Polityka Certyfikacji

i Kodeks Postępowania Certyfikacyjnego

Centrum Certyfikacji PL-Grid Simple CA

Wersja 1.6

Październik 2014

1 Wprowadzenie

PL-Grid Simple CA jest centrum certyfikacji najwyższego poziomu i działa na potrzeby polskiego środowiska gridowego tworzącego i korzystającego z Infrastruktury PL-Grid.

1.1 Opis dokumentu

Poniższy dokument opisuje procedury stosowane przez Centrum Certyfikacji PL-Grid Simple CA podczas certyfikacji klucza publicznego, definiuje uczestników tego procesu oraz określa obszary zastosowań certyfikatów uzyskanych w tym procesie. Dokument ten jest dostępny pod adresem: http://plgrid-sca.wcss.wroc.pl.

1.2 Nazwa dokumentu i identyfikator polityki

Tytuł: Polityka certyfikacji i Kodeks Postępowania Certyfikacyjnego Centrum Certyfikacji PL-Grid Simple CA

Wersja: Wersja 1.6 (30 października 2014)

OID: 1.3.6.1.4.1.35629.1.1.1.1.6

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
35629	PL-Grid
1	Dokumenty
1	PL-Grid Simple CA
1	Polityka Certyfikacji
1	Numer wersji (major)
6	Numer wersji (minor)

1.3 Środowisko działania

Centrum certyfikacji PL-Grid Simple CA poświadcza swoim podpisem elektronicznym klucze publiczne użytkowników końcowych. PL-Grid Simple CA działa na potrzeby polskiego środowiska gridowego związanego z Infrastrukturą PL-Grid. Stroną ufającą są właściciele zasobów udostępnianych w ramach Infrastruktury.

1.3.1 Urzędy certyfikacji

Centrum certyfikacji PL-Grid Simple CA nie wystawia certyfikatów dla urzędów certyfikacji niższego poziomu.

1.3.2 Urzędy rejestracji

Centrum Certyfikacji PL-Grid Simple CA występuje jednocześnie jako urząd rejestracji. W uzasadnionych przypadkach, w odpowiedzi na zapotrzebowanie środowiska PL-Grid, Centrum Certyfikacji może powoływać kolejne urzędy rejestracji. Rolę automatycznego urzędu rejestracji pełni oprogramowanie działające w Infrastrukturze PL-Grid, po zatwierdzeniu przez Centrum Certyfikacji zgodności jego działania z niniejszą Polityką. Ponadto, rolę urzędu rejestracji powierza się zaufanej osobie, wskazanej przez CA. Osoba taka zobowiązuje się do przestrzegania zasad niniejszego dokumentu i musi zostać zatwierdzona przez Centrum Certyfikacji. Lista aktualnych urzędów rejestracji dostępna jest w repozytorium Centrum. Lista ta jest weryfikowana i aktualizowana przynajmniej raz na rok.

1.3.3 Użytkownicy końcowi

Zgodnie z niniejszym dokumentem, użytkownikiem końcowym jest osoba, serwer lub usługa. Użytkownicy końcowi to:

(a) Zarejestrowani użytkownicy Infrastruktury lub osoby zatrudnione przy obsłudze i rozwoju Infrastruktury (zwane dalej "pracownikami Infrastruktury");
(b) Uczestnicy szkoleń organizowanych z wykorzystaniem Infrastruktury PL-Grid;
(c) Serwer lub usługa działająca w ramach Infrastruktury PL-Grid.

1.3.4 Obszar zastosowania

Certyfikaty wystawiane przez PL-Grid Simple CA wykorzystywane są w ramach Infrastruktury PL-Grid. Wydawane są następujące typy certyfikatów:

(a) Certyfikaty osobiste;
(b) Certyfikaty usług;
(c) Certyfikaty serwerów.

1.4 Adresy kontaktowe

Za Politykę Certyfikacji odpowiada Wrocławskie Centrum Sieciowo-Superkomputerowe z siedzibą we Wrocławiu.

Osobą kontaktową w sprawach polityki i kodeksu postępowania certyfikacyjnego jest:

Bartłomiej Balcerek
Wrocławskie Centrum Sieciowo-Superkomputerowe, Politechnika Wrocławska
Wybrzeże Wyspiańskiego 27
50-370 Wrocław, Polska
tel.: +48 71 3202079 / +48 71 3203921
fax: +48 71 3225797
e-mail: plgrid-sca@pwr.edu.pl

2 Zasady ogólne

W tej części polityki są przedstawione zobowiązania, jakie przyjmuje na siebie każda ze stron uczestniczących w procesie certyfikacji. Ponadto ustala się finansowe aspekty korzystania z usług Centrum, poziom niezawodności usługi oraz dopuszczalne metody dystrybucji informacji związanej z procesem certyfikacji.

2.1 Obowiązki

2.1.1 Obowiązki urzędu certyfikacji

Urząd certyfikacji dysponuje zawsze jednym operatorem gotowym do wykonania bieżących zadań. Przynajmniej dwie osoby są uprawnione i przygotowane do wykonywania obowiązków operatora urzędu certyfikacji i rejestracji.

Do zadań urzędu certyfikacji należy:

(a) Świadczenie usługi certyfikacji zgodnie z niniejszą Polityką Certyfikacji;
(b) Przyjmowanie zleceń certyfikacji użytkowników końcowych;
(c) Uwierzytelnianie jednostek ubiegających się o certyfikację (np. za pomocą odpowiedniego urzędu rejestracji);
(d) Wystawianie certyfikatów klucza publicznego X.509 na podstawie otrzymanych zleceń;
(e) Przekazywanie zwrotne gotowego certyfikatu zleceniodawcy;
(f) Obsługa zleceń unieważnienia certyfikatów;
(g) Wystawianie i publikowanie listy unieważnionych certyfikatów;
(h) Ochrona danych zleceniodawcy i przetwarzanie ich wyłącznie do celów związanych z usługami certyfikacji;
(i) Informowanie urzędu rejestracji o wystawieniu i unieważnieniu certyfikatu.

2.1.2 Obowiązki urzędu rejestracji

Do zadań urzędu rejestracji należy:

(a) Działanie zgodnie z niniejszą polityką pełniąc usługę uwierzytelniania;
(b) Sprawdzanie poprawności powiązania klucza publicznego z identyfikatorem jego użytkownika;
(c) Zatwierdzanie zleceń certyfikacji i wysyłanie ich do PL-Grid Simple CA;
(d) Wysyłanie zleceń unieważnienia certyfikatu do PL-Grid Simple CA.

2.1.3 Obowiązki subskrybenta

Subskrybent, czyli użytkownik końcowy, zobowiązuje się:

(a) Przestrzegać zasad niniejszej polityki;
(b) Właściwie chronić swój klucz prywatny (patrz p. 6.4.1);
(c) Upoważnić urząd certyfikacji do przetwarzania danych do celów związanych z usługami certyfikacji;
(d) Występować do urzędu certyfikacji o unieważnienie certyfikatu, gdy zajdzie przynajmniej jedna z przesłanek wymienionych w p. 4.4.1 niniejszej polityki;

(e) Nie udostępniać certyfikatu osobom trzecim.

2.1.4 Obowiązki strony ufającej certyfikatom

Strona ufająca certyfikatom jest zobowiązana do:

(a) Zapoznania się z niniejszą polityką przed wyciągnięciem jakichkolwiek wniosków dotyczących zaufania certyfikatowi wydanemu zgodnie z tą polityką;
(b) Sprawdzenia statusu certyfikatu przed podjęciem decyzji o zaufaniu certyfikatowi;
(c) Używania certyfikatu tylko do celów zgodnych z jego przeznaczeniem.

2.1.5 Obowiązki repozytorium

Urząd certyfikacji PL-Grid Simple CA jest zobowiązany do utrzymywania informacyjnej strony WWW i publikowania na tej stronie informacji o Centrum (patrz 2.6). Ponadto, ma obowiązek niezwłocznego publikowania danych po ich zmianie.

2.1.6 Obowiązki prowadzącego szkolenie

Osoba prowadząca szkolenie, wnioskująca o certyfikaty dla uczestników szkolenia jest zobowiązana do:

(a) Udostępnienia uczestnikom szkolenia niniejszej Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego;

(b) Poprawnego uwierzytelniania uczestników szkolenia przed przekazaniem certyfikatów szkoleniowych;

(c) Dostarczenia do Centrum Certyfikacji listy uczestników szkolenia z przypisanymi certyfikatami, nie później niż następnego dnia roboczego po szkoleniu.

2.2 Odpowiedzialność prawna

Pl-Grid Simple CA gwarantuje:

(a) Podjęcie wszelkich niezbędnych środków do ochrony klucza prywatnego urzędu certyfikacji przed kradzieżą, nadużyciem i utratą;

(b) Należytą weryfikację tożsamości zleceniodawcy zgodnie z niniejszą Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego;

2.3 Odpowiedzialność finansowa

Użytkownik końcowy akceptuje fakt, że urząd certyfikacji nie ponosi odpowiedzialności finansowej za certyfikaty wystawione w ramach niniejszej Polityki.

2.4 Interpretacja i egzekwowanie aktów prawnych

Postanowienia niniejszej polityki należy interpretować zgodnie z polskim prawem. W rozumieniu prawa polskiego Centrum Certyfikacji PL-Grid Simple CA nie jest kwalifikowanym podmiotem świadczącym usługi certyfikacyjne.

2.5 Opłaty

Nie przewiduje się pobierania opłat za świadczenie usług certyfikacyjnych.

2.6 Publikacja i repozytorium

PL-Grid Simple CA publikuje następujące informacje dotyczące urzędu certyfikacji:

(a) Polityka certyfikacji i kodeks postępowania certyfikacyjnego w wersjach aktualnych podczas wystawiania obecnie ważnych certyfikatów;
(b) Certyfikat urzędu certyfikacji;
(c) Lista unieważnionych certyfikatów podpisana przez urząd certyfikacji;
(d) Lista aktualnych urzędów rejestracji.

Jeżeli ulega modyfikacji polityka certyfikacji i kodeks postępowania certyfikacyjnego, to aktualna wersja tego dokumentu jest publikowana równocześnie z terminem jej wejścia w życie. Nowa lista CRL jest publikowana jak tylko zostanie wystawiona.

Nie przewiduje się żadnych niestandardowych metod ochrony dostępu do polityki certyfikacji, kodeksu postępowania certyfikacyjnego oraz list unieważnionych certyfikatów. Repozytorium jest prowadzone z zachowaniem najlepszej możliwej staranności. W uzasadnionych przypadkach Centrum zastrzega sobie prawo ograniczenia dostępu do repozytorium, z podjęciem wszelkich starań technicznych w celu przywrócenia pełnego działania usługi.

Informacja wymieniona powyżej jest utrzymywana i udostępniana za pomocą serwisu WWW pod adresem: http://plgrid-sca.wcss.wroc.pl.

2.7 Audyt zgodności

Struktura PL-Grid Simple CA może zostać poddana wewnętrznym lub zewnętrznym audytom operacyjnym w kontekście zgodności z postanowieniami polityki certyfikacji i kodeksu postępowania certyfikacyjnego. Audyty takie są przeprowadzane przynajmniej raz w roku, na wniosek instytucji zarządzającej lub Rady Konsorcjum PL-Grid i przez osoby przez nie wskazane. Raport z audytu przekazywany jest do wnioskujących i zespołu ds. bezpieczeństwa Infrastruktury PL-Grid .

2.8 Poufność

Urząd certyfikacji PL-Grid Simple CA gromadzi informacje osobiste o subskrybentach niezbędne do obsługi procesu certyfikacji. Dane te są chronione zgodnie z polskim prawem. Urząd certyfikacji nie przechowuje kluczy prywatnych subskrybentów. Jeżeli urząd generuje parę kluczy dla subskrybenta, to klucz prywatny jest usuwany z wszystkich nośników natychmiast po jego przekazaniu subskrybentowi. Na wyraźne życzenie subskrybenta klucze w postaci zaszyfrowanej mogą być składowane w zewnętrznym repozytorium będącym częścią Infrastruktury PL-Grid.

2.8.1 Typy informacji traktowane jako poufne

Wszystkie dane subskrybentów, które nie są zawarte w certyfikacie i liście unieważnionych certyfikatów, wystawionej przez PL-Grid Simple CA, są traktowane jako poufne i nie mogą być udostępniane bez wyraźnego upoważnienia subskrybenta.

2.8.2 Typy informacji nie traktowane jako poufne

Informacje zawarte w wystawionych certyfikatach klucza publicznego i listach unieważnionych certyfikatów nie są traktowane jako poufne.

2.8.3 Ujawnienie informacji o unieważnieniu/zawieszeniu certyfikatu

Kiedy certyfikat jest unieważniony/zawieszony kod przyczyny unieważnienia/zawieszenia może być zawarty we wpisie listy unieważnionych certyfikatów. Jednak żadne inne szczegóły dotyczące unieważnienia nie są ujawniane.

2.8.4 Udostępnianie informacji organom administracyjnym i sądowym

Udostępnianie wszelkich danych poufnych gromadzonych przez urząd certyfikacji jest regulowane przez przepisy prawa obowiązującego w Polsce.

2.8.5 Udostępnianie w celach naukowych

Udostępnianie wszelkich danych poufnych gromadzonych przez urząd certyfikacji jest regulowane przez przepisy prawa obowiązującego w Polsce.

2.8.6 Udostępnianie na żądanie właściciela

Udostępnianie wszelkich danych poufnych gromadzonych przez urząd certyfikacji jest regulowane przez przepisy prawa obowiązującego w Polsce.

2.8.7 Inne okoliczności udostępniania informacji

Udostępnianie wszelkich danych poufnych gromadzonych przez urząd certyfikacji jest regulowane przez przepisy prawa obowiązującego w Polsce.

2.9 Prawo do własności intelektualnej

Niniejsza polityka powstała z wykorzystaniem źródeł:

(a) RFC 2527;
(b) Polityka Certyfikacji Polskiego Centrum Certyfikacji EuroPKI.

Urząd certyfikacji nie rości sobie jakichkolwiek praw własności intelektualnej do wydanych certyfikatów lub list unieważnionych certyfikatów.

3 Identyfikacja i uwierzytelnienie

3.1 Rejestracja wstępna

3.1.1 Typy nazw

Pole podmiotu musi zawierać wyróżnioną nazwę zgodną ze standardem X.500. Nazwa certyfikatów osobistych powinna zawierać imię i nazwisko lub pseudonim osoby, dla której wystawiany jest certyfikat. Nazwa certyfikatów dla serwerów powinna zawierać pełną nazwę domenową (DNS FQDN) serwera. Nazwa certyfikatów usług powinna zawierać pełną nazwę domenową serwera (DNS FQDN) poprzedzoną nazwą usługi.

3.1.2 Konieczność nazw znaczących

Nazwa wyróżniona musi w sposób jednoznaczny identyfikować certyfikowany podmiot. Nazwa ta przybiera jedną z postaci:

(a) „C=PL, O=PL-Grid, O=Uzytkownik, O=organizacja, CN=nazwa podmiotu, CN=identyfikator podmiotu". Pierwszy i drugi parametr O są stałe. Trzeci parametr O określa instytucję, działającą w ramach polskich środowisk gridowych. Zawartość pierwszego pola CN certyfikatów osobistych musi wywodzić się z rzeczywistego imienia i nazwiska certyfikowanej osoby. Drugi parametr CN zawiera dodatkowy ciąg znaków, będący identyfikatorem użytkownika końcowego w Infrastrukturze PL-Grid.

(b) „C=PL, O=PL-Grid, O=Szkolenie, CN=nazwa podmiotu, CN=identyfikator szkolenia, CN=identyfikator podmiotu".
Pierwszy i drugi parametr O są stałe. Zawartość pierwszego pola CN musi wywodzić się z rzeczywistego imienia i nazwiska certyfikowanej osoby lub stanowić jej pseudonim. Pseudonim przyjmuje postać „Pseudonimowy N", gdzie N to kolejna wartość liczbowa (unikalna w obrębie danego szkolenia). Drugi parametr CN zawiera dodatkowy ciąg znaków, będący identyfikatorem szkolenia, który musi zawierać miejsce i datę przeprowadzania szkolenia. Trzeci parametr CN jest opcjonalny i może się pojawić, gdy uczestnik po zarejestrowaniu się na szkolenie uzyska identyfikator użytkownika w Infrastrukturze PL-Grid.

(c) „C=PL, O=PL-Grid, O=Usluga, O=organizacja, CN=nazwa podmiotu".
Pierwszy i drugi parametr O są stałe. Trzeci parametr O określa instytucję dysponującą certyfikowanym serwerem lub usługą. Parametr CN w certyfikatach dla serwerów zawiera pełną nazwę domenową (DNS FQDN), zaś dla usług przyjmuje postać „<nazwa usługi>/<nazwa domenowa serwera>".

3.1.3 Unikatowość nazw

Nazwa wyróżniona subskrybenta musi być unikatowa dla każdej jednostki podmiotu certyfikowanego przez PL-Grid Simple CA przez cały czas działania tego CA. Identyfikator podmiotu zawarty w certyfikatach osobistych nie może być przyznany kolejnej osobie. Dopuszcza się istnienie dwóch ważnych certyfikatów tego samego subskrybenta o takiej samej nazwie wyróżnionej.

3.1.4 Procedura rozwiązywania sporów wynikających z reklamacji nazw

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

3.1.5 Metody dowodu posiadania klucza prywatnego

Dopuszcza się sytuacje:

(a) Użytkownik końcowy zleca certyfikację swojego klucza publicznego (generuje parę kluczy, przygotowuje zlecenie certyfikacji i podpisuje je). Zlecenie certyfikacji musi być złożone w formacie PKCS#10. Urząd certyfikacji weryfikuje podpis pod zleceniem;

(b) Użytkownik końcowy zgłasza się do urzędu rejestracji w celu wystawienia pary kluczy oraz uzyskania certyfikatu klucza publicznego. Urząd rejestracji składa w imieniu użytkownika zlecenie certyfikacji w formacie PKCS#10. Urząd certyfikacji weryfikuje podpis pod zleceniem;

(c) Prowadzący szkolenie zgłasza się do urzędu rejestracji w celu wystawienia par kluczy dla uczestników szkolenia oraz uzyskania certyfikatów kluczy publicznych. Wniosek musi być podpisany cyfrowo ważnym certyfikatem prowadzącego.

3.1.6 Uwierzytelnianie tożsamości użytkownika

Osobę, która jest zarejestrowanym użytkownikiem lub pracownikiem Infrastruktury lub jest uczestnikem szkolenia i została zweryfikowana zgodnie z procedurami przewidzianymi w tych przypadkach, uznaje się za uwierzytelnioną. Dla pozostałych subskrybentów stosuje się weryfikację nie słabszą niż stosowane w powyższych procedurach.

W przypadku certyfikatów szkoleniowych tożsamość użytkownika końcowego może być weryfikowana przez prowadzącego szkolenie, na podstawie dokumentu pozwalającego potwierdzić tożsamość osoby (dokument zawierający zdjęcie i dane osobowe wystawiony przez organ administracji publicznej). Wówczas, prowadzący szkolenie potwierdza tożsamość uczestnika szkolenia w momencie przekazania certyfikatu. Prowadzący szkolenie uwierzytelnia się podpisując zlecenia certyfikacji certyfikatem wystawionym przez Terena TCS (https://tcs.pionier.gov.pl) lub Polish Grid CA (http://www.man.poznan.pl/plgrid-ca) lub PL-Grid Simple CA.

W przypadku certyfikatów serwerów lub usług urząd rejestracji sprawdza możliwie dokładnie czy osoba zlecająca certyfikację posiada prawo użytkowania domeny umieszczonej w zleceniu. Urząd rejestracji może zażądać przesłania przez zlecającego dodatkowych dokumentów potwierdzających to prawo. Zlecający uwierzytelnia się podpisując wiadomość zawierającą zlecenie certyfikacji lub samo zlecenie certyfikacji swoim certyfikatem osobistym wystawionym przez Terena TCS (https://tcs.pionier.gov.pl) lub Polish Grid CA (http://www.man.poznan.pl/plgrid-ca).

3.2 Odnowienie certyfikatu

Odnowienie certyfikatu tego samego klucza publicznego nie jest realizowane. Możliwe jest natomiast wydanie certyfikatu dla nowego klucza w czasie ważności poprzedniego certyfikatu, jednak nie wcześniej niż na 30 dni przed wygaśnięciem poprzedniego certyfikatu.

Czynność ponownej certyfikacji nie jest realizowana dla certyfikatów uzyskanych na potrzeby szkoleń oraz, gdy poprzedni certyfikat został unieważniony lub uległ już przedawnieniu.

Użytkownik końcowy ubiegający się o certyfikat w tym trybie musi wysłać zlecenie certyfikacji (w formacie PKCS#10) przed wygaśnięciem poprzedniego certyfikatu. W tej sytuacji nie są podejmowane procedury zmierzające do identyfikacji i uwiarygodnienia zlecenia. Ponowna certyfikacja jest możliwa wyłącznie w przypadku, gdy nie ulega zmianie wyróżniona nazwa podmiotu.

Urząd certyfikacji ma prawo odmówić ponownej certyfikacji zlecającemu użytkownikowi końcowemu.

3.3 Odnowienie po unieważnieniu

Nie jest możliwe wystawienie certyfikatu na podstawie klucza publicznego, którego poprzedni certyfikat urząd certyfikacji unieważnił. Subskrybent musi ubiegać się o certyfikat za pomocą typowych procedur.

3.4 Żądanie unieważnienia certyfikatu

Urząd certyfikacji musi zidentyfikować osobę przekazującą zlecenie unieważnienia certyfikatu. Jedną z metod uwierzytelnienia jest poświadczenie przekazywanego komunikatu własnym podpisem (do którego użyto aktualnego i ważnego certyfikatu). W innym przypadku do sprawdzenia wiarygodności zlecenia należy stosować takie same procedury, jakie obowiązują w procesie rejestrowania subskrybenta. Dopuszcza się wprowadzenie w tym celu specjalnych metod gwarantujących bezpieczną komunikację. Zgłoszenie, które jednoznacznie dostarcza dowodu kompromitacji klucza prywatnego, nie musi być uwierzytelniane.

4 Wymagania funkcjonalne

4.1 Ubieganie się o certyfikat

Użytkownik końcowy może przekazać zlecenie certyfikacji urzędowi certyfikacji. Zlecenie certyfikacji jest przygotowywane po samodzielnym wygenerowaniu pary kluczy przez użytkownika lub może on zlecić urzędowi rejestracji wygenerowanie pary kluczy i przygotowanie zlecenia certyfikacji klucza publicznego. Tożsamość subskrybenta weryfikuje wówczas urząd rejestracji.

O certyfikaty dla uczestników szkoleń mogą także wnioskować osoby prowadzące szkolenie organizowane z wykorzystaniem Infrastruktury PL-Grid, będące pracownikami Infrastruktury PL-Grid. Prowadzący wysyła wniosek o wydanie certyfikatów pocztą elektroniczną na adres PL-Grid Simple CA. Wniosek musi zawierać następujące informacje:

(a) Imię Nazwisko i adres e-mail prowadzącego;
(b) Miejsce i data szkolenia;
(c) Adres strony WWW z informacjami o szkoleniu;
(d) Lista imienna lub przewidywana liczba uczestników szkolenia.

Certyfikaty dla uczestników szkoleń wydawane są z ważnością maksymalnie 14 dni. Ważność certyfikatu jest ustalana na czas szkolenia, od godziny 0:01 pierwszego dnia szkolenia, przy czym certyfikat może być ważny maksymalnie przez 2 doby po zakończeniu szkolenia. Prowadzący szkolenie także może ubiegać się o certyfikat na potrzeby tego szkolenia, z ważnością początkową maksymalnie na 30 dni przed szkoleniem.

Maksymalny czas ważności certyfikatu użytkownika końcowego nie może przekraczać 366 dni, z wyjątkiem certyfikatów dla serwerów i usług, których ważność nie może przekraczać 1096 dni. Zlecenie certyfikacji musi być zgodne ze schematem nazewnictwa określonym w niniejszej polityce.

4.2 Wydanie certyfikatu

Urząd certyfikacji wystawia certyfikat zgodnie z polityką zdefiniowaną w niniejszym dokumencie w ciągu trzech dni roboczych. Certyfikat jest wydawany tylko po uwierzytelnieniu subskrybenta metodami zgodnymi z tą polityką (patrz p. 3.1.6.). Zleceniodawca jest powiadamiany o niepowodzeniu weryfikacji jego tożsamości i nie wydaniu certyfikatu.

Certyfikaty wystawiane przez urząd certyfikacji działający na podstawie niniejszej polityki są certyfikatami zgodnymi ze standardem X.509 v3.

Termin ważności certyfikatu nie może przekraczać okresu ważności certyfikatów zdefiniowanego w niniejszej polityce. Dopuszcza się wystawienie certyfikatu z przyszłą datą ważności.

W uzasadnionych przypadkach urząd certyfikacji ma prawo odmowy realizacji zlecenia certyfikacji.

Certyfikat może zostać wystawiony automatycznie po uwierzytelnieniu subskrybenta metodami zgodnymi z tą polityką (patrz p. 3.1.6.).

Zleceniodawca może pobrać gotowy certyfikat ze strony WWW lub otrzymać go za pomocą poczty elektronicznej lub dowolnego zewnętrznego nośnika danych (dyskietka, CD-ROM, USB). Na

wyraźne życzenie subskrybenta certyfikat może być udostępniony do pobrania w zewnętrznym repozytorium będącym częścią Infrastruktury PL-Grid.

Komunikacja między RA i CA odbywa się przy użyciu bezpiecznych metod komunikacji sieciowej (patrz p. 6.7). Zdarzenia związane z tą komunikacją są rejestrowane (patrz p. 4.5.1).

4.3 Akceptacja certyfikatu

Po otrzymaniu certyfikatu wnioskodawca ma obowiązek niezwłocznie sprawdzić jego poprawność. W przypadku zaistnienia jakichkolwiek nieprawidłowości ma on obowiązek niezwłocznie zgłosić ten fakt Centrum Certyfikacji. Brak akceptacji certyfikatu sprawia, że Centrum Certyfikacji musi unieważnić ten certyfikat (patrz p. 3.4).

Certyfikaty na potrzeby szkoleń są przekazywane użytkownikom końcowym przez prowadzącego szkolenie po potwierdzeniu rzeczywistych danych użytkownika. Użytkownik podpisuje odbiór certyfikatu i tym samym potwierdza zapoznanie się i zaakceptowanie niniejszej Polityki.

4.4 Zawieszenie i unieważnienie certyfikatu

4.4.1 Okoliczności unieważnienia certyfikatu

Urząd certyfikacji może unieważnić certyfikat w następujących przypadkach:

(a) Uległy zmianie dane dotyczące subskrybenta;
(b) Została naruszona wiarygodność klucza prywatnego subskrybenta lub istnieje takie podejrzenie;
(c) Istnieje podejrzenie, że dane zawarte w certyfikacie nie są prawdziwe;
(d) Wiadomo, że subskrybent naruszył swoje zobowiązania;
(e) Ustał związek subskrybenta z Infrastrukturą PL-Grid;
(f) Subskrybent nie potrzebuje już certyfikatu.

4.4.2 Kto może żądać unieważnienia certyfikatu

Z wnioskiem o unieważnienie certyfikatu może wystąpić jego właściciel, jednostka dostarczająca dowód zaistnienia jednej z okoliczności wymienionych w p. 4.4.1 lub urząd certyfikacji.

4.4.3 Procedura unieważniania certyfikatu

Zlecenie żądania unieważnienia musi zostać uwierzytelnione przez urząd certyfikacji.

Urząd certyfikacji akceptuje zlecenie unieważnienia, które jest podpisane cyfrowo przez właściciela certyfikatu, przy czym certyfikat ten nie może być unieważniony lub przedawniony.

Urząd certyfikacji akceptuje zlecenia unieważnienia przesyłane automatycznie przez urząd rejestracji w przypadku zmian danych identyfikujących subskrybenta w Infrastrukturze PL-Grid, w zakresie mającym wpływ na zawartość certyfikatu, oraz w przypadku gdy ustał związek subskrybenta z tą infrastrukturą. Zlecenie to musi być podpisane ważnym certyfikatem właściwym dla urzędu rejestracji. W przypadku unieważnienia w wyniku zmian danych identyfikujących subskrybenta, może nastąpić automatyczne wystawienie certyfikatu dla nowego zestawu danych subskrybenta, po

akceptacji zmian przez urząd rejestracji.

W innych przypadkach zgłoszenie unieważnienia będzie weryfikowane w sposób typowy dla zlecenia certyfikacji.

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

Zlecenie unieważnienia certyfikatu jest obsługiwane w ciągu 24 godzin roboczych od jego przyjęcia.

4.4.4 Częstotliwość publikowania list unieważnionych certyfikatów (CRL)

Urząd certyfikacji co najmniej raz w miesiącu publikuje listę unieważnionych certyfikatów. Lista ta jest aktualizowana za każdym razem, gdy ulega unieważnieniu certyfikat wystawiony przez ten urząd. Nowa lista CRL jest wystawiana przynajmniej na 3 dni przed upływem terminu ważności poprzedniej listy.

4.4.5 Wymagania dotyczące sprawdzania list unieważnionych certyfikatów

Strona ufająca musi sprawdzić ważność certyfikatu w oparciu o aktualną listę unieważnionych certyfikatów opublikowaną przez urząd certyfikacji, nie starszą niż 6 godzin.

4.5 Procedury audytu bezpieczeństwa

4.5.1 Typy rejestrowanych zdarzeń

(a) Zlecenia certyfikacji;
(b) Zlecenia unieważnienia;
(c) Wydanie certyfikatu;
(d) Wydanie listy unieważnionych certyfikatów;
(e) Zdarzenia w systemie: zalogowanie, wylogowanie, restart;
(f) Komunikacja mailowa z subskrybentami i urzędami rejestracji.

4.5.2 Częstotliwość przetwarzania zapisów

Bez klauzuli.

4.5.3 Okres przechowywania zapisów dla audytu

Rejestrowane zdarzenia są przechowywane przynajmniej przez 3 lata.

4.5.4 Ochrona zapisów dla audytu

Tylko uprawnieni pracownicy urzędu certyfikacji mogą przeglądać i przetwarzać rejestr zdarzeń.

4.5.5 Procedury tworzenia kopii zapisów dla audytu

Rejestr zdarzeń jest kopiowany nie rzadziej niż raz w miesiącu na zewnętrzny nośnik

i przechowywany w bezpiecznym, zamykanym pomieszczeniu o ograniczonym dostępie.

4.6 Archiwizacja danych

4.6.1 Rodzaje archiwizowanych danych

Archiwizowane są następujące dane:

(a) Komunikacja z urzędami rejestracji (w tym mailowa);
(b) Komunikacja z subskrybentami (w tym mailowa);
(c) Wydane certyfikaty;
(d) Wydane listy unieważnionych certyfikatów;
(g) Zdarzenia w systemie: zalogowanie, wylogowanie, restart.

4.6.2 Okres przechowywania archiwum

Minimalny okres archiwizacji wynosi 3 lata.

4.6.3 Ochrona archiwum

Dane archiwalne są kopiowane raz dziennie na zewnętrzny nośnik i przechowywane w bezpiecznym, zamykanym pomieszczeniu o ograniczonym dostępie.

4.7 Zmiana kluczy

Jeżeli zajdzie potrzeba zmiany klucza urzędu certyfikacji, zostanie wygenerowana nowa para kluczy przynajmniej na rok (366 dni) przed wycofaniem z użytku tego klucza. Wszystkie nowe certyfikaty będą wydawane przy użyciu nowego klucza.

4.8 Odtworzenie po kompromitacji i katastrofie

Jeżeli stwierdzono lub podejrzewa się, że naruszono wiarygodność klucza prywatnego urzędu certyfikacji, to urząd ma obowiązek:

(a) Poinformować o tym swoich subskrybentów oraz strony korzystające z certyfikatów wydawanych przy użyciu tego klucza;
(b) Zaprzestać korzystania z niewiarygodnego klucza prywatnego podczas świadczenia usługi certyfikacji oraz wystawiania list unieważnionych certyfikatów;
(c) Wygenerować nową parę kluczy.

W przypadku zaginięcia nośnika z kopią zapasową danych zawierającą klucz prywatny urzędu certyfikacji, zostanie on uznany za skompromitowany.

W przypadku awarii sprzętu (lub jego części), na którym działa oprogramowanie urzędu certyfikacji, zostanie on wymieniony w ciągu 3 dni roboczych. Dane zostaną odzyskane z ostatniej kopii zapasowej. Jeśli uszkodzeniu ulegnie nośnik danych zostanie on zniszczony w sposób uniemożliwiający odzyskanie z niego danych. Przywrócenie listy CRL po awarii nastąpi nie później niż w ciągu 1 dnia roboczego.

4.9 Zakończenie działalności urzędu certyfikacji

Jeśli urząd certyfikacji decyduje się zakończyć świadczenie usług certyfikacji, to powinien:

(a) Poinformować o tym wszystkie zainteresowane strony;
(b) Unieważnić wszystkie wystawione certyfikaty oraz certyfikaty urzędu kończącego działalność;
(c) Zakończyć dystrybucję certyfikatów;
(d) Publikować listę unieważnionych certyfikatów do końca czasu życia certyfikatów użytkowników końcowych.

5 Kontrola zabezpieczeń fizycznych, proceduralnych oraz personelu

5.1 Kontrola zabezpieczeń fizycznych

5.1.1 Lokalizacja i konstrukcja siedziby

PL-Grid Simple CA znajduje się we Wrocławskim Centrum Sieciowo-Superkomputerowym, Wrocław, Polska.

5.1.2 Dostęp fizyczny

Urząd certyfikacji używa dedykowanej stacji roboczej, która znajduje się w pomieszczeniu o ograniczonym dostępie, dedykowanym dla PKI. Dostęp do pomieszczenia jest monitorowany i możliwy tylko przy użyciu kodu i klucza. Kod i klucze posiadają ustaleni pracownicy Centrum, pełniący funkcję operatora PKI. Wszelkie prace serwisowe i dostęp do stacji osób trzecich odbywa się wyłącznie w obecności pracowników Centrum. Gromadzone są zapisy użycia kodu (odblokowanie, zablokowanie).

5.1.3 Zasilanie i klimatyzacja

Stacja robocza PL-Grid Simple CA działa w klimatyzowanym pomieszczeniu i jest podłączona do systemu UPS z redundantnym zasilaniem.

5.1.4 Ochrona przeciwpożarowa

Stacja robocza PL-Grid Simple CA znajduje się w dedykowanym pomieszczeniu chronionym systemem przeciwpożarowym.

5.1.5 Kopia bezpieczeństwa poza siedzibą

Kopia klucza prywatnego, hasło oraz podpisany certyfikat Centrum Certyfikacji zdeponowane są w Kancelarii Tajnej organizacji prowadzącej PL-Grid Simple CA. Kopie składowane są w formie elektronicznej na nośniku niekasowalnym oraz w formie wydruku na papierze.

5.2 Kontrola zabezpieczeń proceduralnych

5.2.1 Zaufane role

Operatorami urzędu certyfikacji są osoby posiadające uprawnienia do wystawiania certyfikatów oraz list unieważnionych certyfikatów. Osoby występujące jako urząd rejestracji muszą zostać zatwierdzone jako jednostki realizujące proces uwierzytelnienia subskrybenta i mające możliwość inicjowania automatycznego wystawienia certyfikatu.

5.3 Kontrola personelu

5.3.1 Wymagania dotyczące pochodzenia, kwalifikacji, doświadczenia i odprawy

Urząd certyfikacji ponosi odpowiedzialność za właściwe przygotowanie i kompetencje swoich operatorów. Pracownicy urzędu certyfikacji i urzędów rejestracji są rekrutowani spośród personelu Wrocławskiego Centrum Sieciowo-Superkomputerowego lub innego centrum wchodzącego w skład Konsorcjum PL-Grid.

5.3.2 Sankcje z tytułu nieuprawnionych działań

Operatorzy urzędu certyfikacji i urzędów rejestracji, którzy nadużyli swoich uprawnień bezzwłocznie tracą swoją funkcję.

6 Kontrola bezpieczeństwa technicznego

6.1 Generacja i instalacja pary kluczy

6.1.1 Generacja pary kluczy

Dopuszcza się sytuacje:

(a) Użytkownik końcowy zleca certyfikację swojego klucza publicznego (generuje parę kluczy, przygotowuje zlecenie certyfikacji i podpisuje je). Zlecenie certyfikacji musi być złożone w formacie PKCS#10. Urząd certyfikacji weryfikuje podpis pod zleceniem;

(b) Użytkownik końcowy zgłasza się do urzędu rejestracji w celu wystawienia pary kluczy oraz uzyskania certyfikatu klucza publicznego. Urząd rejestracji składa w imieniu użytkownika zlecenie certyfikacji w formacie PKCS#10. Urząd certyfikacji weryfikuje podpis pod zleceniem;

(c) Prowadzący szkolenie zgłasza się do urzędu rejestracji w celu wystawienia par kluczy dla uczestników szkolenia oraz uzyskania certyfikatów kluczy publicznych. Wniosek musi być podpisany cyfrowo ważnym certyfikatem prowadzącego.

6.1.2 Dostarczanie klucza prywatnego subskrybentowi

Jeśli subskrybent zleca urzędowi wygenerowanie pary kluczy, a następnie certyfikację klucza publicznego, to wygenerowana para kluczy zostaje zaszyfrowana hasłem podanym przez subskrybenta i w takiej postaci mu przekazana. Dane te mogą zostać przekazane w siedzibie urzędu certyfikacji lub rejestracji lub za pomocą bezpiecznej komunikacji sieciowej.

Pary kluczy generowane na potrzeby szkoleń są przekazywane prowadzącemu szkolenie, za pomocą bezpiecznej komunikacji sieciowej, zaszyfrowane przy użyciu certyfikatu prowadzącego lub szyfrowane hasłem i umieszczane w repozytorium Infrastruktury PL-Grid. Prowadzący przekazuje klucze użytkownikom końcowym zgodnie z procedurą opisaną w p. 4.3.

6.1.3 Dostarczanie klucza publicznego subskrybentowi

Jeśli subskrybent zleca urzędowi wygenerowanie pary kluczy, a następnie certyfikację klucza publicznego, to wygenerowana para kluczy zostaje mu przekazana zgodnie z p. 6.1.2. Gdy subskrybent sam generuje parę kluczy i przekazuje urzędowi tylko klucz publiczny, dane te mogą zostać przekazane w siedzibie urzędu certyfikacji lub rejestracji lub za pomocą komunikacji sieciowej.

Pary kluczy generowane na potrzeby szkoleń są dostarczane subskrybentowi zgodnie z p. 6.1.2.

6.1.4 Dostarczanie użytkownikom klucza publicznego urzędu certyfikacji

Klucz publiczny PL-Grid Simple CA zabezpieczony w podpisanym przez siebie certyfikacie jest dostępny do pobrania ze strony WWW urzędu certyfikacji.

6.1.5 Długości klucza

Klucz prywatny użytkownika końcowego musi mieć długość co najmniej 2048 bitów. Klucz prywatny użytkownika końcowego ubiegającego się o certyfikat ważny dłużej niż 366 dni musi mieć długość 4096 bitów. Klucz prywatny urzędu certyfikacji musi mieć długość co najmniej 4096 bitów. Urząd certyfikacji odmawia certyfikacji klucza o mniejszym rozmiarze niż obowiązujący.

6.1.6 Generowanie parametrów klucza publicznego

Bez klauzuli.

6.1.7 Sprawdzanie jakości parametrów

Bez klauzuli.

6.1.8 Sprzętowe lub programowe generowanie kluczy

Klucze są generowane przez oprogramowanie.

6.1.9 Cele zastosowania kluczy

Klucze mogą być używane w celu uwierzytelniania, szyfrowania danych, szyfrowania klucza, składania podpisów cyfrowych.

6.2 Ochrona klucza prywatnego

Klucze prywatne PL-Grid Simple CA są szyfrowane hasłem. Hasło chroniące klucz ma właściwą jakość i składa się przynajmniej z 15 znaków. Hasło znane jest tylko personelowi CA. Kopia hasła przechowywana jest na stacji CA oraz w kopercie w szafie w pomieszczeniu o ograniczonym dostępie (jak określono w p. 5.1.2). Stacja robocza CA jest chroniona hasłem znanym tylko personelowi CA.

6.2.1 Kontrola klucza prywatnego przez wiele osób

Bez klauzuli.

6.2.2 Depozyt klucza prywatnego

Kopia klucza prywatnego, hasło oraz podpisany certyfikat Centrum Certyfikacji zdeponowane są w Kancelarii Tajnej organizacji prowadzącej PL-Grid Simple CA. Kopie składowane są w formie elektronicznej na nośniku niekasowalnym oraz w formie wydruku na papierze.

6.2.3 Kopie zapasowe klucza prywatnego

Kopia zapasowa klucza prywatnego PL-Grid Simple CA jest przechowywana na stacji roboczej urzędu certyfikacji oraz dodatkowo na pamięci USB zdeponowanej w szafie w pomieszczeniu z ograniczonym dostępem (jak określono w p. 5.1.2).

6.2.4 Archiwizacja klucza prywatnego

Bez klauzuli.

6.2.5 Metoda aktywacji klucza prywatnego

Aktywacja klucza prywatnego wymaga podania przez właściciela odpowiedniego hasła. Klucz prywatny urzędu certyfikacji może zostać aktywowany automatycznie po otrzymaniu zlecenia od RA, z pobraniem hasła przechowywanego lokalnie na stacji CA. Klucze prywatne serwerów i usług mogą nie być chronione hasłem, muszą jednak być wówczas objęte odpowiednią ochroną na poziomie systemu operacyjnego.

6.3 Inne aspekty zarządzania kluczami

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

6.4 Dane aktywacyjne

6.4.1 Generacja i instalacja danych aktywacyjnych

Hasła używane do ochrony danych przesyłanych w procesie certyfikacji oraz chroniące wygenerowane klucze powinny być dobierane według ogólnie znanych zaleceń dotyczących haseł. Klucze prywatne użytkowników końcowych powinny być chronione hasłem nie krótszym niż 10 znaków.

6.4.2 Ochrona danych aktywacyjnych

Hasła muszą być tak przechowywane, by nie trafiły do osób nieupoważnionych.

6.5 Kontrola bezpieczeństwa komputerowego

Urząd certyfikacji używa dedykowanej stacji roboczej do realizacji działań CA oraz dwóch stacji realizujących funkcjonalność repozytorium:

(a) Funkcjonalność systemu operacyjnego i oprogramowania jest ograniczona do niezbędnego minimum, potrzebnego do działania oprogramowania realizującego funkcje PL-Grid Simple CA lub repozytorium danych PL-Grid Simple CA;

(b) Bezpieczeństwo systemu operacyjnego zapewniane jest przez stosowanie stabilnych rozwiązań i zabezpieczeń na poziomie jądra systemu, oraz systematyczne instalowanie poprawek bezpieczeństwa.

(c) Stacja robocza jest monitorowana, rejestrowana jest aktywność w systemie i próby nieautoryzowanego dostępu.

6.6 Cykl kontroli technicznej

Bez klauzuli.

6.7 Kontrola bezpieczeństwa sieci

Stacje komputerowe, na których są realizowane zadania urzędu certyfikacji i udostępniane repozytorium mogą nawiązywać połączenia sieciowe. Stosowana jest wielostopniowa ochrona dostępu:

(a) Stacje chronione są przez zapory sieciowe;

(b) Zezwala się na połączenia między stacją CA i stacją repozytorium w lokalnej sieci, inicjowane przez stację CA, w celu umieszczenia w repozytorium listy CRL. Połączenia możliwe są tylko przy użyciu zaufanych certyfikatów X509 i protokołu SSL v3/ TLS v1, bądź zaufanych kluczy i protokołu SSH. Uwierzytelnianie jest obustronne i obowiązkowe, a komunikacja szyfrowana;

(c) Zezwala się na połączenia między stacją CA a stacją RA inicjowane przez stację RA, z komunikacją dwustronną w obrębie danego połączenia, nawiązywane w celu obsługi procesu certyfikacji (zlecenie wydania certyfikatu, jego unieważnienia, przedłużenia ważności). Połączenia z CA możliwe są tylko przy użyciu zaufanych certyfikatów X509 i protokołu SSL v3/ TLS v1. Uwierzytelnianie jest obustronne i obowiązkowe, a komunikacja szyfrowana;

(d) Zezwala się na połączenia inicjowane przez CA do serwera pocztowego w sieci lokalnej, w celu obsługi procesu certyfikacji, w tym wysyłania powiadomień o czasie życia certyfikatu.

(e) Zezwala się na połączenia ze świata do stacji z repozytorium w celu pobrania danych publicznych udostępnianych na stronie WWW.

7 Profile certyfikatów i list unieważnionych certyfikatów

7.1 Profil certyfikatów

Wszystkie certyfikaty wystawiane przez PL-Grid Simple CA muszą być zgodne ze standardem X.509 v3.

7.1.1 Certyfikat PL-Grid Simple CA

Forma nazwy: C=PL, O=PL-Grid, CN=Simple CA

Rozszerzenia certyfikatu urzędu certyfikacji:

- Signature Algorithm: sha1WithRSAEncryption
- X509v3 Subject Key Identifier
- X509v3 Basic Constraints: CA:TRUE
- X509v3 Authority Key Identifier
- X509v3 CRL Distribution Points:
  URI:http://plgrid-sca.wcss.wroc.pl/crl.der
- X509v3 Key Usage: critical
  Certificate Sign, CRL Sign

7.1.2 Profil wystawianych certyfikatów

Rozszerzenia certyfikatu osobistego lub szkoleniowego:

- Signature Algorithm: sha1WithRSAEncryption
- X509v3 Subject Key Identifier
- X509v3 Basic Constraints: CA:FALSE
- X509v3 Authority Key Identifier
- X509v3 CRL Distribution Points:
  URI:http://plgrid-sca.wcss.wroc.pl/crl.der
- X509v3 Certificate Policies:
  Policy: <OID>
- X509v3 Key Usage: critical
  Digital Signature, Key Encipherment, Data Encipherment
- X509v3 Extended Key Usage:
  TLS Web Client Authentication, E-mail Protection (na wniosek)
- X509v3 Subject Alternative Name (na wniosek, jeden lub więcej adresów email

certyfikowanej osoby)

Rozszerzenia certyfikatu serwera lub usługi:

- Signature Algorithm: sha2WithRSAEncryption
- X509v3 Subject Key Identifier
- X509v3 Basic Constraints: CA:FALSE
- X509v3 Authority Key Identifier
- X509v3 CRL Distribution Points:
  URI:http://plgrid-sca.wcss.wroc.pl/crl.der
- X509v3 Certificate Policies:
  Policy: <OID>
- X509v3 Key Usage: critical
  Digital Signature, Key Encipherment, Data Encipherment
- X509v3 Extended Key Usage:
  TLS Web Server Authentication, TLS Web Client Authentication
- X509v3 Subject Alternative Name:

  DNS: <name1>, DNS: <name2>

7.1.3 Formy nazw

Formy nazw wystawianych certyfikatów:

(a) Certyfikatów osobistych: C=PL, O=PL-Grid, O=Uzytkownik, O=organizacja, CN=nazwa podmiotu, CN=identyfikator podmiotu

(b) Certyfikatów szkoleniowych: C=PL, O=PL-Grid, O=Szkolenie, CN=nazwa podmiotu, CN=identyfikator szkolenia, CN=identyfikator podmiotu

(c) Certyfikatów serwerów i usług: C=PL, O=PL-Grid, O=Usluga, O=organizacja, CN=nazwa podmiotu

7.1.4 Ograniczenia nazw

Ograniczenia nazw certyfikatów osobistych:

(a) Nazwa kraju C musi być „PL”;

(b) Nazwa organizacji O musi być „PL-Grid”;

(c) Nazwa organizacji O (2) musi być „Uzytkownik”;

(d) Nazwa organizacji O (3) musi określać instytucję, działającą w ramach polskich środowisk gridowych;

(e) Nazwa podmiotu CN zawiera imię i nazwisko certyfikowanej osoby;

(f) Nazwa podmiotu CN (2) zawiera identyfikator certyfikowanej osoby przyznawany w Infrastrukturze PL-Grid.

Ograniczenia nazw certyfikatów szkoleniowych:

(a) Nazwa kraju C musi być „PL”;

(b) Nazwa organizacji O musi być „PL-Grid”;

(c) Nazwa organizacji O (2) musi być „Szkolenie”;

(d) Nazwa podmiotu CN zawiera imię i nazwisko lub pseudonim certyfikowanej osoby;

(e) Nazwa podmiotu CN (2) zawiera identyfikator szkolenia, który musi zawierać miejsce i datę prowadzenia szkolenia;

(f) Nazwa podmiotu CN (3) zawiera identyfikator uczestnika szkolenia.

Ograniczenia nazw certyfikatów serwerów i usług:

(a) Nazwa kraju C musi być „PL”;

(b) Nazwa organizacji O musi być „PL-Grid”;

(c) Nazwa organizacji O (2) musi być „Usluga”;

(d) Nazwa organizacji O (3) musi określać instytucję działającą w ramach polskich środowisk gridowych;

(e) Nazwa podmiotu CN zawiera pełną nazwę domenową serwera (DNS FQDN), zaś dla usług przyjmuje postać „<nazwa usługi>/<nazwa domenowa serwera>”.

7.2 Profil listy unieważnionych certyfikatów

Centrum Certyfikacji PL-Grid CA wystawia listy unieważnionych certyfikatów w formacie X.509 v2, podpisane algorytmem SHA-1.

8 Administrowanie specyfikacją

8.1 Procedura zmiany specyfikacji

Dopuszcza się realizację zmian typu edytorskiego w niniejszej polityce. Nowa wersja polityki ze znaczącymi zmianami aspektów technicznych lub proceduralnych będzie dostępna z wyprzedzeniem na stronie WWW. Polityka po znaczących zmianach otrzymuje nowy OID. Znaczące zmiany są przygotowywane i akceptowane przez zespół odpowiedzialny za bezpieczeństwo Infrastruktury PL-Grid.

8.2 Polityka publikacji i powiadamiania

Niniejsza polityka jest dostępna poprzez WWW. Subskrybenci nie są powiadamiani o zmianie niniejszej polityki. Znaczące zmiany będą wysyłane do wiadomości kierownictwa Infrastruktury PL-Grid.

8.3 Procedura zatwierdzania polityki certyfikacji

Zmiany w polityce zatwierdzane są w drodze głosowania, większością głosów. Każdej organizacji należącej do Konsorcjum PL-Grid przysługuje jeden głos. W sytuacjach spornych, przy braku rozstrzygającego wyniku głosowania, głos decydujący ma kierownik instytucji odpowiedzialnej za niniejszą politykę lub osoba przez niego wskazana.