ZATWIERDZAM

.....

DYREKTOR
CENTRUM PERSONALIZACJI DOKUMENTÓW MSWiA

REGULAMIN CERTYFIKACJI CPD MSWIA

Warszawa, dn. 28 czerwca 2006 r.

SPIS TREŚCI

1. Wstęp

Niniejszy dokument oparty jest na polityce certyfikacji CPD MSWiA i rozszerza ją opisując bardziej szczegółowo zagadnienia, o których mowa w polityce.

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 w sprawie 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

Zastosowanie certyfikatów w pełni zdefiniowano w polityce certyfikacji CPD MSWiA.

2. Podstawowe zasady certyfikacji

2.1. Wydawanie certyfikatów

Certyfikaty wydawane są dla osoby wskazanej na odpowiednim wniosku. Certyfikaty, dane użytkownika certyfikatów oraz odpowiednie klucze są zapisane na odpowiednim nośniku, z którego nie mogą zostać usunięte.

Zapotrzebowanie na certyfikaty jest zgłaszane osobie wnioskującej. Osoba wnioskująca gromadzi i weryfikuje dane osobowe pracownika, który zgłosił zapotrzebowanie na certyfikaty.

Należy zgromadzić następujące dane:

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

Do tak przygotowanego wniosku osoba wnioskująca dodaje swoje dane osobowe:

- Imię,
- Nazwisko,
- PESEL
- kod terytorialny

Osoba wnioskująca podpisuje zaświadczenie o zgodności danych osobowych na wniosku, osoba ubiegająca się o certyfikaty podpisuje oświadczenie o zapoznaniu się z treścią dokumentów polityki certyfikacji oraz regulaminu certyfikacji oraz wypełnia umowę o świadczenie usług certyfikacyjnych.

Tak przygotowany wniosek i umowa wysyłane są do CA przez jednostkę lokalną przy użyciu bezpiecznej poczty (poczta specjalna lub przesyłka za potwierdzeniem odbioru). W przypadku wniosków kierowanych do CA przez osobę wnioskującą z CPD, wniosek taki winien być dostarczony bezpośrednio do CA.

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

2.2. Obowiązki stron

Obowiązki stron zostały opisane w polityce bezpieczeństwa

3. Zasady zarządzania certyfikatami

Dokumentację określoną punktem 6 regulaminu 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

Czynności, które należy wykonać w celu złożenia wniosku o wydanie certyfikatów:

1) Osoba, dla której wymagane są certyfikaty, zgłasza się z prośbą o wydanie certyfikatu do osoby wnioskującej.
2) Osoba wnioskująca sama może złożyć wniosek o wydanie certyfikatów dla osoby, dla której uważa, że certyfikaty są wymagane.
3) Osoba, dla której wymagane są certyfikaty winna zapoznać się z niniejszym regulaminem i polityką certyfikacji oraz podpisać oświadczenie o zapoznaniu się z tymi dokumentami.
4) Osoba wnioskująca winna potwierdzić tożsamość osoby, dla której wymagane są certyfikaty i podpisać stosowne zaświadczenie.
5) Osoba wnioskująca do składania wniosków winna wpisać na wniosek swoje dane osobowe:
   - Imię,
   - Nazwisko,
   - PESEL
   - kod terytorialny

   oraz dane osobowe osoby, dla której wymagane są certyfikaty:
   - imię

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

6) Osoba wnioskująca dołącza do wniosku oświadczenie, o którym mowa w podpunkcie 3) oraz zaświadczenie, o którym mowa w podpunkcie 4).
7) Osoba wnioskująca składa na wniosku swój podpis i swoją pieczęć.
8) Wniosek o wydanie certyfikatów należy wysłać pocztą specjalna lub przesyłką za potwierdzeniem odbioru (dot. jednostki lokalnej) lub dostarczyć bezpośrednio do CA (dot. CPD).
9) Osoba wnioskująca nie może złożyć we własnym imieniu wniosku o wydanie certyfikatów.

3.2. Wydanie certyfikatów

Wydanie certyfikatów polega na wykonaniu następujących czynności:

1) Należy zweryfikować poprawność wniosku o wydanie certyfikatów (punkt 4.1).
2) Należy sprawdzić kompletność danych osoby, dla której mają zostać wydane certyfikaty.
3) Certyfikaty należy wygenerować zgodnie z zasadami bezpieczeństwa (punkt 5.1).
4) Należy zweryfikować poprawność wygenerowanych certyfikatów (punkt 4.2).
5) Nośnik z certyfikatami należy wysłać bezpieczną pocztą MSWiA do osoby wnioskującej.

6) Osoba wnioskująca po otrzymaniu karty jest zobowiązana do akceptacji certyfikatów w obecności osoby, dla której certyfikaty zostały wydane (punkt 3.3).
7) Centrum Autoryzacji ma 14 dni na wydanie certyfikatów lub w przypadkach wymagających dodatkowych czynności okres ten wynosi 30 dni.

3.3. Akceptacja certyfikatów

1) Akceptacja certyfikatów winna się odbyć w obecności osoby wnioskującej oraz osoby, dla której certyfikaty zostały wydane.
2) Akceptacja powinna się odbyć w ciągu 2 dni od otrzymania certyfikatów. Po tym czasie uznaje się, że certyfikaty zostały zaakceptowane.
3) Akceptacja certyfikatu polega na próbie użycia go zgodnie z jego przeznaczeniem na stanowisku pracy osoby, dla której certyfikat został wydany.
4) Jeśli akceptacja zakończy się niepowodzeniem, wówczas należy niezwłocznie wysłać do CA wniosek o unieważnienie certyfikatów i o wydanie nowych.

3.4. Zawieszenie certyfikatów

1) Należy zweryfikować poprawność wniosku (punkt 4.1).
2) Należy sprawdzić czy podano przyczynę zawieszenia wniosku.
3) Należy uzyskać potwierdzenie wniosku u osoby upoważnionej przez Dyrektora CPD.
4) Jeśli nie uzyskano potwierdzenia, wówczas należy poinformować o tym fakcie osobę wnioskującą.
5) Należy oznaczyć certyfikaty jako zawieszone.
6) Należy uaktualnić listę CRL oraz wysłać nową listę do jednostek lokalnych.

3.5. Uchylenie zawieszenia certyfikatów

1) Należy zweryfikować poprawność wniosku (punkt 4.1).
2) Należy sprawdzić czy podano powód uchylenia zawieszenia certyfikatów.
3) Należy uzyskać potwierdzenie wniosku u osoby upoważnionej przez Dyrektora CPD.
4) Jeśli nie uzyskano potwierdzenia, wówczas należy poinformować o tym fakcie osobę wnioskującą.
5) Należy oznaczyć certyfikaty jako zawieszone.
6) Należy uaktualnić listę CRL oraz wysłać nową listę do jednostek lokalnych.
7) Uchylenie zawieszenia certyfikatów może nastąpić w ciągu 72 godzin od ich zawieszenia. Po upływie tego czasu certyfikaty automatycznie zostaną unieważnione.

3.6. Unieważnienie certyfikatów

1) Należy zweryfikować poprawność wniosku (punkt 4.1).
2) Należy sprawdzić czy podano powód unieważnienia certyfikatów.
3) Należy sprawdzić czy do wniosku załączono certyfikaty.
4) Jeśli nie załączono certyfikatów, wówczas należy uznać wniosek za nieważny i poinformować o tym fakcie osobę wnioskującą.
5) Należy uzyskać potwierdzenie wniosku u osoby upoważnionej przez Dyrektora CPD.
6) Jeśli nie uzyskano potwierdzenia, wówczas należy poinformować o tym fakcie osobę wnioskującą.
7) Jeśli uzyskano potwierdzenie, wówczas należy unieważnić i zniszczyć certyfikaty.
8) Należy uaktualnić listę CRL oraz wysłać nową listę do jednostek lokalnych.
9) Certyfikaty mogą zostać unieważnione z innych powodów, które zostały opisane w polityce certyfikacji.

10) Certyfikaty nie mogą zostać unieważnione ze wsteczną datą.

3.7. Odnowienie certyfikatów

1) Należy zweryfikować poprawność wniosku (punkt 4.1).
2) Jeśli wniosek został złożony później niż 14 dni przed upływem terminu ważności certyfikatów wówczas należy potwierdzić wniosek u osoby upoważnionej przez Dyrektora CPD.
3) Zakłada się, że dane osobowe znajdujące się w certyfikatach nie zmieniły się i dane te zostaną wykorzystane do wygenerowania nowych certyfikatów.
4) Nowe certyfikaty należy wygenerować zgodnie z zasadami bezpieczeństwa (punkt 5.1).
5) Należy zweryfikować poprawność wygenerowanych certyfikatów (punkt 4.2). Certyfikaty będą ważne od daty wygaśnięcia poprzednich certyfikatów.
6) Nośnik z certyfikatami należy wysłać bezpieczną pocztą MSWiA do osoby wnioskującej.
7) Osoba wnioskująca po otrzymaniu certyfikatów jest zobowiązana do akceptacji certyfikatów w obecności osoby, dla której certyfikaty zostały wydane (punkt 3.3). Akceptacja certyfikatów winna się odbyć w ciągu 2 dni od otrzymania nośnika.
8) Osoba wnioskująca jest zobowiązana do odesłania starych, nieważnych certyfikatów do CA przy pomocy poczty specjalnej lub przesyłki za potwierdzeniem odbioru (dot. jednostki lokalnej) lub dostarczyć bezpośrednio do CA (dot. CPD).
9) Centrum Autoryzacji ma 14 dni na wydanie nowych certyfikatów lub w przypadkach wymagających dodatkowych czynności okres ten wynosi 30 dni.

4. Weryfikacja i uwierzytelnianie tożsamości

Rozdział określa sposób weryfikacji poprawności wniosków oraz uwierzytelnienia tożsamości osób ubiegających się o wydanie certyfikatów.

4.1. Rejestracja wniosków

Weryfikacja poprawności nadesłanych wniosków jest w pełni opisana w polityce certyfikacji CPD MSWiA.

4.2. Wydanie certyfikatów

Weryfikacja poprawności wygenerowanych certyfikatów jest w pełni opisana w polityce certyfikacji CPD MSWiA.

4.3. Zawieszenie certyfikatów

Weryfikacja poprawności informacji zamieszczonych na wniosku o zawieszenie certyfikatów jest w pełni opisana w polityce certyfikacji CPD MSWiA.

4.4. Uchylenie zawieszenia certyfikatów

Weryfikacja poprawności informacji zamieszczonych na wniosku o uchylenie zawieszenia certyfikatów jest w pełni opisana w polityce certyfikacji CPD MSWiA.

4.5. Unieważnienie certyfikatów

Weryfikacja poprawności informacji zamieszczonych na wniosku o unieważnienie certyfikatów jest w pełni opisana w polityce certyfikacji CPD MSWiA.

4.6. Odnowienie certyfikatów

Po wygenerowaniu nowych certyfikatów należy:

1) Sprawdzić czy data początku ważności nowego certyfikatu jest zgodna z datą

końca ważności starego certyfikatu.

2) Sprawdzić czy dane zapisane w nowym certyfikacie zgadzają się z danymi w starym certyfikacie (punkt 4.2 polityki certyfikacji).

5. Środki bezpieczeństwa

5.1. Generowanie kluczy i certyfikatów

Sposób generowania kluczy i certyfikatów został opisany w polityce bezpieczeństwa CPD MSWiA.

5.2. Ochrona kluczy posiadacza certyfikatów

Informacje dotyczące ochrony kluczy posiadacza certyfikatów zostały opisane w polityce bezpieczeństwa CPD MSWiA.

5.3. Niszczenie certyfikatów

Informacje dotyczące niszczenia certyfikatów zostały opisane w polityce bezpieczeństwa CPD MSWiA.

5.4. Osoba wnioskująca

Informacje dotyczące osoby wnioskującej zostały opisane w polityce bezpieczeństwa CPD MSWiA.

5.5. Weryfikacja certyfikatów

Informacje dotyczące weryfikacji certyfikatów zostały opisane w polityce bezpieczeństwa CPD MSWiA.

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.