545

ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI[1)]

z dnia 21 kwietnia 2011 r.

w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do identyfikacji 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. Nr 64, poz. 565, z późn. zm.[2)]) zarządza się, co następuje:

§ 1. Rozporządzenie określa szczegółowe warunki organizacyjne i techniczne, które powinien spełniać system teleinformatyczny służący do wydania certyfikatów oraz stosowania technologii, o których mowa w art. 20a ust. 1 i 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, zwanej dalej „ustawą".

§ 2. Użyte w rozporządzeniu określenia oznaczają:

1) usługi certyfikacyjne — usługi certyfikacyjne w rozumieniu art. 3 pkt 13 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z późn. zm.[3)]);

2) system certyfikujący — system teleinformatyczny służący do świadczenia usług certyfikacyjnych wykorzystywanych przez podmioty publiczne do identyfikacji użytkowników;

3) kwalifikowany certyfikat — kwalifikowany certyfikat w rozumieniu art. 3 pkt 12 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym;

4) system zarządzania tożsamością — system teleinformatyczny, nieświadczący usług certyfikacyjnych, przetwarzający informacje o tożsamości użytkowników i wykorzystywany przez podmioty publiczne do identyfikacji użytkowników;

5) system autoryzujący — system teleinformatyczny używany przez podmiot publiczny, który wykorzystuje usługi systemu certyfikującego lub systemu zarządzania tożsamością do przeprowadzenia procesu identyfikacji użytkownika;

6) rozliczalność — właściwość systemu pozwalającą przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie.

§ 3. Wydanie kwalifikowanego certyfikatu mającego zastosowanie do identyfikacji użytkownika systemów teleinformatycznych udostępnianych przez podmioty realizujące zadania publiczne następuje przy zachowaniu zasad określonych w przepisach wydanych na podstawie ustawy z dnia 18 września 2001 r. o podpisie elektronicznym.

§ 4. 1. System certyfikujący posiada następujące właściwości:

1) świadczy usługi niezwłocznego unieważnienia certyfikatu;

2) 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. Nr 16, poz. 144);

3) potwierdza tożsamość osoby, dla której jest wydawany certyfikat;

4) spełnia wymagania w zakresie bezpieczeństwa teleinformatycznego, dobierane na podstawie analizy ryzyka;

5) nie gromadzi ani nie kopiuje danych służących do składania podpisu elektronicznego.

2. Administrowanie systemem certyfikującym wymaga realizowania następujących czynności:

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) przeciwdziałania fałszowaniu certyfikatów, w tym zapewniania poufności podczas procesu tworzenia danych do składania podpisu elektronicznego;

5) przechowywania informacji dotyczących wydanych certyfikatów prz ez okres 20 lat, licząc od dnia 1 stycznia roku następnego po ich wytworzeniu;

6) informowania osób ubiegających się o certyfikat o warunkach stosowania certyfikatu, w szczególności o ograniczeniach użycia certyfikatu i postępowaniu w przypadku skarg i rozstrzygania sporów.

[1)] Minister Spraw Wewnętrznych i Administracji kieruje działem administracji rządowej — informatyzacja, na podstawie § 1 ust. 2 pkt 2 rozporządzenia Prezesa Rady Ministrów z dnia 16 listopada 2007 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych i Administracji (Dz. U. Nr 216, poz. 1604).

[2)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 12, poz. 65 i Nr 73, poz. 501, z 2008 r. Nr 127, poz. 817, z 2009 r. Nr 157, poz. 1241 oraz z 2010 r. Nr 40, poz. 230, Nr 167, poz. 1131 i Nr 182, poz. 1228.

[3)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 153, poz. 1271, z 2003 r. Nr 124, poz. 1152 i Nr 217, poz. 2125, z 2004 r. Nr 96, poz. 959, z 2005 r. Nr 64, poz. 565, z 2006 r. Nr 145, poz. 1050, z 2009 r. Nr 18, poz. 97 oraz z 2010 r. Nr 40, poz. 230 i Nr 182, poz. 1228.

3. Wymagania określone w ust. 1 i 2 uważa się za spełnione, gdy:

1) została wdrożona polityka certyfikacji spełniająca wymagania wskazane w standardzie ETSI TS 102 042 w wersji 1.2.4 lub nowszym;

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.

4. Politykę certyfikacji oraz deklarację o spełnieniu wymagań określonych w ust. 3 udostępnia się:

1) w Biuletynie Informacji Publicznej — zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198, z późn. zm.[4)]) albo

2) na stronie internetowej podmiotu — w przypadku gdy przepisów ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej nie stosuje się.

§ 5. 1. System zarządzania tożsamością posiada następujące właściwości:

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;

6) zapewnia integralność, autentyczność i poufność danych identyfikacyjnych i uwierzytelniających użytkownika;

7) zapewnia codzienną synchronizację czasu systemowego z czasem UTC(PL).

2. Administrowanie systemem zarządzania tożsamością wymaga realizowania następujących czynności:

1) zapewniania wiarygodności procesu rejestracji użytkowników i potwierdzania ich tożsamości;

2) przechowywania informacji dotyczących tożsamości użytkownika przez okres 20 lat, licząc od dnia 1 stycznia roku następnego od chwili wykonania w systemie ostatniej operacji z użyciem tożsamości;

3) utrzymywania w stanie aktualnym dokumentacji operacyjnej i technicznej systemu, zapewniającej jego bezpieczną eksploatację;

4) opracowania i wdrożenia polityki zarządzania bezpieczeństwem informacji.

3. Wymagania określone w ust. 2 uważa się za spełnione, jeśli dla systemu zarządzania tożsamością została opracowana i wdrożona polityka zarządzania bezpieczeństwem informacji, w której określono wymagania bezpieczeństwa zgodne z Polską Normą PN ISO/IEC 27001:2007 lub nowszą, zweryfikowaną pozytywnie przez jednostkę certyfikującą akredytowaną, zgodnie z ustawą z dnia 30 sierpnia 2002 r. o systemie oceny zgodności (Dz. U. z 2010 r. Nr 138, poz. 935).

§ 6. 1. System autoryzujący, identyfikując użytkownika z wykorzystaniem systemu certyfikującego, dokonuje weryfikacji podpisu elektronicznego i przechowuje dane potwierdzające tę weryfikację.

2. System autoryzujący, identyfikując użytkownika z wykorzystaniem systemu zarządzania tożsamością, dokonuje weryfikacji danych otrzymanych z tego systemu i przechowuje dane potwierdzające tę weryfikację.

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

1) identyfikację tożsamości osoby, która dokonała czynności w postaci elektronicznej;

2) stwierdzenie ważności uprawnień w momencie dokonania czynności;

3) ustalenie czasu dokonania czynności.

§ 7. Rozporządzenie wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

Minister Spraw Wewnętrznych i Administracji:
J. Miller

[4)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 153, poz. 1271, z 2004 r. Nr 240, poz. 2407, z 2005 r. Nr 64, poz. 565 i Nr 132, poz. 1110 oraz z 2010 r. Nr 182, poz. 1228.