Projekt z dnia 17 czerwca 2010 r.

ROZPORZĄDZENIE
MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI[1])

z dnia ..... 2010 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. z 2005 r. Nr 64, poz. 565 z późn. zm.[2]) zarządza się, co następuje:

§ 1.

Rozporządzenie określa szczegółowe warunki organizacyjne i techniczne, które winien 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", o ile nie dotyczy to wydawania kwalifikowanych certyfikatów.

§ 2.

Użyte w rozporządzeniu określenia oznaczają:

1) usługi certyfikacyjne – usługi certyfikacyjne określone w ustawie z dnia 18 września 2001 o podpisie elektronicznym (Dz.U. Nr 130, poz. 1450, z późn.zm.[3]);
2) system certyfikacyjny – system teleinformatyczny realizujący zadania określone w art. 20a ustawy służący do świadczenia usług certyfikacyjnych wykorzystywanych przez podmioty publiczne;

[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.

[3] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 153, poz. 1271, z 2003 r. Nr 124, poz. 1452 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 oraz z 2009 r. Nr 18, poz. 97.

3) kwalifikowany certyfikat – kwalifikowany certyfikat w rozumieniu ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. Nr 130, poz. 1450, z późn.zm.[4]);
4) system zarządzania tożsamością – system teleinformatyczny przetwarzający informacje o tożsamości użytkowników, realizujący zadania określone art. 20a ustawy, niepolegające na świadczeniu usług certyfikacyjnych.
5) system autoryzujący – system teleinformatyczny, który wykorzystuje do przeprowadzenia procesu identyfikacji certyfikaty, (w tym kwalifikowane certyfikaty), profil zaufany ePUAP lub inne technologie określone art. 20a ust. 2 ustawy;
6) rozliczalność – właściwość systemu pozwalająca przypisać określone działanie w systemie do konkretnej osoby fizycznej lub procesu, który wykonuje się automatycznie oraz umiejscowić je w czasie.

§ 3.

1. System certyfikacyjny posiada następujące właściwości:
1) świadczy usługi natychmiastowego unieważnienia certyfikatu;
2) precyzyjnie określa czas wystawienia lub 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.

2. Administrowanie systemem certyfikacyjnym wymaga realizowania następujących czynności:
1) systematycznego przeglądu skuteczności zastosowanych zabezpieczeń, o których mowa w ust. 1 pkt 4, w celu wprowadzania ich usprawnień;
2) utrzymywania w stanie aktualnym dokumentacji operacyjnej i technicznej systemu, zapewniającej jego bezpieczną eksploatację;

[4] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 153, poz. 1271, z 2003 r. Nr 124, poz. 1452 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).

3) zapewniania organizacyjnego, technicznego i kryptograficznego bezpieczeństwa działania systemu;
4) przeciwdziałania fałszowaniu certyfikatów, w tym zapewniania poufności podczas procesu tworzenia danych do składania podpisu;
5) przechowywania przez okres 20 lat informacji dotyczących wydanych certyfikatów, 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.

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 nowszej,
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.[5]),
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.

§ 4.

1. System zarządzania tożsamością posiada następujące właściwości:
1) rejestruje użytkowników;
2) potwierdza tożsamość użytkowników;
3) przechowuje i udostępniania dane identyfikacyjne użytkowników systemom autoryzującym uprawnionym do ich otrzymania;
4) umożliwia zablokowanie konta użytkownika na jego żądanie;

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

5) jednoznacznie identyfikuje wszystkie operacje realizowane w systemie oraz czas ich wykonania;
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 stwierdzania ich tożsamości;
2) przechowywania przez okres 20 lat informacji dotyczących tożsamości użytkownika, 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 2004 r. Nr 204, poz. 2087, z późn. zm.[6]).

§ 5.

1. System autoryzujący wykorzystując usługi identyfikacyjne systemu certyfikacyjnego dokonuje weryfikacji podpisu elektronicznego i przechowuje dane potwierdzające tę weryfikację.

2. System autoryzujący wykorzystując usługi identyfikacyjne 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,

[6]Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2005 r. Nr 64, poz. 565 i Nr 267, poz. 2258, z 2006 r. Nr 170, poz. 1217, Nr 249, poz. 1832, Nr 235, poz. 1700 i Nr 249, poz. 1834, z 2007 r. Nr 21, poz. 124 i Nr 192, poz. 1381, z 2008 r. Nr 157, poz. 976 i Nr 227, poz. 1505 oraz z 2009 r. Nr 18, poz. 97.

2) stwierdzenie ważności uprawnień w momencie dokonania czynności,
3) ustalenie czasu dokonania czynności.

§ 6

Rozporządzenie wchodzi w życie po upływie 3 miesięcy od dnia ogłoszenia.

MINISTER SPRAW WEWNĘTRZNYCH
I ADMINISTRACJI

Uzasadnienie

Projektowane rozporządzenie wykonuje upoważnienie ustawowe zawarte w art. 20a ust. 3 pkt 1 nowelizowanej ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565, z późn.zm.).

Rozporządzenie określa szczegółowe warunki organizacyjne i techniczne, które winien 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. Z przepisów tych wynika, że możliwe są następujące sposoby identyfikacji użytkowników w systemach teleinformatycznych udostępnianych przez podmioty publiczne:

- kwalifikowane certyfikaty,
- profil zaufany ePUAP,
- inne metody identyfikacji (w tym certyfikaty niekwalifikowane).

Kwestie związane z identyfikacją użytkownika na podstawie kwalifikowanego certyfikatu pozostają poza sferą regulacji niniejszego rozporządzenia, ponieważ normują to przepisy wykonawcze do ustawy z dnia 18 września 2001 r. o podpisie elektronicznym.
Rozporządzenie odnosi się zatem do:

1) Systemów teleinformatycznych do świadczenia usług certyfikacyjnych wykorzystywanych przez podmioty publiczne - tzw. systemów certyfikacyjnych, które zdefiniowano w §2 pkt 2.
2) Systemów teleinformatycznych przetwarzających informacje o tożsamości użytkowników niepolegające na świadczeniu usług certyfikacyjnych - tzw. systemów zarządzania tożsamością, które zdefiniowano w §2 pkt 3.

W związku z tym, że identyfikacja tożsamości na podstawie certyfikatu różni się organizacyjnie i technologicznie od sposobów identyfikacji nieopartych o certyfikat, także istotne wymagania dotyczące wymaganych właściwości oraz zasad administrowania systemami certyfikacyjnymi i systemami zarządzania tożsamością są różne. Odpowiednio określono to dla obu rodzajów systemów w §3 ust.1 i 2 i §4 ust. 1 i 2. Dodatkowo wskazano uznane normy i standardy międzynarodowe, których zastosowanie spowoduje, że

odpowiednie wymagania dla systemów certyfikacyjnych lub systemów zarządzania tożsamością będzie uważać się za spełnione.

W związku z tym, że każdy z ww. sposobów identyfikacji będzie rodził skutki prawne w kontaktach z podmiotami określonymi w art.2 ustawy, określono (odpowiednio w §3 ust.2 pkt 5 oraz w §4 ust.2 pkt 2) wymaganie przechowywania przez okres 20 lat informacji dotyczących wydanych certyfikatów albo tożsamości użytkowników, podobnie jak wymaga tego ustawa z dnia 18 września 2001 r. o podpisie elektronicznym wobec podmiotów wydających certyfikaty kwalifikowane w art. 113 ust.2.

Dla potrzeb rozporządzenia zdefiniowano także pojęcie systemu autoryzującego, czyli systemu wykorzystującego do procesu identyfikacji dane identyfikacyjne z różnych źródeł zewnętrznych. Celem tego zabiegu było określenie w §5 wymagań dotyczących danych potwierdzających weryfikację tożsamości które, niezależnie od zastosowanej technologii (certyfikaty, profil zaufany ePUAP, inne technologie) powinny zawierać te same elementy tj.

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

Projekt rozporządzenia nie zawiera przepisów technicznych, a zatem nie podlega notyfikacji, zgodnie z trybem przewidzianym w przepisach rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz.U.Nr 239, poz. 2039 oraz z 2004 Nr 65, poz. 597).

OCENA SKUTKÓW REGULACJI

1. Podmioty, na które wpływa projekt aktu prawnego

Podmioty publiczne administrujące systemami teleinformatycznymi służącymi do wydania certyfikatów lub używającymi do realizacji zadań publicznych systemów teleinformatycznych identyfikujących użytkowników w inny sposób niż certyfikat kwalifikowany lub profil zaufany ePUAP.

2. Konsultacje społeczne

Projekt rozporządzenia został poddany konsultacjom społecznym z następującymi partnerami społecznymi:
- Polskim Towarzystwem Informatycznym (PTI),
- Polską Izbą Informatyki i Telekomunikacji (PIIT),
- Krajową Izbą Gospodarczą Elektroniki i Telekomunikacji (KIGEiT),
- Polską Konfederacją Pracodawców Prywatnych Lewiatan,
- Stowarzyszeniem Instytutu Informatyki Śledczej,
- Związkiem Pracodawców Branży Internetowej Interactive Advertising Bureau Polska.

a także
- Komisją Wspólna Rządu i Samorządu Terytorialnego,
- Generalnym Inspektorem Ochrony Danych Osobowych.

Ponadto projekt rozporządzenia został przekazany do konsultacji Prezesowi Zakładu Ubezpieczeń Społecznych i wojewodom.

3. Wpływ regulacji na sektor finansów publicznych, w tym na budżet państwa i budżety jednostek samorządu terytorialnego

Wdrożenie projektu będzie wywoływać skutki finansowe dla budżetu państwa i budżetów zainteresowanych podmiotów, związane głównie z dostosowaniem tych podmiotów do wydawania certyfikatów oraz identyfikacji użytkowników systemów teleinformatycznych za pomocą profilu zaufanego ePUAP. Koszty wdrożenia projektu są trudne do oszacowania ze względu na różną specyfikę podmiotów określonych w art. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne udostępniających systemy teleinformatyczne umożliwiające identyfikację ich użytkowników.

4. Wpływ regulacji na rynek pracy; wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw; wpływ regulacji na sytuację i rozwój regionów.

Rozporządzenie nie będzie miało wpływu na segmenty rynku i zakłócać mechanizmów konkurencji. Przedmiotu regulacji nie stanowią bowiem kwestie konkurencji, monopolizacji, prywatyzacji, itp. Regulacje nie zmieniają także istoty funkcjonowania gospodarki oraz zadań i roli przedsiębiorców.

5. Zainteresowanie pracami nad projektem

W ramach konsultacji społecznych i w celu wykonania obowiązku wynikającego z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. Nr 169, poz. 1414 oraz z 2009 r. Nr 42, poz. 337) projekt rozporządzenia został zamieszczony w Biuletynie Informacji Publicznej na stronie internetowej Ministerstwa Spraw Wewnętrznych i Administracji.

6. Zgodność z prawem Unii Europejskiej.

Proponowane regulacje nie pozostają w kolizji z przepisami obowiązującymi w Unii Europejskiej.