INSTRUKCJA Nr 13 / 2010

DYREKTORA GENERALNEGO SŁUŻBY WIĘZIENNEJ

z dnia 13 sierpnia 2010 r.

w sprawie szczegółowych zasad i trybu postępowania certyfikacyjnego wobec użytkowników systemu Centralna Baza Danych Osób Pozbawionych Wolności Noe.NET

Na podstawie art. 11 ust. 1 pkt 11 ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej (Dz. U. Nr 79, poz. 523) ustala się, co następuje:

Rozdział 1
Przepisy ogólne

§ 1.

Instrukcja określa szczegółowe zasady i tryb postępowania certyfikacyjnego wobec użytkowników systemu Centralna Baza Danych Osób Pozbawionych Wolności Noe.NET oraz obowiązki i zakres odpowiedzialności uczestników tego postępowania.

§ 2.

Przez użyte w instrukcji określenie lub skrót należy rozumieć:

1) Active Directory – usługa katalogowa mająca postać hierarchicznej bazy danych, w której przechowuje się informacje o: obiektach tworzących sieć, komputerach, polityce zabezpieczeń, użytkownikach systemu oraz zablokowanych kontach użytkowników systemu, umożliwiająca hierarchiczne zarządzanie grupami użytkowników systemu pracującymi w wydzielonej sieci;
2) Administrator Danych – Administrator Danych Osobowych Centralnego Zarządu Służby Więziennej lub upoważniona przez niego osoba;
3) Centralny Zarząd – Centralny Zarząd Służby Więziennej;
4) certyfikacja – realizacja czynności certyfikacyjnych wobec funkcjonariuszy i pracowników Służby Więziennej, prowadzonych celem wykonywania przez nich zadań służbowych w systemie Centralna Baza Danych Osób Pozbawionych Wolności Noe.NET;
5) certyfikat – zapisany na karcie kryptograficznej elektroniczny dokument, za pomocą którego dane służące do uwierzytelnienia są przyporządkowane do konkretnego funkcjonariusza lub pracownika Służby Więziennej;
6) CRL – lista certyfikatów unieważnionych, dostępna tylko dla Punktu Certyfikacji, prowadzona w formie elektronicznego dokumentu zawierającego numery unieważnionych certyfikatów oraz daty i przyczyny ich unieważnienia;

7) czynności certyfikacyjne – czynności związane z rejestracją użytkowników systemu, w szczególności wydawaniem kart kryptograficznych, wydawaniem i unieważnianiem certyfikatów użytkownikom systemu, przyznawaniem i usuwaniem ról użytkownikom systemu;
8) Dyrektor Generalny – Dyrektor Generalny Służby Więziennej;
9) jednostka organizacyjna - Centralny Zarząd Służby Więziennej, okręgowe inspektoraty Służby Więziennej, zakłady karne i areszty śledcze, Centralny Ośrodek Szkolenia Służby Więziennej, ośrodki szkolenia i ośrodki doskonalenia kadr Służby Więziennej;
10) karta kryptograficzna – elektroniczna karta identyfikacyjna, na której znajduje się certyfikat wydany dla konkretnego, imiennie określonego funkcjonariusza lub pracownika Służby Więziennej;
11) nieaktywna karta kryptograficzna – karta kryptograficzna do czasu jej aktywacji przez użytkownika systemu, która następuje poprzez pierwsze zalogowanie do systemu Centralna Baza Danych Osób Pozbawionych Wolności Noe.NET;
12) kod PIN – osobisty numer identyfikacyjny, poufny kod zabezpieczający kartę kryptograficzną przed możliwością jej użycia przez osoby nieuprawnione, który łącznie z certyfikatem zapisanym na karcie służy do elektronicznej weryfikacji użytkownika systemu;
13) komunikat – informacja wymieniana pomiędzy wnioskodawcą a Punktem Certyfikacyjnym za pośrednictwem poczty elektronicznej lub telefaksu;
14) Punkt Certyfikacji – powołane w Centralnym Zarządzie, zespołowe stanowisko pracy realizujące czynności certyfikacyjne;
15) rola – określony poziom uprawnień związanych z dostępem do systemu Centralna Baza Danych Osób Pozbawionych Wolności Noe.NET, który odpowiada aktualnemu zakresowi obowiązków służbowych wykonywanych przez funkcjonariusza lub pracownika Służby Więziennej;
16) system – system Centralna Baza Danych Osób Pozbawionych Wolności Noe.NET;
17) unieważnienie certyfikatu – odwołanie ważności certyfikatu w przypadku, gdy zachodzi konieczność uniemożliwienia użytkownikowi dostępu do systemu;
18) użytkownik systemu – uprawniony funkcjonariusz albo pracownik Służby Więziennej, posiadający dostęp do systemu;
19) wdrożenie systemu – rozpoczęcie procesu wprowadzania systemu do użytkowania w jednostkach organizacyjnych;
20) wniosek certyfikacyjny – dokument dotyczący wydania lub unieważnienia certyfikatu użytkownika systemu, przyznania albo usunięcia roli lub ról dla użytkownika systemu, zmiany danych identyfikacyjnych użytkownika systemu;
21) wnioskodawca – kierownik komórki organizacyjnej Centralnego Zarządu, dyrektor okręgowy Służby Więziennej, dyrektor aresztu śledczego lub zakładu karnego, komendant Centralnego Ośrodka Szkolenia Służby Więziennej, ośrodka szkolenia lub ośrodka doskonalenia kadr Służby Więziennej, jak również osoba upoważniona do złożenia wniosków przez wyżej wymienione osoby;
22) wydanie certyfikatu – wygenerowanie i zapisanie certyfikatu na karcie kryptograficznej przez Punkt Certyfikacji;
23) wygaśnięcie certyfikatu – upływ okresu, na jaki certyfikat został wydany lub jego unieważnienie przez Administratora Danych;
24) zablokowanie konta użytkownika systemu – zablokowanie w Active Directory możliwości dostępu do systemu przez użytkownika systemu.

Rozdział 2
Punkt Certyfikacji

§ 3.

1. Punkt Certyfikacji przeprowadza czynności certyfikacyjne wobec użytkowników systemu.
2. Punkt Certyfikacji nie ujawnia informacji o certyfikatach i użytkownikach systemu osobom trzecim. Informacje takie mogą być ujawnione na żądanie sądu lub prokuratora, w związku z toczącym się postępowaniem, a w innych przypadkach udzielone jedynie za zgodą Administratora Danych.
3. Punkt Certyfikacji nie ponosi odpowiedzialności za skutki użycia certyfikatów w jednostkach organizacyjnych.
4. Nadzór nad wykonywaniem zadań przez Punkt Certyfikacji sprawuje Administrator Danych.

§ 4.

1. Punkt Certyfikacji prowadzi w postaci elektronicznej rejestr użytkowników systemu, w którym odnotowuje się, w szczególności, dane identyfikacyjne użytkowników systemu, daty wydania i unieważnienia certyfikatów, daty upływu ważności certyfikatów, identyfikatory użytkowników systemu oraz przyznane im role.
2. Punkt Certyfikacji gromadzi dokumentację dotyczącą postępowania certyfikacyjnego oraz prowadzi niezbędną korespondencję w tym zakresie.
3. Wzór rejestru użytkowników systemu, zwanego dalej „rejestrem użytkowników", określa załącznik nr 1 do instrukcji.

Rozdział 3
Wniosek certyfikacyjny

§ 5.

1. Rejestracja nowych użytkowników systemu, wydawanie i unieważnianie certyfikatów, przyznawanie ról oraz ich usuwanie, a także zmiana danych identyfikacyjnych użytkownika systemu następuje na podstawie wniosku certyfikacyjnego.
2. Wniosek certyfikacyjny sporządza wnioskodawca. Wzór wniosku certyfikacyjnego określa załącznik nr 2 do instrukcji.
3. Wniosek certyfikacyjny sporządza się w formie pisemnej w dwóch egzemplarzach. Jeden egzemplarz wniosku doręcza się listem poleconym do Punktu Certyfikacji, z zastrzeżeniem § 7, a drugi egzemplarz włącza się do akt osobowych użytkownika systemu.
4. Komórka kadrowa w jednostce organizacyjnej, gromadzi dokumentację dotyczącą postępowania certyfikacyjnego prowadzonego wobec użytkowników pełniących służbę albo zatrudnionych w tej jednostce.
5. Zasady gromadzenia i prowadzenia dokumentacji, o której mowa w ust.4, w Centralnym Zarządzie regulują odrębne przepisy.
6. Wydanie nowego certyfikatu wiąże się z wydaniem nowej nieaktywnej karty kryptograficznej; ust. 1 i 3 stosuje się odpowiednio.
7. Przyznanie użytkownikowi systemu nowej roli lub ról lub też ich usunięcie nie wymaga wydania nowego certyfikatu.

8. Certyfikat jest ważny przez okres jednego roku od dnia jego wydania.
9. Użytkownik systemu może posiadać tylko jedną kartę kryptograficzną. W uzasadnionych przypadkach Administrator Danych może wyrazić zgodę na wydanie jednemu użytkownikowi systemu więcej niż jednej karty kryptograficznej; ust. 1 i 3 stosuje się odpowiednio.
10. Punkt Certyfikacji potwierdza otrzymanie wniosku certyfikacyjnego odpowiednim komunikatem.

§ 6.

1. Określona we wniosku rola lub role, o których przyznanie dla użytkownika systemu wnosi wnioskodawca, powinny być zgodne z jego aktualnym zakresem obowiązków, a zawarte we wniosku dane identyfikacyjne zgodne z danymi zawartymi w jego aktach osobowych. Wykaz ról użytkowników systemu stanowi załącznik nr 3 do instrukcji.
2. Jeśli zachodzi konieczność zmiany roli lub ról w związku ze zmianą zakresu obowiązków służbowych użytkownika systemu, stosuje się odpowiednio § 5 ust. 1 i 3.

§ 7.

1. Wniosek certyfikacyjny może być przesłany do Punktu Certyfikacji za pośrednictwem telefaksu, tylko w nagłym przypadku, uzasadnionym ważnym interesem służby.
2. W okolicznościach, o których mowa w ust. 1, oryginał wniosku należy niezwłocznie doręczyć listem poleconym do Punktu Certyfikacji; § 5 ust. 3 stosuje się odpowiednio.
3. Wniosek, o którym mowa w ust. 1, może dotyczyć wyłącznie unieważnienia certyfikatu albo przyznania lub usunięcia nowej roli lub ról użytkownikowi systemu, który już posiada kartę kryptograficzną.

Rozdział 4
Czynności certyfikacyjne

§ 8.

1. Po otrzymaniu wniosku certyfikacyjnego Punkt Certyfikacji dokonuje odpowiednich czynności certyfikacyjnych.
2. W razie wystąpienia wątpliwości co do:
   1) autentyczności wniosku certyfikacyjnego;
   2) prawidłowości danych zawartych we wniosku certyfikacyjnym;
   3) zgodności użytkownika systemu z danymi identyfikacyjnymi zawartymi we wniosku certyfikacyjnym;
   4) spełnienia wymogów określonych w załącznikach 2, 4,5 i 7 do instrukcji

   - Punkt Certyfikacji powiadamia o tym wnioskodawcę komunikatem, celem potwierdzenia autentyczności wniosku, sprostowania omyłek lub jego uzupełnienia.
3. Punkt Certyfikacji nie jest uprawniony do dokonywania zmian we wniosku certyfikacyjnym.

§ 9.

1. W przypadku konieczności dokonania zmian we wniosku certyfikacyjnym przed jego akceptacją przez Administratora Danych, w szczególności w przypadkach, o których

mowa w § 8 ust. 2, wnioskodawca przesyła ponownie wniosek certyfikacyjny do Punktu Certyfikacji.

2. W przypadku, gdy zmiana dotyczy oczywistych omyłek pisarskich, wniosek o którym mowa w ust. 1, wnioskodawca przesyła niezwłocznie za pośrednictwem telefaksu, zaś oryginał w sposób określony w § 5 ust. 3.

§ 10.

1. Po wykonaniu czynności certyfikacyjnych, wniosek certyfikacyjny podlega akceptacji przez Administratora Danych. Punkt Certyfikacji, wraz z wnioskiem certyfikacyjnym, przedstawia Administratorowi Danych opinię w zakresie spraw objętych wnioskiem.
2. Administrator Danych odmawia akceptacji wniosku certyfikacyjnego w przypadku, gdy zakres uprawnień związanych z proponowaną do przyznania użytkownikowi systemu rolą lub grupą ról nie odpowiada aktualnemu zakresowi obowiązków służbowych wykonywanych przez użytkownika systemu.
3. Administrator Danych nie jest uprawniony do dokonywania zmian we wniosku certyfikacyjnym.
4. O odmowie akceptacji wniosku certyfikacyjnego przez Administratora Danych, Punkt Certyfikacji powiadamia wnioskodawcę odpowiednim komunikatem.

§ 11.

W przypadkach, o których mowa w § 8 ust. 2 i § 10 ust. 2, wnioskodawca, jeżeli nie wystąpiły inne okoliczności uniemożliwiające posiadanie przez funkcjonariusza lub pracownika Służby Więziennej dostępu do systemu, zobowiązany jest do usunięcia uchybień i ponownego przesłania wniosku certyfikacyjnego do Punktu Certyfikacji; § 5 ust. 3 stosuje się odpowiednio.

§ 12.

1. W przypadku akceptacji przez Administratora Danych wniosku certyfikacyjnego, Punkt Certyfikacji rejestruje użytkownika systemu w rejestrze użytkowników oraz tworzy jego unikalny identyfikator w Active Directory oraz wystawia nieaktywną kartę kryptograficzną.
2. Punkt Certyfikacji odnotowuje we wniosku certyfikacyjnym:
   1) identyfikator użytkownika systemu;
   2) datę upływu ważności certyfikatu;
   3) przyznaną rolę lub grupę ról.
3. Punkt Certyfikacji przechowuje i gromadzi wnioski certyfikacyjne oraz pozostałą korespondencję w tym zakresie.

§ 13.

1. W przypadku, gdy wniosek certyfikacyjny dotyczy unieważnienia certyfikatu, Punkt Certyfikacji niezwłocznie blokuje konto użytkownika systemu w Active Directory oraz unieważnia certyfikat; § 10 ust. 1 stosuje się odpowiednio.

2. Unieważniony certyfikat umieszcza się na liście CRL.
3. Punkt Certyfikacji odpowiednim komunikatem powiadamia wnioskodawcę o unieważnieniu certyfikatu. W przypadku, o którym mowa w § 14 ust. 3, informuje się wnioskodawcę o przyczynie unieważnienia certyfikatu.

§ 14.

1. W przypadku przewidywanego ustania stosunku służby lub pracy z użytkownikiem systemu, wnioskodawca przesyła listem poleconym, z odpowiednim wyprzedzeniem, wniosek certyfikacyjny do Punktu Certyfikacji. We wniosku określa się datę, z której upływem certyfikat powinien być unieważniony. Punkt Certyfikacji w wyznaczonym dniu:
   1) blokuje konto użytkownika systemu w Active Directory;
   2) unieważnia certyfikat, który umieszczony zostaje na liście CRL.
2. W przypadku, gdy użytkownik systemu:
   1) zostanie przeniesiony albo delegowany do czasowego pełnienia służby w innej jednostce organizacyjnej;
   2) ma powierzone pełnienie obowiązków służbowych na innym stanowisku w tej samej miejscowości;
   3) zostanie zawieszony w czynnościach służbowych

   - następuje zablokowanie konta użytkownika systemu przez Punkt Certyfikacji, do czasu przesłania nowego wniosku certyfikacyjnego przez właściwego wnioskodawcę.
3. Punkt Certyfikacji w przypadku:
   1) otrzymania pisemnego żądania zablokowania użytkownika systemu wystawionego przez sąd lub prokuratora prowadzącego postępowanie karne;
   2) uzyskania informacji, że użytkownik systemu jest podejrzany lub oskarżony o czyn przestępny, którego popełnienie związane było z korzystaniem lub dostępem do systemu

   - dokonuje zablokowania konta takiego użytkownika systemu, do czasu otrzymania pisemnego potwierdzenia od wnioskodawcy, iż użytkownik może korzystać z systemu.
4. W przypadku, o którym mowa w ust. 3, § 10 ust. 1 stosuje się odpowiednio.

§ 15.

1. Punkt Certyfikacji komunikatem powiadamia wnioskodawcę o upływie daty ważności certyfikatu, nie później niż na miesiąc przed jej upływem. Wnioskodawca niezwłocznie po otrzymaniu komunikatu podejmuje decyzję w zakresie wydania nowego certyfikatu, w szczególności przesyła wniosek certyfikacyjny, w którym wnosi o wydanie nowego certyfikatu użytkownikowi systemu oraz przyznanie mu roli lub ról; w przypadku wystąpienia z wnioskiem o wydanie nowego certyfikatu użytkownikowi systemu § 5 stosuje się odpowiednio.
2. Punkt Certyfikacji, po wykonaniu czynności certyfikacyjnych, przesyła wnioskodawcy nieaktywną kartę kryptograficzną, wraz z kodem PIN; § 16 ust. 1-5 stosuje się odpowiednio.

Rozdział 5
Postępowanie z kartami kryptograficznymi

§ 16.

1. Punkt Certyfikacji wystawia użytkownikom systemu nieaktywne karty kryptograficzne wraz z kodem PIN, zgodnie z wnioskiem certyfikacyjnym.
2. Nieaktywne karty kryptograficzne, o których mowa w ust. 1, przesyłane są wnioskodawcy, w miarę możliwości jedną, odpowiednio zabezpieczoną przesyłką poleconą. Przesyłka składa się z dwóch kopert:
   1) koperty zewnętrznej – adresowanej do rąk wnioskodawcy;
   2) koperty wewnętrznej – zawierającej nieaktywną kartę kryptograficzną z dopiskiem „do rąk własnych", adresowanej do użytkownika systemu.
3. W przypadku, o którym mowa w ust. 2, § 17 stosuje się odpowiednio.
4. Zabezpieczenie kart kryptograficznych, o których mowa w ust. 2, polega na użyciu kopert bąbelkowych lub usztywnień zapobiegających uszkodzeniu fizycznemu.
5. Dla każdej karty kryptograficznej, kod PIN przesyła się użytkownikowi systemu za pośrednictwem wnioskodawcy, osobną przesyłką poleconą, w sposób uniemożliwiający jego odczytanie.
6. Wnioskodawca powiadamia komunikatem Punkt Certyfikacji o otrzymaniu:
   1) przesyłki zawierającej nieaktywną kartę kryptograficzną;
   2) koperty zawierającej kod PIN.
7. Wnioskodawca przekazuje nieaktywną kartę kryptograficzną użytkownikowi systemu wraz z właściwą kopertą, zawierającą kod PIN. Użytkownik systemu własnoręcznym i czytelnym podpisem potwierdza fakt odbioru nieaktywnej karty kryptograficznej oraz kodu PIN. Kopie druków podpisanych przez użytkownika systemu wnioskodawca dołącza do wniosku certyfikacyjnego, zaś oryginały tych druków doręcza przesyłką poleconą do Punktu Certyfikacji.
8. Wzór druku potwierdzającego otrzymanie nieaktywnej karty kryptograficznej użytkownika systemu stanowi załącznik nr 4 a wzór druku potwierdzającego otrzymanie kodu PIN karty kryptograficznej użytkownika systemu stanowi załącznik nr 5 do instrukcji.

§ 17.

1. Po otrzymaniu nieaktywnej karty kryptograficznej, uprawniony użytkownik systemu dokonuje niezwłocznej zmiany kodu PIN.
2. Kod PIN powinien składać się z co najmniej 4 cyfr.
3. Trzykrotne wprowadzenie nieprawidłowego kodu PIN powoduje zablokowanie karty kryptograficznej lub nieaktywnej karty kryptograficznej oraz utratę możliwości korzystania z systemu; § 20 stosuje się odpowiednio.
4. Użytkownik systemu:
   1) aktywuje kartę kryptograficzną, poprzez zalogowanie się do systemu;
   2) sprawdza, czy przyznany dostęp do systemu jest zgodny z jego aktualnym zakresem obowiązków służbowych;
   3) w przypadku stwierdzenia niezgodności zakresu dostępu do systemu z zakresem jego obowiązków służbowych, niezwłocznie informuje o tym bezpośredniego przełożonego;
   4) nie odstępuje karty kryptograficznej osobom trzecim;

5) samodzielnie zmienia kod PIN, nie rzadziej, niż co 30 dni;
6) nie udostępnia swojego kodu PIN osobom trzecim;
7) posługuje się kartą kryptograficzną wyłącznie podczas pracy w systemie;
8) zamyka system oraz usuwa kartę kryptograficzną z czytnika przy każdorazowym opuszczeniu stanowiska pracy, nawet w przypadku, gdy stanowisko to jest zabezpieczone przed dostępem innych osób;
9) nie wynosi karty kryptograficznej poza teren jednostki organizacyjnej, w której pełni służbę lub jest zatrudniony, z zastrzeżeniem ust. 6-9;
10) przechowuje kartę kryptograficzną w bezpiecznym miejscu;
11) po zakończeniu wykonywania zadań służbowych, wymagających pracy w systemie, pozostawia kartę kryptograficzną w miejscu wyznaczonym przez wnioskodawcę, z zastrzeżeniem ust. 6-9.

5. W przypadku, o którym mowa w ust. 4 pkt 3, wnioskodawca przesyła do Punktu Certyfikacji komunikat informujący o konieczności sprawdzenia, czy przyznany użytkownikowi dostęp do systemu odpowiada roli lub rolom, o których przyznanie wnioskodawca wnosił we wniosku certyfikacyjnym; § 7 stosuje się odpowiednio.
6. W przypadku wykonywania przez funkcjonariuszy lub pracowników Centralnego Zarządu czynności służbowych w okręgowych inspektoratach Służby Więziennej, zakładach karnych, aresztach śledczych oraz Centralnym Ośrodku Szkolenia Służby Więziennej, ośrodkach szkolenia i ośrodkach doskonalenia kadr Służby Więziennej, w szczególności czynności kontrolnych, ust. 4 pkt 9 i 11 nie stosuje się.
7. Przepis ust. 6 stosuje się odpowiednio do funkcjonariuszy lub pracowników okręgowego inspektoratu Służby Więziennej.
8. Funkcjonariusz lub pracownik, o którym mowa w ust. 6 i 7, musi uzyskać pisemną zgodę wnioskodawcy na wyniesienie karty kryptograficznej poza teren jednostki organizacyjnej użytkownika systemu. Zgodę tę dołącza się do dokumentacji użytkownika systemu w jednostce organizacyjnej.
9. Wzór wniosku o uzyskanie zgody, o której mowa w ust. 8, określa załącznik nr 6 do instrukcji.

§ 18.

W przypadku, o którym mowa w § 14 ust. 1, po ustaniu stosunku służbowego lub stosunku pracy użytkownika systemu, wnioskodawca listem poleconym dostarcza kartę kryptograficzną do Punktu Certyfikacji i odnotowuje ten fakt we wniosku certyfikacyjnym. Otrzymanie karty kryptograficznej Punkt Certyfikacji odnotowuje w rejestrze, powiadamiając o tym odpowiednim komunikatem wnioskodawcę. Kopertę z kartą kryptograficzną zabezpiecza się w sposób, o którym mowa w § 16 ust. 2, 4 i 5.

§ 19.

1. Użytkownik systemu przekazuje wnioskodawcy używaną przez siebie kartę kryptograficzną niezwłocznie po otrzymaniu nowej nieaktywnej karty kryptograficznej lub po wygaśnięciu certyfikatu. Wnioskodawca odnotowuje ten fakt we wniosku certyfikacyjnym.
2. Wnioskodawca niezwłocznie doręcza przesyłką poleconą dotychczas używaną kartę kryptograficzną do Punktu Certyfikacji; § 16 ust. 2 i 4 stosuje się odpowiednio.

3. Punkt Certyfikacji po otrzymaniu karty kryptograficznej, o której mowa w ust. 2, odnotowuje ten fakt w rejestrze, powiadamiając o tym odpowiednim komunikatem wnioskodawcę.
4. Konto użytkownika systemu, którego certyfikat wygasł, zostaje zablokowane w Active Directory, do czasu wystawienia nowego certyfikatu. Wygasły certyfikat znajduje się na liście CRL.

§ 20.

1. Użytkownik systemu niezwłocznie powiadamia wnioskodawcę o zagubieniu albo zniszczeniu lub uszkodzeniu karty kryptograficznej.
2. W przypadku powzięcia informacji o zagubieniu, zniszczeniu lub uszkodzeniu karty kryptograficznej użytkownika systemu, wnioskodawca natychmiast powiadamia odpowiednim komunikatem Punkt Certyfikacji lub dyżurującego Administratora systemu Neo.NET w Centralnym Zarządzie, przesyłając jednocześnie dokument, o którym mowa w ust. 3. Po otrzymaniu komunikatu konto użytkownika systemu zostaje zablokowane w Active Directory.
3. Wzór zgłoszenia, o którym mowa w ust.2, stanowi załącznik nr 7 do instrukcji.
4. Punkt Certyfikacji po otrzymaniu powiadomienia, o którym mowa w ust. 2, niezwłocznie odnotowuje ten fakt w rejestrze, unieważnia certyfikat i usuwa przyznane role, powiadamiając o tym odpowiednim komunikatem wnioskodawcę.
5. O czynnościach, o których mowa w ust. 4, Punkt Certyfikacji powiadamia niezwłocznie Administratora Danych.
6. Wnioskodawca podejmuje decyzję w zakresie wydania nowego certyfikatu użytkownikowi systemu, o którym mowa w ust. 1, po przesłaniu wniosku certyfikacyjnego, w którym wnosi o wydanie nowej karty kryptograficznej z nowym certyfikatem oraz dotychczasowa rolą lub rolami; tryb określony w § 7 stosuje się odpowiednio.
7. Nieaktywną kartę kryptograficzną, wraz z kodem PIN, przesyła się wnioskodawcy; § 16 stosuje się odpowiednio.
8. Wnioskodawca niezwłocznie przesyła do Punktu Certyfikacji zniszczoną lub uszkodzoną kartę kryptograficzną, a także kartę kryptograficzną odnalezioną, którą uprzednio zgłoszono jako zagubioną. Kopertę z kartą kryptograficzną zabezpiecza się w sposób, o którym mowa w § 16 ust. 2, 4 i 5. Punkt Certyfikacji odnotowuje fakt otrzymania karty w prowadzonym rejestrze.
9. W razie zablokowania karty kryptograficznej, zabrania się użytkownikowi systemu wykonywania prób samodzielnego jej odblokowania. W przypadku zablokowania karty kryptograficznej wnioskodawca niezwłocznie przesyła ją do Punktu Certyfikacji, celem odblokowania. Przy przesłaniu zablokowanej karty kryptograficznej stosuje się § 16 ust. 2, 4 i 5. Punkt Certyfikacji po odblokowaniu karty przesyła ją w sposób określony w § 16.
10. W przypadku stwierdzenia przez Punkt Certyfikacji trwałego zablokowana karty kryptograficznej przez użytkownika systemu, spowodowanego próbą samodzielnego jej odblokowania, Punkt Certyfikacji pisemnie powiadamia o tym fakcie Administratora Danych.
11. Ustęp 1-10 stosuje się odpowiednio do nieaktywnych kart kryptograficznych.

Rozdział 6
Tryb szczególny certyfikacji

§ 21.

W przypadku uzasadnionym koniecznością zapewnienia sprawnego funkcjonowania systemu, Administrator Danych może, na czas określony, zmienić zakres uprawnień związanych z dostępem do systemu, poprzez ograniczenie lub rozszerzenie przyznanych ról, określonych w wykazie stanowiącym załącznik nr 3 do instrukcji.

§ 22.

1. Dostęp do systemu mogą również uzyskać, na podstawie odrębnych przepisów, inni użytkownicy, niż określeni w § 2 pkt 18.
2. Wydanie certyfikatu i karty kryptograficznej użytkownikom, o których mowa w ust. 1, odbywa się za zgodą Administratora Danych, na zasadach określonych w niniejszej instrukcji. Administrator Danych określa w odrębnym porozumieniu, w szczególności, zakres uprawnień przysługujących tym użytkownikom.

Rozdział 7
Przepisy wprowadzające i końcowe

§ 23.

Wnioskodawca określi i wdroży, w terminie 30 dni od dnia wejścia w życie niniejszej instrukcji, przepisy wewnętrzne, określające sposób przechowywania kart kryptograficznych, z uwzględnieniem, w szczególności, konieczności zabezpieczenia ich przed użyciem przez nieuprawnione osoby.

§ 24.

1. Certyfikaty wydane przed wejściem w życie niniejszej instrukcji zachowują ważność przez okres jednego roku od momentu ich wydania, z zastrzeżeniem ust. 2 i 3.
2. W przypadku, o którym mowa w ust. 1, wnioskodawca przesyła wniosek, o którym mowa w § 5 ust. 3. Wniosek ten przesyła się w terminie 30 dni od dnia wejścia w życie niniejszej instrukcji
3. Po upływie terminu, o którym mowa w ust. 2, Punkt Certyfikacji niezwłocznie blokuje konto użytkownika systemu w Active Directory oraz unieważnia certyfikat.

§ 25.

Instrukcja wchodzi w życie z dniem 13 sierpnia 2010 r.

Dyrektor Generalny Służby Więziennej

ZARZĄD SŁUŻBY WIĘZIENNEJ CENTRALNY

płk Kajetan Dubiel