Załącznik nr 12, część C
do Regulaminu świadczenia usług certyfikacyjnych
przez Centrum Certyfikacji Województwa Podlaskiego

Polityka Certyfikacji emailCA

1 Wstęp

Polityka Certyfikacji emailCA Centrum Certyfikacji Województwa Podlaskiego (CCWP) prowadzonego przez Urząd Marszałkowski Województwa Podlaskiego określa ogólne zasady stosowane przez CCWP w ramach świadczonych usług certyfikacji kluczy publicznych w celu budowy zaufania użytkowników, definiuje obowiązki i odpowiedzialność uczestników Infrastruktury Klucza Publicznego, typy certyfikatów i ich obszary zastosowań.

1.1 Identyfikacja Polityki

Nazwa polityki	Polityka Certyfikacji dla emailCA
Wersja	1.0
Zastrzeżenie	Certyfikat wystawiony zgodnie z dokumentem „Polityka Certyfikacji emailCA" nie jest certyfikatem kwalifikowanym w rozumieniu ustawy z dn. 18.09.2001 o podpisie elektronicznym.
Status	finalna
Identyfikator polityki (OID)	1.2.616.1.113637.1.3.1
Data wydania	2007-08-10
Data ważności	do odwołania

1.2 Historia zmian

Wersja	*Data*	*Opis zmian*
1.0	2006-10-02	pierwsza wersja

Kolejne wprowadzane zmiany w polityce certyfikacji – o ile nie podano inaczej - mają także zastosowanie do certyfikatów wystawionych na podstawie niniejszej polityki.

2 Postanowienia Polityki Certyfikacji

2.1 Zakres stosowalności

Certyfikaty wydane zgodnie z Polityką są przeznaczone do:
- zapewnia integralność informacji przesyłanych pocztą elektroniczną;
- uwierzytelniania klienta wobec serwera w protokole SSL;
- uwierzytelniania nadawcy;
- szyfrowania informacji poczty elektronicznej

Certyfikaty wydane zgodnie z Polityką są wydawane na wniosek osoby fizycznej, będącej pracownikiem UMWP lub Jednostek Samorządu Terytorialnego, używającej podanego we wniosku adresu poczty elektronicznej. Wydawane certyfikaty mają okres ważności 1 (jeden) rok.

Certyfikaty wydawane w ramach Polityki nie są certyfikatami kwalifikowanymi w rozumieniu ustawy z dnia 18 września 2001 o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450). W szczególności podpis elektroniczny weryfikowany na podstawie certyfikatu nie jest równoważny w skutkach z podpisem własnoręcznym.

2.2 Prawa i obowiązki

2.2.1 Obowiązki posiadacza certyfikatu

Przed uzyskaniem certyfikatu, wnioskodawca zobowiązany jest do zapoznania się z treścią Polityki. Złożenie wniosku o wydanie certyfikatu jest równoznaczne z akceptacją warunków świadczenia usługi.
Strona będąca posiadaczem certyfikatu zobowiązana jest do bezpiecznego przechowywania swojego klucza prywatnego.

W przypadku utraty kontroli nad kluczem prywatnym, odpowiadającym kluczowi publicznemu umieszczonemu w certyfikacie, jego ujawnienia lub też uzasadnionego podejrzenia, iż fakt taki mógł mieć miejsce, posiadacz certyfikatu zobowiązuje się niezwłocznie powiadomić o tym CCWP poprzez złożenie wniosku o unieważnienie tego certyfikatu.

Posiadacz certyfikatu jest odpowiedzialny za prawdziwość danych przekazywanych we wniosku o wydanie certyfikatu. Posiadacz certyfikatu zobowiązuje się do informowania wydawcy certyfikatu o wszelkich zmianach informacji podanych we wniosku o wydanie certyfikatu.

Po upływie daty ważności posiadacz certyfikatu ma obowiązek zaprzestać używania klucza prywatnego skojarzonego z kluczem publicznym zawartym w tym certyfikacie.

2.2.2 Obowiązki strony ufającej

Strona ufająca jest zobowiązana do pobrania z Repozytorium w sposób bezpieczny certyfikatu CCWP, który obdarzyła zaufaniem oraz zweryfikowania skrótu klucza publicznego CCWP.

W trakcie określania swojego zaufania wobec usługi bazującej na certyfikacie wydanym w ramach Polityki, obowiązkiem strony ufającej jest przeprowadzenie stosownej weryfikacji ważności certyfikatu. W procesie weryfikacji strona ufająca musi zweryfikować ścieżkę certyfikacji przy użyciu informacji publikowanych przez CCWP w Repozytorium.

2.2.3 Obowiązki CCWP

CCWP odpowiada za weryfikację i zgodność informacji zawartych w wydanych certyfikatach z danymi zamieszczonymi we wniosku oraz odpowiada za publikowanie informacji o unieważnionych certyfikatach zgodnie z procedurami opisanymi w niniejszym dokumencie. CCWP nie odpowiada za prawdziwość tych danych.

2.3 Publikacja i repozytorium

Informacja o unieważnionych certyfikatach jest publikowana w Repozytorium w chwili tworzenia nowej listy certyfikatów unieważnionych. Nowa lista certyfikatów unieważnionych dla certyfikatów wydawanych zgodnie z Polityką jest tworzona w terminie do 1 godziny po każdym unieważnieniu certyfikatu, jednak nie rzadziej, niż co 7 dni.

2.4 Ochrona informacji

Dane przechowywane i przetwarzane w ramach realizacji Polityki podlegają ochronie zgodnie z ustawą o ochronie danych osobowych oraz powszechnie obowiązującymi przepisami prawa. Centrum gwarantuje, że stronie ufającej udostępniane są wyłącznie informacje zawarte w certyfikacie.

2.5 Interpretacja i obowiązujące akty prawne

Funkcjonowanie Centrum Certyfikacji Województwa Podlaskiego oparte jest na zasadach ujętych Regulaminie.

3 Identyfikacja i uwierzytelnienie

3.1 Rejestracja

Procedurę rejestracji określa Regulamin.

Wydanie certyfikatu musi być poprzedzone złożeniem odpowiedniego wniosku w Centrum Certyfikacji i pozytywnie zakończoną procedurą rejestracji wniosku. Do centrum certyfikacji muszą zostać dostarczone następujące dane:

- imię i nazwisko,
- nazwę jednostki i jednostki organizacyjnej do której należy wnioskodawca,
- adres (zgodny ze standardem SMTP) konta poczty elektronicznej,
- klucz publiczny wnioskodawcy zawarty w elektronicznym wniosku w formacie PKCS#10.

W trakcie rejestracji weryfikowane są następujące dane:
- dostęp wnioskodawcy do konta e-mail podanego wniosku,
- prawdziwość danych personalnych i danych jednostki wnioskodawcy.

Wniosek o wydanie certyfikatu należy składać w Punkcie Rejestracji.

Termin wydania certyfikatu określa Regulamin. Po wygenerowaniu certyfikatu, Centrum wysyła na podany adres e-mail informację zawierającą odnośnik do strony WWW, z której wnioskodawca będzie mógł pobrać certyfikat.

3.2 Akceptacja certyfikatu

Właściciel certyfikatu zobowiązany jest do zweryfikowania poprawności danych zawartych w certyfikacie pod względem zgodności z danymi zawartymi we wniosku. W przypadku stwierdzenia niezgodności zobowiązany jest do niezwłocznego zawiadomienia CCWP o tym fakcie i złożenia wniosku o unieważnienie certyfikatu. CCWP zobowiązany jest do wydania nowego poprawionego certyfikatu. Brak zgłoszenia niezgodności danych w ciągu 24 godzin jest równoważny z potwierdzeniem przez subskrybenta zgodności danych.

Akceptacja przez subskrybenta certyfikatu zawierającego niezgodne dane w porównaniu do zawartych w wniosku przez jego posiadacza obciąża go skutkami prawnymi używania tego certyfikatu.

3.3 Unieważnienie certyfikatu

Do unieważnienia certyfikatu wystawionego zgodnie z niniejszą Polityką Certyfikacji wymagane jest przesłanie odpowiedniego wniosku o unieważnienie i weryfikacji uprawnień osoby przesyłającej wniosek do złożenia takiego wniosku.

Warunkiem rozpoczęcia procedury unieważnienia certyfikaty jest poprawna weryfikacja wnioskodawcy.
Unieważnienie certyfikatu jest procedurą NIEODWRACALNĄ.

Warunkiem rozpoczęcia procedury unieważnienia certyfikatu jest podanie przez wnioskodawcę informacji pozwalającej zidentyfikować unieważniany certyfikat i powodu jego unieważnienia.

Procedurę unieważnienia certyfikatu określa regulamin.

Certyfikat jest również unieważniany w następujących przypadkach:
1. otrzymania pisemnego wniosku o unieważnieni certyfikatu od uprawnionej osoby trzeciej,
2. zdezaktualizowaniu informacji zawartych w certyfikacie,
3. niedozwolonego lub błędnego wydania certyfikatu na skutek:
   - fałszerstwa danych zawartych w certyfikacie,
   - niespełnienia istotnych warunków wstępnych do wydania certyfikatu,
   - popełnienia błędów przy wprowadzaniu danych lub innych błędów przetwarzania.

3.4 Odnowienie certyfikatu

Certyfikat może być odnawiany, także gdy upłynął jego termin ważności. Po upływie terminu ważności właściciel musi ubiegać się o nowy certyfikat zgodnie z procedurą wydawania certyfikatu lub o odnowienie certyfikatu.

Odnawianie certyfikatu jest równoznaczne z wydaniem nowego certyfikatu zawierającego jednakowe (z wyjątkiem okresu ważności i klucza publicznego) dane. Centrum Certyfikacji nie wydaje nowego certyfikatu dla klucza publicznego zawartego w certyfikacie.

Odnowienie certyfikatu jest możliwe przed upływem terminu ważności odnawianego certyfikatu.

Podczas odnowienia certyfikatu jest sprawdzany dostęp posiadacza odnawianego certyfikatu do klucza prywatnego. Tożsamość posiadacza certyfikatu nie jest weryfikowana.

Odnowienie certyfikatu odbywa się przez zlecenie odnowienia certyfikatu zawierającego:

- informację pozwalające zidentyfikować certyfikat,
- klucz publiczny wnioskodawcy zawarty w elektronicznym wniosku w formacie PKCS#10

W trakcie procedury odnawiana certyfikatu weryfikowany jest dostęp wnioskodawcy do konta poczty elektronicznej zapisanego w certyfikacie.

4 Techniczne środki zapewnienia bezpieczeństwa

4.1 Generowanie pary kluczy

Polityka wymaga, aby para kluczy subskrybenta była wygenerowana zgodnie z algorytmem RSA. Długość klucza (rozumiana jako moduł p*q) to co najmniej 1024 bitów. Para kluczy jest generowana przez przez pracownika Punktu Rejestracji.

4.2 Ochrona klucza prywatnego subskrybenta

Za ochronę klucza prywatnego skojarzonego z kluczem publicznym umieszczonym w certyfikacie odpowiedzialny jest wyłącznie posiadacz certyfikatu.

4.3 Aktywacja kluczy

Polityka nie przewiduje wymogów w odniesieniu do sposobu aktywacji klucza subskrybenta certyfikatu.

4.4 Niszczenie kluczy

Po wygaśnięciu ważności certyfikatu skojarzony z nim klucz prywatny może być wykorzystywany do odszyfrowywania danych. W tym przypadku klucz prywatny powinien być chroniony. Właściciel może zniszczyć klucz prywatny skojarzony z kluczem publicznym z wygasłego certyfikatu w wybrany przez siebie sposób.

5 Możliwość dostosowania Polityki do wymagań subskrybenta

Subskrybent nie ma możliwości zmiany Polityki.