DZIENNIK USTAW
RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 6 października 2016 r.

Poz. 1627

ROZPORZĄDZENIE
MINISTRA CYFRYZACJI[1)]

z dnia 5 października 2016 r.

w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników

Na podstawie art. 20a ust. 3 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352 i 1579) zarządza się, co następuje:

§ 1. Rozporządzenie określa szczegółowe warunki organizacyjne i techniczne, które powinien spełniać system teleinformatyczny służący do wydania certyfikatu oraz stosowania technologii, o których mowa w art. 20a ust. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, w tym zakres i okres przechowywania danych w systemie oraz obowiązki informacyjne, do których zobowiązany jest administrator systemu.

§ 2. 1. System certyfikujący służący do wydawania i unieważniania certyfikatów wykorzystywanych przez podmioty publiczne do uwierzytelniania użytkowników:

1) umożliwia wystawienie certyfikatu oraz jego wydanie użytkownikowi, dla którego został on wystawiony;
2) umożliwia niezwłoczne unieważnienie certyfikatu;
3) precyzyjnie określa czas wystawienia i unieważnienia certyfikatu, zgodnie z urzędowym czasem określonym w przepisach wydanych na podstawie art. 4 ust. 2 ustawy z dnia 10 grudnia 2003 r. o czasie urzędowym na obszarze Rzeczypospolitej Polskiej (Dz. U. z 2004 r. poz. 144);
4) potwierdza tożsamość osoby, dla której jest wydawany certyfikat;
5) spełnia wymagania w zakresie bezpieczeństwa teleinformatycznego, dobierane na podstawie analizy ryzyka;
6) nie gromadzi ani nie kopiuje danych służących użytkownikom do potwierdzania tożsamości z wykorzystaniem certyfikatów.

2. System certyfikujący przechowuje dane dotyczące wydanych certyfikatów przez okres 20 lat, licząc od dnia 1 stycznia roku następującego po roku, w którym certyfikat został wystawiony.

3. Bieżące zapewnienie poprawności i użyteczności funkcjonalnej systemu certyfikującego wymaga:

1) systematycznego przeglądu skuteczności zastosowanych środków w zakresie bezpieczeństwa teleinformatycznego, w celu wprowadzania ich usprawnień;
2) utrzymywania w stanie aktualnym dokumentacji operacyjnej i technicznej systemu, zapewniającej jego bezpieczną eksploatację;
3) zapewniania organizacyjnego, technicznego i kryptograficznego bezpieczeństwa działania systemu;
4) prowadzenia działań zapobiegających fałszowaniu certyfikatów, w tym zapewniania poufności podczas procesu tworzenia danych do potwierdzania tożsamości;
5) zapewniania osobom ubiegającym się o certyfikat dostępu do informacji o warunkach stosowania certyfikatu.

[1)] Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 1910 i 2090).

4. Warunki określone w ust. 1–3 uważa się za spełnione, gdy:

1) została wdrożona polityka certyfikacji spełniająca wymagania wskazane w standardzie ETSI TS 102 042;
2) zapewnione zostały warunki organizacyjne i techniczne zgodne z wymaganiami standardu CWA 14167-1 lub nowszego w zakresie świadczenia usług innych niż wydawanie certyfikatów kwalifikowanych;
3) zastosowane zostały systemy i produkty zgodne z wymaganiami standardu CWA 14167-2, 3 i 4 lub nowszego.

5. Administrator systemu certyfikującego udostępnia deklarację o spełnieniu wymagań określonych w ust. 3 oraz politykę certyfikacji:

1) w Biuletynie Informacji Publicznej albo
2) na stronie internetowej podmiotu – w przypadku podmiotów niezobowiązanych przez przepisy prawa do prowadzenia Biuletynu Informacji Publicznej.

§ 3. 1. System zarządzania tożsamością przetwarzający dane dotyczące tożsamości użytkowników wykorzystywany przez podmioty publiczne do uwierzytelniania użytkowników w oparciu o inne metody niż certyfikat:

1) rejestruje użytkowników;
2) potwierdza tożsamość użytkowników;
3) przechowuje i udostępnia dane identyfikacyjne użytkowników systemom autoryzującym uprawnionym do ich otrzymania;
4) umożliwia zablokowanie konta użytkownika na jego żądanie;
5) zapewnia rozliczalność, rozumianą jako przypisanie określonego działania w systemie do osoby fizycznej lub procesu oraz umiejscowienie ich w czasie;
6) zapewnia integralność, autentyczność i poufność danych identyfikacyjnych i uwierzytelniających użytkownika;
7) zapewnia codzienną synchronizację czasu systemowego z czasem UTC(PL).

2. System zarządzania tożsamością przechowuje dane dotyczące tożsamości użytkownika przez okres 20 lat, licząc od dnia 1 stycznia roku następującego po roku, w którym wykonano w systemie ostatnią operację z użyciem tożsamości.

3. Administrowanie systemem zarządzania tożsamością wymaga:

1) zapewniania wiarygodności procesu rejestracji użytkowników i potwierdzania ich tożsamości;
2) utrzymywania w stanie aktualnym dokumentacji operacyjnej i technicznej systemu, zapewniającej jego bezpieczną eksploatację;
3) opracowania i ustanawiania, wdrażania i eksploatowania, monitorowania i przeglądania oraz utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zgodnie z wymogami określonymi w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

4. Warunki określone w ust. 2 i 3 uważa się za spełnione, jeśli system zarządzania bezpieczeństwem informacji został zweryfikowany pozytywnie przez jednostkę certyfikującą akredytowaną, zgodnie z ustawą z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. poz. 542, 1228 i 1579).

§ 4. 1. System autoryzujący, uwierzytelniając użytkowników, dokonuje weryfikacji tożsamości użytkowników, wykorzystując usługi systemu certyfikującego lub systemu zarządzania tożsamością, oraz przechowuje dane potwierdzające tę weryfikację.

2. Dane potwierdzające weryfikację, o których mowa w ust. 1, powinny w sposób jednoznaczny umożliwiać:

1) ustalenie tożsamości osoby, która dokonała czynności w postaci elektronicznej;
2) stwierdzenie ważności uprawnień w momencie dokonania czynności;
3) ustalenie czasu dokonania czynności.

§ 5. Rozporządzenie wchodzi w życie z dniem 7 października 2016 r.[2)]

Minister Cyfryzacji: *A. Streżyńska*

[2)] Niniejsze rozporządzenie było poprzedzone rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 21 kwietnia 2011 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do identyfikacji użytkowników (Dz. U. poz. 545), które traci moc z dniem 7 października 2016 r. na podstawie art. 142 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579).