1768

ROZPORZĄDZENIE MINISTRA FINANSÓW[1)]

z dnia 30 grudnia 2010 r.

w sprawie sposobu przesyłania zgłoszeń oraz rodzajów podpisu elektronicznego, którymi powinny być opatrzone

Na podstawie art. 10b ust. 2 ustawy z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (Dz. U. z 2004 r. Nr 269, poz. 2681, z późn. zm.[2)]) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) sposób przesyłania zgłoszeń za pomocą środków komunikacji elektronicznej;

2) rodzaje podpisu elektronicznego, którymi powinny być opatrzone poszczególne typy zgłoszeń.

§ 2. Zgłoszenia są przesyłane za pomocą interfejsu dostępnego na stronie, której adres podany jest na stronie Biuletynu Informacji Publicznej Ministerstwa Finansów, poprzez zastosowanie protokołu wywoływania zdalnego dostępu do obiektów (SOAP), opisanego językiem opisu usług sieciowych (WSDL), dostępnego przez protokół komunikacyjny sieci WWW (HTTP), szyfrowanego przy użyciu protokołu szyfrującego dla sieci WWW (SSL).

§ 3. 1. Zgłoszenia są opatrywane bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu w rozumieniu ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z późn. zm.[3)]).

2. Sposób opatrywania zgłoszeń bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu określa załącznik do niniejszego rozporządzenia.

§ 4. Rozporządzenie wchodzi w życie z dniem 1 stycznia 2011 r.[4)]

Minister Finansów: w z. *L. Kotecki*

[1)] Minister Finansów kieruje działem administracji rządowej — finanse publiczne, na podstawie § 1 ust. 2 pkt 2 rozporządzenia Prezesa Rady Ministrów z dnia 16 listopada 2007 r. w sprawie szczegółowego zakresu działania Ministra Finansów (Dz. U. Nr 216, poz. 1592).

[2)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2005 r. Nr 14, poz. 113, z 2006 r. Nr 104, poz. 708 i 711, z 2007 r. Nr 112, poz. 769, z 2008 r. Nr 209, poz. 1318, z 2009 r. Nr 3, poz. 11, Nr 18, poz. 97 i Nr 166, poz. 1317 oraz z 2010 r. Nr 182, poz. 1228 i Nr 197, poz. 1306.

[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.

[4)] Niniejsze rozporządzenie było poprzedzone rozporządzeniem Ministra Finansów z dnia 31 grudnia 2008 r. w sprawie struktury logicznej zgłoszeń, sposobu ich przesyłania oraz rodzajów podpisu elektronicznego, którymi powinny być opatrzone (Dz. U. z 2009 r. Nr 2, poz. 10), które traci moc z dniem 1 stycznia 2011 r. na podstawie art. 6 pkt 1 ustawy z dnia 24 września 2010 r. o zmianie ustawy — Ordynacja podatkowa oraz ustawy o zasadach ewidencji i identyfikacji podatników i płatników (Dz. U. Nr 197, poz. 1306).

Załącznik do rozporządzenia Ministra Finansów
z dnia 30 grudnia 2010 r. (poz. 1768)

SPOSÓB OPATRYWANIA ZGŁOSZEŃ BEZPIECZNYM PODPISEM ELEKTRONICZNYM WERYFIKOWANYM ZA POMOCĄ WAŻNEGO KWALIFIKOWANEGO CERTYFIKATU

Przyjmuje się następujące zasady opatrywania zgłoszeń bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu:

1) Zgłoszenia opatruje się podpisem elektronicznym z wykorzystaniem jednego z formatów określonych przez:

   a) specyfikację techniczną ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES Basic Electronic Signature, w skrócie XAdES-BES) wydaną przez European Telecommunications Standards Institute, w którym do przygotowania formy kanonicznej zgłoszenia wykorzystano standardową metodę wyspecyfikowaną w standardzie XMLDSIG oraz treść podpisywanego zgłoszenia została umieszczona w elemencie ds:Object. Atrybut Id dla elementu ds:Object zawierającego zgłoszenie musi przyjmować wartość „Dokument”,

   b) dokument PKCS#7 Cryptographic Message Syntax Standard wydany przez RSA Security;

2) Algorytmem bezpiecznego podpisu elektronicznego jest Sha-1WithRSAEncryption, którego specyfikacja techniczna jest jednoznacznie określona poprzez następujący identyfikator obiektu: identyfikator iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5;

3) Algorytmem szyfrowania jest RSA, którego specyfikacja techniczna jest jednoznacznie określona poprzez następujący identyfikator obiektu: identyfikator joint-iso-ccitt(2) ds(5) module(1) algorithm(8) encryptionAlgorithm(1) 1;

4) Funkcją skrótu jest SHA-1, którego specyfikacja techniczna jest jednoznacznie określona poprzez następujący identyfikator obiektu: identyfikator iso(1) identifiedOrganization(3) oIW(14) oIWSecSig(3) oIWSecAlgorithm(2) 26;

5) Kwalifikowany certyfikat zawiera w polu identyfikatora podmiotu „subject” przynajmniej następujące atrybuty: nazwa kraju, nazwisko, imię (imiona), numer seryjny;

6) Wykorzystany zostanie certyfikat kwalifikowany;

7) Formaty, o których mowa w pkt 1, zawierają w szczególności:
   — dla pkt 1a parametry identyfikujące jednoznacznie certyfikat kwalifikowany podmiotu podpisującego (tj. nazwa wystawcy certyfikatu i jego numer seryjny oraz wartość skrótu SHA-1 z certyfikatu), który musi zostać użyty podczas weryfikacji podpisu, są umieszczone w atrybucie podpisanym, którego specyfikacja techniczna jest określona poprzez następujący znacznik: SigningCertificate oraz treść kwalifikowanego certyfikatu X.509 jest umieszczona w elemencie ds:X509Data, zawartym w elemencie KeyInfo,
   — dla pkt 1b jako podpisany atrybut, „certyfikat podpisującego”, na który składa się treść kwalifikowanego certyfikatu X.509, służącego do weryfikacji bezpiecznego podpisu elektronicznego osoby składającej zgłoszenia.