Polityka Certyfikacji rootCA

1 Wstęp

Polityka Certyfikacji rootCA 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 Informacje dla subskrybenta

Przed użyciem certyfikatów wydanym zgodnie z niniejszą Polityką Certyfikacji, należy upewnić się, że wszystkie klauzule w niej zawarte zostały przeczytane i zrozumiane.

1.2 Identyfikacja Polityk

Nazwa polityki	Polityka Certyfikacji dla rootCA
Zastrzeżenie	Certyfikat wystawiony zgodnie z dokumentem „Polityka Certyfikacji rootCA" nie jest certyfikatem kwalifikowanym w rozumieniu ustawy z dn. 18.09.2001 o podpisie elektronicznym.
Wersja	1
Status	Finalna
Identyfikator polityki (OID)	1.2.616.1.113637.1.1.1
Data wydania	2007-08-10
Data ważności	do odwołania

1.3 Historia zmian

Wersja	*Data*	*Opis zmian*
	2007-08-10	pierwsza wersja

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

1.4 Odbiorcy usług certyfikacyjnych oraz zastosowanie certyfikatów

Certyfikaty wystawione zgodnie z niniejszą polityką mają zastosowanie jedynie w odniesieniu do certyfikatów wystawionych dla EsigCA, EmailCA, NetCA Centrum Certyfikacji Województwa Podlaskiego.

2 Wprowadzenie

Niniejsza Polityka Certyfikacji znajduje zastosowanie w procesie certyfikacji kluczy publicznych wykorzystywanych do następujących zadań:

- wystawienie certyfikatu Centrum Certyfikacji rootCA
- wystawianie certyfikatów pośrednich Centrum Certyfikacji: esigCA, emailCA, netCA
- unieważnienie certyfikatów pośrednich Centrum Certyfikacji: esigCA, emailCA, netCA
- wydawanie listy certyfikatów unieważnionych (zwanych CRL) zawierającej unieważnione certyfikaty Centrum Certyfikacji.

CCWP − rootCA nie wydaje certyfikatów klucza publicznego dla subskrybentów, ale wyłącznie dla Centrum Certyfikacji: esigCA, emailCA, netCA. Kontakt z Centrum Certyfikacji rootCA jest możliwy jedynie za pomocą wydzielonej sieci dostępnej jedynie dla pracowników CCWP. System Centrum Certyfikacji rootCA nie jest podłączony do żadnej sieci logicznej ani fizycznej wychodzącej poza obręb pomieszczeń CCWP.

3 Postanowienia Polityki Certyfikacji

3.1 Zakres stosowalności

Certyfikaty wydawane zgodnie z niniejszą Polityką Certyfikacji są wydawane przez CCWP wyłącznie dla rootCA, esigCA, emailCA, netCA.

3.2 Prawa i obowiązki

3.2.1 Obowiązki Centrum Certyfikacji rootCA

Centrum Certyfikacji rootCA zobowiązane jest do bezpiecznego przechowywania swojego klucza prywatnego, w sposób zapobiegający jego ujawnieniu. Wszelkie operacje, w tym generowanie i używanie klucza publicznego, powinny być wykonywane w sprzętowym module kryptograficznym (HSM) posiadającym certyfikowany poziom ochrony FIPS140-2 L3 lub wyższy. Klucz prywatny Centrum Certyfikacji rootCA może opuścić bezpieczne środowisko modułu sprzętowego HSM wyłącznie w postaci zaszyfrowanej w obecności przynajmniej dwóch upoważnionych przez dyrektora Departamentu Informatyki osób.

3.2.2 Obowiązki subskrybenta

Subskrybent, który otrzymał esigCA, emailCA lub netCA zobowiązany jest do pobrania w sposób bezpieczny certyfikatu rootCA oraz zweryfikowania skrótu klucza publicznego na podstawie informacji publikowanych przez Centrum Certyfikacji Województwa Podlaskiego. Obowiązkiem subskrybenta jest przeprowadzenie weryfikacji ważności certyfikatów pośrednich Centrum Certyfikacji przez pobranie i zastosowanie listy certyfikatów unieważnionych (zwanych CRL) publikowanej przez Centrum Certyfikacji Województwa Podlaskiego.

3.3 Odpowiedzialność

CCWP odpowiada za weryfikację informacji zawartych w certyfikatach poświadczonych przez rootCA. CCWP odpowiada za publikowanie informacji o unieważnionych certyfikatach zgodnie z procedurami opisanymi w niniejszym dokumencie.

3.4 Publikacja i repozytorium

CCWP w ramach świadczonych usług certyfikacyjnych publikuje wszystkie poświadczone przez Centrum Certyfikacji rootCA certyfikaty w publicznie dostępnym Repozytorium, na stronie: http://www.ccwp.wrotapodlasia.pl/repozytorium.php. Szczegóły organizacji Repozytorium i opis metod dostępu do tych informacji znajdują się na stronach publicznych CCWP. Certyfikaty pośrednie CCWP publikowane są w repozytorium natychmiast po ich wydaniu. Informacja o unieważnieniu certyfikatu pośredniego publikowana jest natychmiast po zaistnieniu tego faktu przez wygenerowanie nowej listy certyfikatów unieważnionych (zwanych CRL).

4 Identyfikacja i uwierzytelnienie

4.1 Odnowienie certyfikatu

CCWP nie przewiduję procedury odnowienia certyfikatu rootCA.

4.2 Unieważnienie

Nie jest przewidziane unieważnienie certyfikatu rootCA.

4.3 Wydanie certyfikatu

Wydany certyfikat rootCA dostarczony jest w trybie off—line dla esigCA, netCA, emailCA na nośniku magnetycznym, optycznym lub elektronicznym.

5 Techniczne procedury kontroli bezpieczeństwa

5.1 Generowanie pary kluczy

Para kluczy dla esigCA, emailCA lub netCA powinna być wygenerowana w bezpiecznym środowisku sprzętowego modułu kryptograficznego (HSM) posiadającego certyfikowany poziom ochrony FIPS140-2 L3 lub wyższym. Klucz prywatny subskrybenta może opuścić środowisko sprzętowego modułu kryptograficznego jedynie w postaci zaszyfrowanej. Za ochronę klucza prywatnego pośredniego Centrum Certyfikacji odpowiedzialny jest pracownik CCWP.

5.2 Ochrona klucza prywatnego rootCA

Klucz prywatny rootCA jest generowany i używany wyłącznie w bezpiecznym środowisku sprzętowego modułu kryptograficznego posiadającego certyfikat poziomu ochrony FIPS140-2 L3 lub wyższy. Klucz prywatny opuszcza bezpieczne środowisko modułów sprzętowych wyłącznie w postaci zaszyfrowanej. Dodatkowo system rootCA chroniony jest fizycznie przed dostępem osób niepowołanych i elektromagnetycznie przed podsłuchem i nieautoryzowanym dostępem do urządzeń serwerowych wchodzących w skład CCWP.