzędu Certyfikacji PIONIER PKI Root-CA wydawane są wyłącznie dla subskrybentów, będących podmiotami (instytucjami) przyłączonymi do sieci PIONIER, w szczególności związanych ze środowiskiem naukowo-badawczym i akademickim.

Subskrybentami MOGĄ być wyłącznie podmioty (instytucje) ubiegające się o certyfikat (posługujące się certyfikatem), uprawnione do otrzymania (posługiwania się) certyfikatu.

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 Root-CA.

Strona ufająca NIE MUSI być Subskrybentem usług certyfikacyjnych Urzędu Certyfikacji PIONIER PKI Root-CA, a jej działania polegają wówczas na 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 Root-CA MOGĄ być stosowane jako certyfikaty Urzędów Certyfikacji niższego poziomu, służąc do poświadczania kluczy publicznych Urzędów Certyfikacji najniższego poziomu.

1.4.2 Zabronione zastosowania

Certyfikaty wystawiane przez PIONIER PKI Root-CA 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 organ d.s. PIONIER PKI wskazany przez *Radę Konsorcjum PIONIER*.

Organ d.s. PIONIER PKI wskazany przez *Radę Konsorcjum PIONIER*:

```
Biuro Konsorcjum PIONIER
ul.  Noskowskiego 10
61-704 Poznań
tel.:  +48 61 858 20 00
fax:  +48 61 852 59 54

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

1.5.2 Kontakt

Organ d.s. PIONIER PKI wskazany przez *Radę Konsorcjum PIONIER*:

```
Biuro Konsorcjum PIONIER
ul.  Noskowskiego 10
61-704 Poznań
```

tel.: +48 61 858 20 00
fax: +48 61 852 59 54

http://root-ca.pki.pionier.net.pl
e-mail: root-ca@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*) - podrzędny urząd certyfikacji; występujący w rozbudowanej hierarchii PKI urząd podrzędny, posiadający certyfikat klucza publicznego wydany przez urząd nadrzędny

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 Root-CA jest dostępne w serwisie WWW pod adresem `http://root-ca.pki.pionier.net.pl`.

2.2 Publikowane informacje

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

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 Root-CA 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).

3.1.2 Konieczność używania nazw znaczących

Nazwa wyróżniona stosowana w certyfikacie MUSI pozwalać na jednoznaczną identyfikację pośredniego Urzędu Certyfikacji, dla którego wystawiony został certyfikat.

3.1.3 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.

3.1.4 Unikatowość nazw

Nazwa wyróżniona MUSI być unikatowa dla każdego Urzędu Certyfikacji certyfikowanego przez Urząd Certyfikacji PIONIER PKI Root-CA.

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

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

3.2.2 Uwierzytelnienie instytucji

Urząd Rejestracji MUSI sprawdzić, czy podmiot ubiegający się o certyfikat jest uprawniony do uzyskania certyfikatu z Urzędu Certyfikacji PIONIER PKI Root-CA.

3.2.3 Uwierzytelnienie danych osoby fizycznej

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

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

3.3 Identyfikacja i uwierzytelnianie przy ponownej rejestracji

Uwierzytelnienie podmiotu ubiegającego się o certyfikat (ponowną rejestrację) musi się odbywać zgodnie z procedurą pierwszej rejestracji opisaną w punkcie 3.2.3.

Jeśli certyfikat podmiotu stracił ważność lub został unieważniony, to uwierzytelnienie podmiotu 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 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 PIONIER PKI Root-CA MOGĄ zostać wystawione dla Urzędów Certyfikacji, które mają pełnić rolę pośrednich Urzędów Certyfikacji w infrastrukturze PIONIER PKI. Ich właścicielem jest PIONIER, natomiast operatorem organizacja przyłączona w sposób pośredni lub bezpośredni do sieci PIONIER. O certyfikat Urzędu Certyfikacji MUSI wystąpić osoba odpowiedzialna za funkcjonowanie danego Urzędu Certyfikacji.

Certyfikaty PIONIER PKI Root-CA MOGĄ zostać wystawione dla Urzędów Certyfikacji, w których spełnione są wytyczne dotyczące zabezpieczeń fizycznych, technicznych, osobowych oraz proceduralnych wymagane dla Pośrednich Urzędów Certyfikacji zdefiniowane w Regulaminie Usług Certyfikacyjnych PIONIER PKI.

4.1.2 Zasady składania wniosków o wydanie certyfikatu

Subskrybent MUSI zapoznać się i zaakceptować Politykę Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego i potwierdzić to podpisanym oświadczeniem.

Subskrybent wraz z podpisanym oświadczeniem MUSI przedstawić, zaakceptowaną przez organ nadzorujący niniejszą politykę, Politykę Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego Urzędu Certyfikacji, dla którego ubiega się o podpisanie klucza publicznego.

Subskrybent przygotowuje zlecenie certyfikacji w formacie PKCS10 i przekazuje je do Urzędu Rejestracji.

4.2 Przetwarzanie wniosku o wydanie certyfikatu

4.2.1 Weryfikacja tożsamości

Niezbędne jest potwierdzenie prawa podmiotu występującego o certyfikat do funkcjonowania jako Urząd Certyfikacji i wydawania certyfikatów dla użytkowników końcowych danej organizacji (instytucji).

4.2.2 Zasady akceptacji i odrzucania wniosków o wydanie certyfikatu

Wniosek zostaje zaakceptowany, jeśli:

- parametry techniczne są zgodne z niniejszym dokumentem,
- wnioskodawca został uwierzytelniony,

- wnioskodawca podpisał oświadczenie o akceptacji Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego,
- wnioskodawca przedstawił zaakceptowaną, przez organ nadzorujący niniejszą, politykę Politykę Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego, dla którego ubiega się o podpisanie klucza publicznego.

Jeśli wniosek o certyfikat nie spełnia wymagań technicznych, to wnioskodawca jest o tym fakcie informowany i wezwany do poprawienia wniosku.

Wnioskodawca jest informowany o odrzuceniu wniosku i przyczynach odrzucenia.

4.2.3 Czas przetwarzania wniosku wydanie certyfikatu

Certyfikat zostaje wystawiony w ciągu **30 dni** od skompletowania niezbędnych dokumentów (wymienionych w punkcie 4.2.2.

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. 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 w repozytorium każdego wystawionego certyfikatu.

4.5 Zastosowanie certyfikatu i pary kluczy

4.5.1 Wykorzystanie pary kluczy i certyfikatu

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

Urząd Certyfikacji nie odnawia certyfikatów w oparciu o tą samą parę kluczy.

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 Root-CA nie dopuszcza możliwości zmian danych w certyfikacie. W przypadku zmiany danych, podmiot posługujący się certyfikatem, 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,
- uległy zmianie dane dotyczące subskrybenta,
- została naruszona wiarygodność klucza prywatnego subskrybenta lub istnieje takie podejrzenie,
- subskrybent utracił prawo do certyfikatu (opisane w punkcie 4.1.1),
- subskrybent, we wskazanym czasie, nie wykonał zaleceń wynikających z audytu zewnętrznego,
- subskrybent, we wskazanym czasie, nie dostosował własnej polityki certyfikacji do polityki nadrzędnego urzędu certyfikacji,
- 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, urząd certyfikacji 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 zgodnie z punktem 3.4.

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

Urząd Certyfikacji informuje organ nadzorujący 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 niezwłocznie (z zachowaniem procedury) od jego przyjęcia.

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 Root-CA, 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

Główny Urząd Certyfikacji PIONIER PKI Root-CA nie udostępnia możliwości sprawdzania unieważnienia, bądź statusu certyfikatu online.

4.9.10 Warunki zawieszania certyfikatu

Polityka Certyfikacji nie przewiduje możliwości zawieszania i odwieszania wydanych certyfikatów.

4.10 Udostępnianie statusu certyfikatów

Urząd Certyfikacji PIONIER PKI Root-CA udostępnia status certyfikatów poprzez listy unieważnionych certyfikatów (CRL).

Lista unieważnionych certyfikatów (CRL) jest ważna maksymalnie **1 rok** od daty wystawienia i zawiera certyfikaty, których data ważności jeszcze nie minęła, a które zostały unieważnione.

Najnowsza lista CRL jest dostępna publicznie. Urząd Certyfikacji PIONIER PKI Root-CA dokłada wszelkich starań, by usługa CRL była 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 Głównego Urzędu Certyfikacji znajdują się w budynkach oraz pomieszczeniach należących do instytucji będącej operatorem Głównego Urzędu Certyfikacji (Politechnika Wrocławska, Wrocławskie Centrum Sieciowo-Superkomputerowe).

Serwer, którego używa Głównego 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

Stacja robocza 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.

System plików z danymi Urzędu Certyfikacji oraz karta kryptograficzna z kluczem prywatnym przechowywane są w bezpiecznym miejscu, do którego dostęp mają wyłącznie upoważnione osoby (operatorzy urzędu 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 (Kancelaria Tajna Politechniki Wrocławskiej). 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
   Operatorami Urzędu Rejestracji są operatorzy Urzędu Certyfikacji.
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 podmiotu: 2 operatorów
- unieważnienie certyfikatu podmiotu: 2 operatorów
- utworzenie listy unieważnionych certyfikatów (CRL): 1 operator
- przeprowadzenie audytu: 2 operatorów i audytorzy

Dodatkowo, w zadaniach, w których niezbędnych jest 2 operatorów, MUSZĄ oni przynależeć do różnych podmiotów (organizacji).

5.2.3 Identyfikacja i uwierzytelnienie osób pełniących zaufane role

Osoby pełniące rolą operatora Urzędu Certyfikacji wyznaczone są przez podmiot zarządzający danym Urzędem Certyfikacji.

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 operatorów, a także gwarantuje operatorom dostęp do wszystkich narzędzi potrzebnych w procesie certyfikacji. Urząd Certyfikacji zapewnia poufność i bezpieczeństwo swoich danych.

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 miesiącu**.

5.4.3 Okres przechowywania rejestrów zdarzeń

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

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 3 miesiące**.

5.5 Archiwizacja danych

5.5.1 Rodzaje archiwizowanych danych

Urząd Certyfikacji MUSI przechowywać:

- wszystkie informacje i dokumenty otrzymane od subskrybenta w procesie rejestracji,
- wszystkie komunikaty wymieniane z subskrybentami.
- rejestry zdarzeń (patrz punkt 5.4),
- kopie wszystkich wystawionych certyfikatów,
- kopie wszystkich wystawionych List Unieważnionych Certyfikatów (CRL).

5.5.2 Okres przechowywania archiwizowanych danych

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

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.

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 miesiącu**.

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 osoby uprawnione.

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

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 oraz Strony ufające informowane są za pośrednictwem stosownego komunikatu zamieszczonego w Repozytorium oraz na stronach WWW Portalu Informacyjnego. Powiadomienie POWINNO nastąpić przynajmniej z miesięcznym wyprzedzeniem.

6 Zabezpieczenia techniczne

6.1 Tworzenie i przekazywanie pary kluczy

6.1.1 Tworzenie par kluczy

Klucz prywatny Głównego Urzędu Certyfikacji jest tworzony zgodnie z niniejszą polityką.

Podmiot występujący o certyfikat samodzielnie tworzy parę kluczy.

6.1.2 Przekazywanie klucza prywatnego użytkownikom końcowym

Klucz prywatny Subskrybenta nigdy nie jest w posiadaniu Urzędu Certyfikacji.

6.1.3 Dostarczanie klucza publicznego do Urzędu Certyfikacji

Subskrybenci, którzy sami wygenerowali parę kluczy i przygotowali zlecenie certyfikacji przekazują to zlecenie do Głównego Urzędu Certyfikacji.

6.1.4 Dostarczanie użytkownikom klucza publicznego urzędu certyfikacyjnego

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

6.1.5 Długość klucza

Klucz prywatny Głównego Urzędu Certyfikacji PIONIER PKI Root-CA MA długość **2048 bitów**.

Klucz prywatny podmiotu występującego o certyfikat POWINIEN mieć długość co najmniej **2048 bitów**.

6.1.6 Zastosowanie kluczy zgodnie z rozszerzeniami X.509 v3

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

6.2 Ochrona klucza prywatnego

Klucz prywatny Subskrybenta NIE MOŻE być używany przez inny podmiot, niż odpowiedzialny za Urząd Certyfikacji dla którego wystawiony został certyfikat. Klucz prywatny Subskrybenta MOŻE być przechowywany w systemie plików w postaci zaszyfrowanej pod warunkiem zapewnienia ograniczenia dostępu tylko dla upoważnionych użytkowników.

6.2.1 Standard modułu kryptograficznego

Klucze prywatne Urzędu Certyfikacji PIONIER PKI Root-CA 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 Root-CA jest kontrolowany w schemacie N z M. Do użycia klucza prywatnego niezbędna jest obecność dwóch operatorów.

6.2.3 Deponowanie klucza prywatnego

Klucz prywatny Urzędu Certyfikacji PIONIER PKI Root-CA nie podlega operacji deponowania (ang. key escrow).

6.2.4 Kopie bezpieczeństwa klucza prywatnego

Kopia zapasowa klucza prywatnego Urzędu Certyfikacji PIONIER PKI Root-CA jest zdeponowana w bezpiecznym miejscu o ograniczonym dostępie (Kancelaria Tajna Politechniki Wrocławskiej).

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.

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.

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 NIE MOŻE być dłuższa niż **20 lat** i nie może być dłuższa niż ważność klucza prywatnego Głównego Urzędu Certyfikacji PIONIER PKI Root-CA.

Ważność klucza prywatnego Głównego Urzędu Certyfikacji PIONIER PKI Root-CA wynosi **20 lat**.

6.4 Dane aktywacyjne

6.4.1 Generowanie danych aktywujących

Hasło używane do ochrony danych Urzędu Certyfikacji POWINNY być definiowane przez Urząd Certyfikacji i MUSZI być nie krótsze niż 8 znaków. Hasła używane do ochrony danych Subskrybenta POWINNY być definiowane przez Subskrybenta i nie krótsze niż 8 znaków.

6.4.2 Ochrona danych aktywujących

Hasła MUSZĄ być tak przechowywane, by nie trafiły do osób nieupoważnionych. Hasła NIE MOGĄ być przesyłane w postaci niezaszyfrowanej. Hasła MOGĄ być zapisywane, z zastrzeżeniem rozdzielności zapisanego hasła i elementu, który jest chroniony przez dane hasło.

6.5 Zabezpieczanie systemów komputerowych

Główny 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.

Dane Urzędu Certyfikacji oraz konfiguracja oprogramowania znajdują się na zewnętrznym (względem stacji roboczej), przenośnym systemie plików. Klucz prywatny Urzędu Certyfikacji znajduje się na karcie kryptograficznej. System plików z danymi Urzędu Certyfikacji oraz karta kryptograficzna z kluczem prywatnym są włączane do stacji roboczej tylko w trakcie wykonywania prac przez operatora Urzędu Certyfikacji.

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 Root-CA lub pod ich bezpośrednim nadzorem. Powyższe prace mogą być wykonywane wyłącznie, gdy stacja robocza nie zawiera kluczy prywatnych Urzędu Certyfikacji.

6.7 Kontrola bezpieczeństwa sieci

Stacja robocza Urzędu Certyfikacji dedykowana do realizacji zadań podpisywania certyfikatów (w ktróej znajduje się klucz prywatny Urzędu Certyfikacji) NIE MOŻE mieć żadnego połączenia sieciowego z innym komputerem lub urządzeniem (uwzględniając połączenie logiczne oraz fizyczne).

7 Profile certyfikatów i list CRL

7.1 Profil certyfikatów

7.1.1 Numer wersji

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

7.1.2 Pola rozszerzeń

Certyfikat urzędu certyfikacji

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

Certyfikaty podległych urzędów certyfikacji

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

7.1.3 Stosowane algorytmy

W certyfikatach wystawianych przez Urząd Certyfikacji PIONIER PKI Root-CA 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 Root-CA ma nazwę wyróżnioną postaci: *C=PL, O=PIONIER, CN=PIONIER PKI Root CA*

Nazwy wyróżnione w certyfikatach subskrybentów mają następującą strukturę:

- C=PL
- O=PIONIER
- CN: nazwa pośredniego urzędu certyfikacji - pole obowiązkowe

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.

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 Root-CA 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, CN=PIONIER PKI Root CA`

- 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 Root-CA nie rzadziej niż **1 raz w roku** MUSI przeprowadzić wewnętrzną kontrolę usług i zgodności funkcjonowania z Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego.

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

Koszt audytu jest w całości ponoszony przez organizację wnioskującą.

8.1.2 Tożsamość/kwalifikacje audytora

Audytor MUSI posiadać

- wystarczające, potwierdzone kwalifikacje,
- 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 Root-CA.

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 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. Operatorzy Głównego Urzędu Certyfikacji PIONIER PKI.
3. Organ d.s. PIONIER PKI wskazany przez *Radę Konsorcjum PIONIER.*
4. Organ zlecający audyt.

9 Inne postanowienia

9.1 Opłaty

Nie przewiduje się pobierania opłat za świadczenie usług certyfikacyjnych.

9.2 Odpowiedzialność finansowa

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

9.3 Informacje poufne

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

Pracownicy Urzędu Certyfikacji 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

Główny Urząd Certyfikacji PIONIER PKI Root-CA nie gromadzi, jak również nie przetwarza danych osobowych.

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

Główny Urząd Certyfikacji PIONIER PKI Root-CA gwarantuje przestrzeganie procedur opisanych w niniejszym dokumencie.

9.7 Zwolnienia z domyślnie udzielanych gwarancji

Główny Urząd Certyfikacji PIONIER PKI Root-CA 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

Główny Urząd Certyfikacji PIONIER PKI Root-CA nie ponosi odpowiedzialności za szkody poniesione w wyniku decyzji podjętych na podstawie działań Głównego Urzędu Certyfikacji PIONIER PKI Root-CA, 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 Root-CA 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.

O zmianach w polityce informowane są podległe Urzędy Certyfikacji, tj. takie, których certyfikat został podpisany przez Urząd Certyfikacji Root-CA. Podległe Urzędy Certyfikacji MUSZĄ dostosować swoją politykę do zmieinonej polityki Urzędu Certyfikacji Root-CA.

9.12 Obowiązujące prawo

Działalność Głównego Urzędu Certyfikacji PIONIER PKI Root-CA opisanego niniejszą polityką podlega prawu polskiemu.

W rozumieniu prawa polskiego, tj. ustawy o podpisie elektronicznym, Dziennik Ustaw 130 z dnia 15.11.2001r., Główny Urząd Certyfikacji PIONIER PKI Root-CA 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 Głównego Urzędu Certyfikacji PIONIER PKI Root-CA.

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

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