Warszawa, dnia 5 lutego 2014 r.

Poz. 9

ZARZĄDZENIE NR 5
KOMENDANTA GŁÓWNEGO POLICJI

z dnia 29 stycznia 2014 r.

w sprawie form uwierzytelniania użytkowników systemów teleinformatycznych Policji przeznaczonych do przetwarzania informacji jawnych

Na podstawie art. 7 ust. 1 pkt 2 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2011 r. Nr 287, poz. 1687, ze. zm.[1)]) zarządza się, co następuje:

§ 1. Zarządzenie określa tryb przydzielania oraz postępowania z kartami mikroprocesorowymi, wykorzystywanymi w celu identyfikacji i uwierzytelniania użytkowników podczas logowania się do części jawnej systemów teleinformatycznych Policji.

§ 2. Użyte w zarządzeniu określenia oznaczają:

1) administrator centralny – Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji;

2) administrator lokalny – kierownika właściwej do spraw łączności i informatyki, komórki organizacyjnej komendy wojewódzkiej (Stołecznej) Policji;

3) KM – kartę mikroprocesorową, umożliwiającą identyfikację i uwierzytelnienie użytkownika;

4) KSD – kartę typu microSD z wbudowanym kryptoprocesorem, umożliwiającą identyfikację i uwierzytelnienie użytkownika mobilnego terminala noszonego;

5) aktywacja – umieszczenie w bazie danych systemu BTUU informacji o certyfikacie klucza publicznego wygenerowanym na KM lub KSD;

6) BTUU – bezpieczny tryb uwierzytelnienia użytkowników, stanowiący system umożliwiający identyfikację, uwierzytelnianie i autoryzację użytkowników zasobów informacyjnych systemów teleinformatycznych Policji;

7) certyfikat – zestaw podpisanych cyfrowo danych;

8) PKI – Infrastrukturę Klucza Publicznego, stanowiącą system organizacyjno-informatyczny, w którego skład wchodzą urzędy certyfikacyjne, urzędy (punkty) rejestracyjne, użytkownicy certyfikatów klucza publicznego (subskrybenci – użytkownicy systemów teleinformatycznych Policji), oprogramowanie i sprzęt;

9) PR – zlokalizowany w komendzie wojewódzkiej (Stołecznej) Policji punkt rejestracji, stanowiący element systemu PKI, realizujący czynności związane z aktywacją, dezaktywacją, recertyfikacją i odblokowaniem KM lub KSD - dla użytkowników pełniących służbę lub zatrudnionych w komendzie wojewódzkiej (Stołecznej) Policji oraz w podległych jednostkach organizacyjnych Policji;

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2012 r. poz. 627, 664, 908, 951 i 1529, z 2013 r. poz. 628, 675, 1351 i 1635 oraz z 2014 r. poz. 24. Tekst jednolity nie uwzględnia zmian ogłoszonych w Dz. U. z 2011 r. Nr 217, poz. 1280 i Nr 230, poz. 1371.

10) PR KGP – zlokalizowany w Komendzie Głównej Policji punkt rejestracji realizujący czynności związane z aktywacją, dezaktywacją, recertyfikacją i odblokowaniem KM lub KSD - dla użytkowników pełniących służbę lub zatrudnionych w Komendzie Głównej Policji, Centralnym Laboratorium Kryminalistycznym Policji, Wyższej Szkole Policji w Szczytnie oraz szkołach policyjnych;

11) dezaktywacja – umieszczenie w bazie danych BTUU informacji o unieważnieniu certyfikatów z KM lub KSD;

12) identyfikator kadrowy – indywidualny numer identyfikacyjny nadany policjantowi lub pracownikowi Policji przez komórkę organizacyjną Policji właściwą do spraw kadrowych;

13) inspektor ds. rejestracji – osobę upoważnioną do wykonywania w PR KGP lub PR czynności polegających na aktywacji, dezaktywacji, recertyfikacji i odblokowaniu KM lub KSD;

14) kod PIN – przydzielony użytkownikowi kod, przypisany do karty mikroprocesorowej;

15) odblokowanie – odblokowanie kodu PIN przypisanego do karty mikroprocesorowej;

16) recertyfikacja – wygenerowanie na KM lub KSD certyfikatu na kolejny okres ważności;

17) użytkownik – funkcjonariusza lub pracownika Policji autoryzowanego do przetwarzania danych w systemach teleinformatycznych Policji z wykorzystaniem KM lub KSD albo inną osobę uprawnioną w tym zakresie na podstawie odrębnych przepisów;

18) zablokowanie – automatyczne zablokowanie karty mikroprocesorowej, po trzykrotnym, błędnym wprowadzeniu kodu PIN.

§ 3. Nadzór nad funkcjonowaniem BTUU sprawują:

1) administrator centralny – w Komendzie Głównej Policji;

2) administratorzy lokalni – w komendach wojewódzkich (Stołecznej) Policji.

§ 4. 1. Aktywacji KM i KSD dokonuje inspektor ds. rejestracji, poprzez zapisanie w BTUU i pamięci KM lub KSD danych niezbędnych do bezpiecznego logowania w jawnych systemach teleinformatycznych Policji – na podstawie wniosku:

1) kierownika właściwej komórki organizacyjnej – w przypadku wniosków dotyczących policjantów lub pracowników Policji pełniących służbę lub zatrudnionych w Komendzie Głównej Policji, komendach wojewódzkich (Stołecznej) Policji, Centralnym Laboratorium Kryminalistycznym Policji, Wyższej Szkole Policji w Szczytnie oraz szkołach policyjnych;

2) kierownika właściwej jednostki organizacyjnej Policji – w przypadku wniosków dotyczących policjantów lub pracowników Policji pełniących służbę lub zatrudnionych w komendach powiatowych (miejskich, rejonowych) Policji, komisariatach Policji i komisariatach specjalistycznych Policji.

2. Wniosek o aktywację KM lub KSD sporządza się w dwóch, jednobrzmiących egzemplarzach, według wzoru określonego w załączniku nr 1 do zarządzenia w przypadku aktywacji KM lub według wzoru określonego w załączniku nr 2 do zarządzenia w przypadku aktywacji KSD, a następnie przekazuje do zatwierdzenia przez:

1) kierownika komórki organizacyjnej Biura Łączności i Informatyki Komendy Głównej Policji spełniającej funkcje PR KGP – w przypadku użytkowników pełniących służbę lub zatrudnionych w Komendzie Głównej Policji, Centralnym Laboratorium Kryminalistycznym Policji, Wyższej Szkole Policji w Szczytnie oraz w szkołach policyjnych;

2) właściwego administratora lokalnego – w przypadku pozostałych użytkowników.

3. Kierownik lub administrator lokalny, o których mowa w ust. 2, przekazuje wniosek o aktywację do PR lub PR KGP w celu realizacji.

§ 5. 1. Po aktywacji KM lub KSD, jeden egzemplarz odpowiednio uzupełnionego wniosku o aktywację przekazuje się zwrotnie kierownikowi komórki organizacyjnej, w której pełni służbę lub jest zatrudniony użytkownik KM lub KSD, wraz z kartą oraz kodem PIN, umieszczonym w oddzielnej kopercie zamkniętej w sposób uniemożliwiający odczytanie kodu przez osobę nieuprawnioną. Drugi egzemplarz wniosku o aktywację przechowuje się we właściwym PR lub KGP.

2. KM oraz kod PIN są przekazywane użytkownikowi przez kierownika komórki organizacyjnej, w której użytkownik pełni służbę lub jest zatrudniony.

3. Użytkownik potwierdza na wniosku o aktywację własnoręcznym podpisem odebranie karty KM wraz z kodem PIN.

4. KSD instaluje się w mobilnym terminalu noszonym pozostającym na stanie ewidencyjnym komórki organizacyjnej, o której mowa w ust. 1. Kody PIN do KSD są przekazywane użytkownikom mobilnych terminali noszonych przez kierowników komórek organizacyjnych, w których użytkownicy pełnią służbę lub są zatrudnieni. Odbiór kodu PIN użytkownik potwierdza własnoręcznym podpisem na wniosku o aktywację.

5. Egzemplarz wniosku o aktywację z potwierdzeniem odbioru karty KM wraz z kodem PIN lub kodu PIN do karty KSD jest przechowywany w komórce organizacyjnej, w której pełni służbę lub jest zatrudniony użytkownik KM lub KSD.

6. W komórkach organizacyjnych, w których pełnią służbę lub są zatrudnieni użytkownicy KM lub KSD, prowadzi się ewidencję otrzymanych KM i KSD.

§ 6. 1. Do recertyfikacji stosuje się odpowiednio § 4 i 5.

2. Do wniosku o recertyfikację należy dołączyć podlegającą recertyfikacji KM lub KSD.

3. Wniosek o recertyfikację należy przesłać do właściwego PR lub PR KGP nie później niż 30 dni przed terminem wygaśnięcia ważności certyfikatu.

§ 7. 1. KM lub KSD podlegają dezaktywacji w przypadku:

1) zmiany danych osobowych użytkownika;

2) zwolnienia ze służby użytkownika lub rozwiązania albo wygaśnięcia stosunku pracy użytkownika;

3) przeniesienia użytkownika do pełnienia służby lub świadczenia pracy w innej komórce lub jednostce organizacyjnej Policji;

4) zmiany zakresu obowiązków, polegającej na zaprzestaniu wykonywania zadań wymagających dostępu do informacji jawnych przetwarzanych w systemach teleinformatycznych Policji;

5) podjęcia decyzji o dezaktywacji przez kierownika komórki organizacyjnej, w której pełni służbę lub jest zatrudniony użytkownik karty KM lub KSD;

6) utraty lub uszkodzenia KM lub KSD w stopniu, uniemożliwiającym dalsze użytkowanie;

7) likwidacji jednostki lub komórki organizacyjnej Policji, w której użytkownik pełni służbę lub jest zatrudniony.

2. W przypadku dezaktywacji z powodu utraty KM lub KSD stosuje się odpowiednio § 4 i 8 - z tym, że wniosek o dezaktywację sporządza się w jednym egzemplarzu.

3. Wnioski o dezaktywację są przechowywane we właściwym PR lub PR KGP.

§ 8. 1. W przypadku utraty aktywowanej KM lub KSD użytkownik:

1) pełniący służbę lub zatrudniony w Komendzie Głównej Policji, Wyższej Szkole Policji w Szczytnie i w szkole policyjnej – jest obowiązany niezwłocznie powiadomić o utracie dyżurnego Sekcji do Spraw Obsługi Całodobowej Wydziału Utrzymania Systemów Informatycznych Biura Łączności i Informatyki Komendy Głównej Policji, poprzez przesłanie faksem wniosku o zablokowanie uprawnień użytkownika (użytkowników) w trybie awaryjnym, sporządzonego według wzoru określonego w załączniku nr 3 do zarządzenia;

2) inny niż wymieniony w pkt 1 – jest obowiązany niezwłocznie powiadomić o utracie dyżurnego właściwej terytorialnie jednostki organizacyjnej Policji.

2. Dyżurny, o którym mowa w ust. 1 pkt 2, jest obowiązany niezwłocznie sporządzić wniosek o zablokowanie uprawnień użytkownika (użytkowników) w trybie awaryjnym, według wzoru określonego w załączniku nr 3 do zarządzenia.

3. Wniosek, o którym mowa w ust. 2, przekazuje się:

1) w dni wolne od pracy (służby) oraz w dni robocze poza obowiązującym w danej jednostce organizacyjnej, czasie służby lub pracy – dyżurnemu Sekcji do Spraw Obsługi Całodobowej Wydziału Utrzymania Systemów Informatycznych Biura Łączności i Informatyki Komendy Głównej Policji – faksem na numer w policyjnej sieci telekomunikacyjnej 72 159 02 lub pocztą elektroniczną na adres „technologia@policja.gov.pl”;

2) w dni robocze w obowiązującym w danej jednostce organizacyjnej, czasie służby lub pracy – kierownikowi właściwej terytorialnie komórki organizacyjnej komendy wojewódzkiej (Stołecznej) Policji do spraw łączności i informatyki.

4. Dyżurny lub kierownik, o których mowa w ust. 1 pkt 1 oraz ust. 3, na podstawie otrzymanego wniosku o zablokowanie uprawnień, niezwłocznie podejmuje czynności powodujące zablokowanie uprawnień w trybie awaryjnym i przekazuje informację o zablokowaniu operatorowi właściwego terytorialnie PR lub PR KGP, w celu unieważnienia certyfikatu użytkownika utraconej karty KM lub KSD.

5. Czynności określone w ust. 4 mogą być wykonywane przez pełniących całodobowe dyżury dyżurnych komórek organizacyjnych Policji właściwych do spraw informatyki i łączności, do których należy kierować wnioski o zablokowanie uprawnień.

6. Użytkownik utraconej karty KM lub KSD, powiadamia o utracie karty również bezpośredniego przełożonego, notatką służbową opisującą okoliczności zdarzenia.

§ 9. 1. W przypadku trzykrotnego, wprowadzenia błędnego kodu PIN karta KM lub KSD jest automatycznie blokowana.

2. W przypadku określonym w ust. 1 odblokowanie karty KM lub KSD następuje na podstawie wniosku o odblokowanie, sporządzonego według wzoru określonego odpowiednio w załączniku nr 1 lub 2 do zarządzenia.

3. Do wniosku o odblokowanie karty KM lub KSD, należy dołączyć zablokowaną kartę KM lub KSD.

§ 10. 1. Użytkownik jest obowiązany do:

1) wykorzystywania KM lub KSD wyłącznie do realizacji zadań służbowych;

2) użytkowania i przechowywania KM lub KSD w sposób uniemożliwiający wykorzystanie przez osobę nieuprawnioną;

3) nieujawniania kodu PIN;

4) ochrony KM lub KSD przed zniszczeniem lub utratą;

5) niezwłocznego zwrotu KM lub KSD:

a) uszkodzonej,

b) uprzednio utraconej a następnie odnalezionej,

c) w przypadkach określonych w § 7 ust. 1 pkt 1-5 i 7.

2. W przypadkach, o których mowa w ust. 1 pkt 5, karta KM lub KSD powinna być zwrócona kierownikowi komórki organizacyjnej, w której pełni służbę lub jest zatrudniony użytkownik karty, a następnie przesłana kierownikowi komórki organizacyjnej Biura Łączności i Informatyki Komendy Głównej Policji spełniającej funkcje PR KGP lub właściwemu administratorowi lokalnemu. Zwrócone i nieuszkodzone KM lub KSD mogą być ponownie aktywowane.

3. Kierownik lub administrator, o których mowa w ust. 2, jest obowiązany spowodować fizyczne zniszczenie uszkodzonych KM lub KSD, co powinno być udokumentowane protokołem zniszczenia wskazującym rodzaje i numery seryjne zniszczonych kart.

§ 11. Komenda Główna Policji oraz komendy wojewódzkie (Stołeczna) Policji, każda we własnym zakresie, organizują przechowywanie nieaktywnych KM i KSD.

§ 12. Karty KSIM dotychczas użytkowane na podstawie zarządzenia wymienionego w § 13 należy przekazać do właściwych PR lub PR KGP w celu ich fizycznego zniszczenia. Zniszczenie kart KSIM inspektor ds. rejestracji potwierdza protokołem zniszczenia.

§ 13. Traci moc zarządzenie nr 645 Komendanta Głównego Policji z dnia 5 czerwca 2009 r. w sprawie metod i form wykonywania zadań w zakresie przydzielania oraz postępowania z identyfikatorami umożliwiającymi dostęp do części jawnej centralnych systemów teleinformatycznych Policji (Dz. Urz. KGP z 2013 r. poz. 72).

§ 14. Zarządzenie wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

Komendant Główny Policji

nadinsp. Marek DZIAŁOSZYŃSKI

Załączniki do zarządzenia nr 5
Komendanta Głównego Policji
z dnia 29 stycznia 2014 r.

Załącznik nr 1

ZATWIERDZAM

Ldz. .....

.....
(miejscowość, data)

Egz. Nr .....

Adresat:
.....
.....

Nadawca:
.....
.....

Wniosek o aktywację/dezaktywację/recertyfikację/odblokowanie[1] karty mikroprocesorowej KM

Lp	Imię i nazwisko użytkownika – F/P/I[2]	Rodzaj czynności do wykonania[3]	Numer KM[4]	Identyfikacyjny numer kadrowy użytkownika / Numer PESEL użytkownika	Nazwa jednostki organizacyjnej
1					
2					

Załączniki:[5]
.....

Uzasadnienie:
.....
.....

.....
(pieczęć i podpis kierownika jednostki lub komórki organizacyjnej)

Uwagi:
.....
.....

Data realizacji	Imię, nazwisko i podpis osoby realizującej wniosek

Potwierdzam odbiór KM wraz z kodem PIN.

Jednocześnie oświadczam, że zapoznałem/am[1] się z treścią zarządzenia nr ..... Komendanta Głównego Policji z dnia .....2014 r. w sprawie form uwierzytelniania użytkowników systemów teleinformatycznych Policji przeznaczonych do przetwarzania informacji jawnych

Nr KM	Imię, nazwisko i podpis wydającego	Data odbioru i czytelny podpis użytkownika

[1] Niepotrzebne skreślić.
[2] Po myślniku wstawić: „F" – w przypadku funkcjonariusza lub „P" – w przypadku pracownika lub „I" – w przypadku innej uprawnionej osoby.
[3] Wstawić: A – w przypadku aktywacji, D – w przypadku dezaktywacji, R – w przypadku recertyfikacji, O – w przypadku odblokowania.
[4] W przypadku aktywacji KM rubrykę wypełnia inspektor ds. rejestracji, w pozostałych przypadkach - podmiot wnioskujący.
[5] Numery kart KM.

Załącznik nr 2

ZATWIERDZAM

.....
(miejscowość, data)
Egz. Nr .....

L.dz. .....

Adresat:
.....

Nadawca:
.....

Wniosek o aktywację/dezaktywację/recertyfikację/odblokowanie[1] karty mikroprocesorowej KSD

Lp	KSD Nr[2]	Kontener[3]	Rodzaj czynności do wykonania[4]	Imię i nazwisko użytkownika – F/P/I[5]	Identyfikacyjny numer kadrowy użytkownika / Numer PESEL użytkownika	Nazwa jednostki organizacyjnej
1						
2						
3						
4						
5						
6						
7						
8						

Załączniki:[6] .....

Uzasadnienie:

.....

.....
(pieczęć i podpis kierownika jednostki lub komórki organizacyjnej Policji)

Uwagi: .....

Data realizacji	Imię i nazwisko osoby realizującej wniosek

Potwierdzam odbiór KSD wraz z kodem PIN.

Jednocześnie oświadczam, że zapoznałem/am[1] się z treścią zarządzenia nr ..... Komendanta Głównego Policji z dnia .....2014 r. w sprawie form uwierzytelniania użytkowników systemów teleinformatycznych Policji przeznaczonych do przetwarzania informacji jawnych

Imię, nazwisko i podpis wydającego oraz numer KSD	Data odbioru i czytelny podpis pobierającego użytkownika

---

1 Niepotrzebne skreślić.

2 W przypadku aktywacji KSD rubrykę wypełnia inspektor ds. rejestracji, w pozostałych przypadkach – podmiot wnioskujący.

3 F1 do F8.

4 Wstawić: A - w przypadku aktywacji, D - w przypadku dezaktywacji, R - w przypadku recertyfikacji, O - w przypadku odblokowania.

5 Po myślniku wstawić: "F" - w przypadku funkcjonariusza, "P" - w przypadku pracownika lub "I" - w przypadku innej uprawnionej osoby.

6 Numery aktywowanej karty KSD

Załącznik nr 3

.....
(miejscowość, data)

Sekcja do Spraw Obsługi Całodobowej
Wydziału Utrzymania Systemów Informatycznych
Biura Łączności i Informatyki Komendy Głównej Policji/[1]
Kierownik właściwej do spraw łączności i informatyki komórki organizacyjnej
Komendy Wojewódzkiej/Stołecznej/[1] Policji w
..... /[1]

Wniosek
o zablokowanie uprawnień użytkowników karty mikroprocesorowej KM/KSD[1] w trybie awaryjnym

Lp.	Imię i nazwisko użytkownika	Identyfikacyjny numer kadrowy użytkownika Numer PESEL użytkownika
1		
2		
3		
4		
5		
6		
7		
8		

.....
(Imię, nazwisko i podpis zgłaszającego dyżurnego właściwej terytorialnie jednostki organizacyjnej Policji lub użytkownika)

Uwagi:
.....
.....
.....

[1] – niepotrzebne skreślić