ZATWIERDZAM

.....

DYREKTOR

CENTRUM PERSONALIZACJI DOKUMENTÓW MSWiA

POLITYKA CERTYFIKACJI CPD MSWIA

Warszawa, dn. 28 czerwca 2006 r.

SPIS TREŚCI

1. Wstęp

Niniejszy dokument określa cel i sposób zarządzania certyfikatami wydawanymi przez Centrum Personalizacji Dokumentów Ministerstwa Spraw Wewnętrznych i Administracji w Warszawie. Polityka certyfikacji obejmuje zagadnienia związane z wystawianiem, odnawianiem, wstrzymywaniem oraz unieważnianiem certyfikatów. Reguluje także sprawy związane z ich bezpieczeństwem.

Celem certyfikacji wykorzystywanej w CPD MSWiA jest zagwarantowanie dużego bezpieczeństwa dostępu do systemów informatycznych wykorzystywanych w procesie produkcji dowodów osobistych i paszportów.

1.1. Słownik

Poprzez poniższe pojęcia rozumie się:

1) ***CA*** – Centrum Autoryzacji,
2) ***CPD*** – Centrum Personalizacji Dokumentów MSWiA,
3) ***Certyfikat*** – elektroniczne zaświadczenie – plik podpisany cyfrowo przez Centrum Autoryzacji, które zawiera dane o użytkowniku certyfikatu, jego klucz publiczny oraz informacje kto wystawił ten certyfikat. Zaświadczenie, za pomocą którego dane są przyporządkowane do określonej osoby fizycznej, urządzenia (np. serwera) czy podmiotu (np. Urzędu Certyfikacji lub Urzędu Rejestracji) bądź służą do innych celów (np. szyfrowania danych, potwierdzenie autentyczności podpisu elektronicznego, potwierdzenie autentyczności klucza publicznego adresata wiadomości),
4) ***PKI*** – Infrastruktura Klucza Publicznego. Jest to szeroko pojęty kryptosystem, w skład którego wchodzą urzędy certyfikacyjne (CA), urzędy rejestracyjne (RA), subskrybenci certyfikatów (użytkownicy), oprogramowanie i sprzęt,
5) ***Klucz publiczny*** – klucz wielodostępu, klucz jawny. Jeden z pary kluczy szyfrujących obok klucza prywatnego przeznaczony do stosowania przez dowolny podmiot w celu szyfrowanego komunikowania się z posiadaczem odpowiedniego klucza prywatnego,
6) ***Klucz prywatny*** – klucz tajny. Jeden z pary kluczy szyfrujących obok klucza

publicznego, bierze udział w procesie tworzenia elektronicznego podpisu,

7) ***Nośnik*** – karta SMART obsługująca infrastrukturę PKI na której zapisano Certyfikat, klucz publiczny CA, oraz parę kluczy publiczny i prywatny osoby dla której został wydany certyfikat,
8) ***Jednostka lokalna*** – urząd miasta, gminy, miejski lub wojewódzki,
9) ***Osoba wnioskująca*** – osoba składająca wniosek dotyczący certyfikatu, będąca przedstawicielem władzy lokalnej, pełniąca funkcję Wójta, Burmistrza, Prezydenta Miasta, Dyrektora, Dyrektora Wydziału, Naczelnika, Naczelnika Wydziału,
10) ***Usługobiorca*** – użytkownik nośnika certyfikatów, tj. pracownik jednostki lokalnej lub administrator i pracownik CPD w Warszawie,
11) ***CRL*** – Certificate Revocation List – Lista Unieważnionych lub zawieszonych certyfikatów,
12) ***WSPD*** – Wydzielone Stanowisko Produkcji Dokumentów, system personalizacji dokumentów osobistych (dowodów osobistych, paszportów, paszportów dyplomatycznych i służbowych) wykorzystywany w CPD.

1.2. Zastosowanie certyfikatów

CA generuje i wydaje certyfikaty dla pracowników jednostek lokalnych oraz dla administratorów i pracowników CPD w Warszawie.

Certyfikaty wydaje się w celu :

1) umożliwienia autoryzacji dostępu do lokalnych stanowisk roboczych systemu wydawania dowodów i paszportów,
2) umożliwienia szyfrowania i podpisywania informacji przesyłanych pomiędzy jednostkami lokalnymi a CPD w Warszawie,
3) umożliwienia autoryzacji dostępu do stanowisk systemu WSPD w CPD,
4) umożliwienia podpisywania operacji przyjęcia lub wydania blankietów podczas procesu personalizacji dokumentów w CPD.

2. Podstawowe zasady certyfikacji

2.1. Wydawanie certyfikatów

Certyfikaty wydawane są dla osoby wskazanej na odpowiednim wniosku po zweryfikowaniu jej tożsamości oraz po otrzymaniu oświadczenia o zapoznaniu się z niniejszą polityką certyfikacji oraz regulaminem certyfikacji. Certyfikaty, dane użytkownika certyfikatów oraz odpowiednie klucze są zapisane na odpowiednim nośniku, z którego nie mogą zostać usunięte.

Na nośniku zapisywane są następujące informacje:

- imię,
- nazwisko,
- PESEL,
- nr dowodu osobistego,
- zajmowane stanowisko,
- miejscowość,
- nazwa firmy,
- adres firmy,
- typ uprawnienia,
- kod terytorialny (gminy lub urzędu wojewódzkiego).

W certyfikacie zapisywane są następujące informacje:

- imię,
- nazwisko,
- PESEL.

W dalszej części dokumentu poprzez wydanie certyfikatu należy rozumieć wydanie odpowiedniego nośnika wraz z certyfikatami i odpowiednimi kluczami.

Certyfikaty służące do podpisywania danych oraz do autoryzacji zapisywane są na tej samej karcie SMART.

2.2. Obowiązki stron

Obowiązkiem użytkownika certyfikatów jest:

1) przechowywać nośnik z certyfikatami w sposób zapewniający ochronę przed nieuprawnionym wykorzystaniem w okresie ich ważności,
2) chronić nośnik przed zniszczeniem,
3) chronić wszelkie hasła i numery PIN otrzymane razem z nośnikiem,
4) w przypadku zmiany danych osobowych użytkownik winien niezwłocznie wystąpić o wydanie nowego nośnika z certyfikatami,
5) nie opuszczać lokalnego stanowiska bez uprzedniego wyciągnięcia nośnika z certyfikatami,
6) natychmiast poinformować CA o utracie lub ujawnieniu certyfikatu oraz złożyć wniosek o jego unieważnienie.

Obowiązkiem Centrum Autoryzacji jest:

1) zapewnienie poprawnego generowania certyfikatów,
2) weryfikacja poprawności danych zapisanych na nośniku,
3) zapewnienie możliwości ciągłości pracy osób zatrudnionych w jednostkach lokalnych poprzez sprawną generację i wydawanie nowych certyfikatów,
4) zapewnienie dostępu osobom zainteresowanym do polityki i regulaminu certyfikacji.
5) Ochrona danych osobowych osoby wnioskującej oraz użytkownika certyfikatów.

3. Zasady zarządzania certyfikatami

Dokumentację określoną punktem 6 polityki certyfikacji dotyczącą zarządzaniem certyfikatami składa się w CA znajdującym się w CPD w Warszawie.

Wypełniona dokumentacja winna zostać przesłana do CA przez jednostkę lokalną przy użyciu bezpiecznej poczty (poczta specjalna lub przesyłka za potwierdzeniem odbioru). W przypadku dokumentów kierowanych do CA przez osobę wnioskującą z CPD, wniosek taki winien być dostarczony bezpośrednio do CA.

3.1. Złożenie wniosku o wydanie certyfikatów

Wniosek o wydanie certyfikatów składa osoba wnioskująca w imieniu pracownika, dla którego certyfikaty są wymagane. Wniosek winien zawierać dane osobowe pracownika, które określa pkt. 2.1. polityki i regulaminu certyfikacji oraz dane osobowe osoby wnioskującej, które określa pkt. 2.1. regulaminu certyfikacji. We wniosku winno być wypełnione oświadczenie o zapoznaniu się z polityką certyfikacji i regulaminem certyfikacji przez osobę, dla której wydawany jest certyfikat. Ponadto osoba wnioskująca wypełnia zaświadczenie potwierdzające zgodność danych osobowych pracownika ubiegającego się o certyfikat. Osoba wnioskująca winna na wniosku złożyć swój podpis i pieczęć.

3.2. Wydanie certyfikatów

Certyfikaty są generowane i wydawane po uprzedniej weryfikacji wnioskodawcy pod względem tożsamości i uprawnień do składania wniosków, oraz tożsamości osoby, dla której certyfikaty mają zostać wydane.

Wydanie certyfikatów polega na wygenerowaniu certyfikatów i dostarczeniu nośnika z certyfikatami przy użyciu bezpiecznej poczty MSWiA do osoby wnioskującej.

Certyfikaty zostaną wygenerowane i wydane w ciągu 14 dni od złożenia wniosku lub w przypadkach wymagających dodatkowych czynności okres ten wynosi 30 dni. Certyfikat ważny jest przez okres pięciu lat.

3.3. Akceptacja certyfikatów

Akceptacja certyfikatów polega na sprawdzeniu poprawności działania, poprzez użycie certyfikatów zgodnie z ich przeznaczeniem. Akceptacji dokonują osoba wnioskująca oraz osoba dla której wystawiono certyfikaty (użytkownik certyfikatów).

W przypadku stwierdzenia nieprawidłowości należy natychmiast powiadomić Centrum Autoryzacji oraz złożyć wniosek o unieważnienie certyfikatów oraz wniosek o wydanie nowych certyfikatów.

Akceptacja certyfikatów powinna się odbyć w przeciągu 2 dni od otrzymania certyfikatów. Po upływie tego czasu uznaje się, że certyfikaty zostały zaakceptowane.

3.4. Zawieszenie certyfikatów

Zawieszenie certyfikatów może nastąpić tylko na wniosek osoby wnioskującej. Wniosek winien zawierać powód zawieszenia certyfikatów. Certyfikaty zostają zawieszone na okres 72 godzin i po upływie tego czasu, jeśli nie zostanie złożony wniosek o uchylenie zawieszenia, to certyfikaty automatycznie zostaną unieważnione.

3.5. Uchylenie zawieszenia certyfikatów

Uchylenie zawieszenia certyfikatów może nastąpić na wniosek osoby wnioskującej. Wniosek winien zawierać powód uchylenia zawieszenia certyfikatów. Wniosek winien zostać zatwierdzony przez osobę upoważnioną przez Dyrektora CPD.

3.6. Unieważnienie certyfikatów

Certyfikaty zostają automatycznie unieważnione po upływie terminu ważności certyfikatów lub po upływie terminu zawieszenia certyfikatów. Unieważnienie może nastąpić po zatwierdzeniu przez osobę upoważnioną przez

Dyrektora CPD wniosku o unieważnienie certyfikatów złożonego przez osobę wnioskującą. Ponadto certyfikaty mogą zostać unieważnione gdy :

1) zostanie stwierdzona niezgodność danych osobowych zawartych w certyfikacie z danymi osobowymi osoby, dla której certyfikat został wydany,
2) ulegną zmianie dane osobowe osoby, dla której certyfikaty zostały wydane,
3) osoba, dla której certyfikaty zostały wystawione przestanie być pracownikiem jednostki lokalnej lub CPD,
4) osoba będąca właścicielem certyfikatów nie dopełniła obowiązków związanych z bezpieczeństwem certyfikatów, które określa pkt 2.2. polityki certyfikacji,
5) podmiot świadczący usługi certyfikacyjne zaprzestaje świadczenia usług certyfikacyjnych, a jego praw i obowiązków nie przejmie inny podmiot,
6) osoba będąca właścicielem certyfikatów utraciła pełną zdolność do czynności prawnych.

Jeśli zaistnieją inne przesłanki do unieważnienia certyfikatów, to CA jest zobowiązane do zawieszenia certyfikatów, powiadomienia osoby, dla której certyfikaty zostały wydane oraz osoby wnioskującej, która składała wniosek o wydanie certyfikatów lub jeśli ta osoba już nie pracuje, to osoby wnioskującej, która ją zastępuje.

Unieważnienie certyfikatów nie może nastąpić z datą wsteczną.

3.7. Odnowienie certyfikatów

Odnowienie może nastąpić tylko na wniosek osoby wnioskującej. Wniosek winien zostać złożony nie później niż na 30 dni przed upływem terminu ważności odnawianych certyfikatów. Jeśli przed upływem tego terminu nie zostanie złożony wniosek o odnowienie certyfikatów, to certyfikaty zostaną automatycznie unieważnione z chwilą wygaśnięcia ich daty ważności.

4. Weryfikacja i uwierzytelnianie tożsamości

4.1. Rejestracja wniosków

Wnioski, które nie zostały dostarczone do CA pocztą specjalną lub przesyłką za poręczeniem odbioru, lub nie zostały złożone do CA przez osobę wnioskującą z CPD są odrzucane. Wniosek jest uznawany za niepoprawny jeśli nie posiada pieczęci i podpisu osoby wnioskującej. We wniosku winno być wypełnione zaświadczenie podpisane przez osobę wnioskującą o poprawności danych osoby będącej właścicielem lub ubiegającej się o certyfikaty. W przypadku wniosku o wydanie certyfikatów należy zweryfikować czy zostały prawidłowo wypełnione oświadczenia o zapoznaniu się z niniejszym dokumentem oraz z regulaminem certyfikacji, przez osoby ubiegające się o certyfikaty.

W systemie można złożyć następujące rodzaje wniosków:

1) wniosek o wydanie certyfikatów – zawiera dane personalne osoby, dla której certyfikaty mają zostać wygenerowane, zaświadczenie o poprawności danych i oświadczenie o zapoznaniu się z polityką certyfikacji i regulaminem certyfikacji,
2) wniosek o odnowienie certyfikatów – zawiera Imię, Nazwisko, PESEL osoby, dla której należy odnowić certyfikaty lub pełne informacje, jak w przypadku generowania nowych certyfikatów, gdy zmieniły się dane osobowe właściciela starych certyfikatów. Sprawdzane jest także zaświadczenie i poprawności danych,
3) wniosek o unieważnienie certyfikatów – zawiera Imię, Nazwisko, PESEL osoby, której certyfikaty trzeba unieważnić, przyczynę unieważnienia i zaświadczenie o poprawności danych,
4) wniosek o zawieszenie certyfikatów – zawiera Imię, Nazwisko, PESEL osoby, której certyfikaty trzeba zawiesić, przyczynę zawieszenia i zaświadczenie o poprawności danych,
5) wniosek o uchylenie zawieszenia certyfikatów – zawiera Imię, Nazwisko, PESEL osoby, dla której trzeba uchylić zawieszenie certyfikatów, powód uchylenia zawieszenia i zaświadczenie o poprawności danych.

4.2. Wydanie certyfikatów

Wygenerowane certyfikaty oraz dane osoby, dla której zostały wygenerowane są zapisywane na odpowiednim nośniku. Po zapisaniu na nośniku informacji należy zweryfikować w CA poprawność zapisanych danych poprzez odczytanie zapisanych informacji i sprawdzenie czy odczytane dane zgadzają się z danymi umieszczonymi na wniosku o wydanie certyfikatów.

Zgodnie z art. 14 pkt 3 ustawy o podpisie elektronicznym z dnia 18 września 2001 roku, podpis elektroniczny weryfikowany przy pomocy certyfikatu niekwalifikowanego nie powoduje skutków prawnych.

4.3. Zawieszenie certyfikatów

Wniosek o zawieszenie certyfikatów uznaje się za poprawny jeśli spełnia warunki punktu 4.1 oraz zawiera powód zawieszenia certyfikatów. Wniosek o zawieszenie certyfikatów winien zostać zatwierdzony przez osobę upoważnioną przez Dyrektora CPD.

4.4. Uchylenie zawieszenia certyfikatów

Wniosek o uchylenie zawieszenia certyfikatów uznaje się za poprawny jeśli spełnia warunki punktu 4.1 oraz zawiera powód uchylenia zawieszenia certyfikatów. Wniosek o uchylenie zawieszenia certyfikatów winien zostać zatwierdzony przez osobę upoważnioną przez Dyrektora CPD.

4.5. Unieważnienie certyfikatów

Wniosek o unieważnienie certyfikatów uznaje się za poprawny jeśli spełnia warunki punktu 4.1 oraz zawiera powód unieważnienia certyfikatów. Wniosek o unieważnienie certyfikatów winien zostać zatwierdzony przez osobę upoważnioną przez Dyrektora CPD.

4.6. Odnowienie certyfikatów

Wniosek o odnowienie certyfikatów uznaje się za poprawny jeśli spełnia warunki punktu 4.1 oraz został złożony przed upływem 14 dni przed terminem wygaśnięcia certyfikatów. Jeśli wniosek został złożony po tym terminie, ale przed terminem wygaśnięcia certyfikatów, to wniosek winien zostać zatwierdzony przez osobę upoważnioną przez Dyrektora CPD.

5. Środki bezpieczeństwa

5.1. Generowanie kluczy i certyfikatów

Generowanie kluczy i certyfikatów polega na włożeniu nośnika do czytnika kart, wpisaniu danych osobowych osoby, dla której mają zostać wygenerowane certyfikaty i uruchomieniu procesu generowania certyfikatów. Proces ten polega na utworzeniu dwóch par kluczy (publiczny i prywatny) i zapisaniu ich na nośniku. Po pobraniu z nośnika klucza publicznego, następuje utworzenie odpowiadających temu kluczowi certyfikatów klucza publicznego.

Klucze i certyfikaty generuje administrator lokalny CA lub osoba go zastępująca.

5.2. Ochrona kluczy posiadacza certyfikatów

Posiadacz certyfikatów jest właścicielem dwóch par kluczy: prywatnego i publicznego. Para kluczy jest generowana wewnątrz nośnika, a klucza prywatnego nie można odczytać.

Posiadacz certyfikatu jest zobowiązany do strzeżenia nośnika z certyfikatami przed zniszczeniem i przed nieautoryzowanym użyciem.

5.3. Niszczenie certyfikatów

Wszystkie certyfikaty, które zostały unieważnione muszą zostać odesłane do CA poprzez pocztę specjalną lub przesyłkę za potwierdzeniem odbioru w celu fizycznego zniszczenia nośnika. Nośniki z certyfikatami może niszczyć tylko osoba upoważniona przez Dyrektora CPD.

5.4. Osoba wnioskująca

Do obowiązków osoby wnioskującej należy:

1) przyjmować zapotrzebowanie na certyfikaty od pracowników z jednostki lokalnej oraz rzetelnie i obiektywnie oceniać czy należy pracownikowi wydać certyfikaty,

2) wypełniać wniosek o wydanie certyfikatów w obecności osoby zainteresowanej oraz zweryfikować tożsamość osoby ubiegającej się o wydanie certyfikatów,
3) dopilnować, aby osoba zainteresował uzyskaniem certyfikatów podpisała oświadczenie o zapoznaniu się ze wspomnianymi wcześniej dokumentami,
4) przygotować i podpisać zaświadczenie o zgodności danych osobowych pracownika zainteresowanego z danymi znajdującymi się na wniosku,
5) dopilnować, aby do wysyłanego wniosku załączyć wspomniane wyżej oświadczenie i zaświadczenie,
6) wysłanie wniosku przesyłką pocztową (dot. jednostki lokalnej) lub dostarczenie wniosku do CA (dot. CPD).

5.5. Weryfikacja certyfikatów

Każdy unieważniony lub zawieszony certyfikat zostanie wpisany do listy unieważnionych lub zawieszonych wniosków - CRL. Lista CRL jest przechowywana w Centrum Autoryzacji i natychmiast po dodaniu nowego wpisu jest rozsyłana do wszystkich jednostek lokalnych. Każda jednostka lokalna przechowuje kopie listy CRL.

Każda osoba próbująca zalogować się do systemu musi podać numer PIN nośnika certyfikatów, po którego wprowadzeniu w jednostce lokalnej następuje weryfikacja poprawności certyfikatu autoryzacji znajdującego się na nośniku poprzez sprawdzenie:

1) okresu ważności certyfikatu,
2) ścieżki certyfikacji – sprawdzenie wszystkich certyfikatów znajdujących się w ścieżce certyfikacji,
3) obecności certyfikatu na lokalnej liście CRL.:

Lokalna lista CRL znajduje się na serwerze w jednostce lokalnej i nie może się znajdować na stanowisku do wydawania dowodów osobistych i paszportów.

6. Dokumentacja

CA generuje i wydaje certyfikaty dla pracowników jednostek lokalnych oraz dla administratorów i pracowników CPD w Warszawie na podstawie niżej wymienionych dokumentów:

1) Wniosek o wydanie certyfikatów - wypełnia osoba wnioskująca oraz osoba ubiegająca się o certyfikat (usługobiorca),
2) Umowa o świadczenie usług certyfikacyjnych – wypełnia usługobiorca,

Dokumentacja winna być uzupełniona o załączoną do ww. dokumentacji jedną fotografią (w formie papierowej lub elektronicznej) usługobiorcy (użytkownika certyfikatów).

Komplet prawidłowo wypełnionej dokumentacji winien być przesłany do CA przez jednostkę lokalną przy użyciu bezpiecznej poczty (poczta specjalna lub przesyłka za potwierdzeniem odbioru). W przypadku dokumentów kierowanych do CA przez osobę wnioskującą z CPD, wniosek taki winien być dostarczony bezpośrednio do CA.