



DZIENNIK USTAW

RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 28 czerwca 2013 r.

Poz. 753

ROZPORZĄDZENIE MINISTRA FINANSÓW¹⁾

z dnia 25 czerwca 2013 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 2012 r. poz. 1314 oraz z 2013 r. poz. 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:

- 1) opisanego językiem opisu usług sieciowych (WSDL),
- 2) dostępnego na stronie, której adres podany jest na stronie podmiotowej Biuletynu Informacji Publicznej Ministerstwa Finansów,
- 3) dostępnego przez protokół komunikacyjny sieci WWW (HTTP), szyfrowanego przy użyciu protokołu szyfrującego dla sieci WWW (SSL),

z wykorzystaniem protokołu wywoływania zdalnego dostępu do obiektów (SOAP).

§ 3. Struktura logiczna urzędowego poświadczenia odbioru zgłoszenia jest udostępniona na stronie podmiotowej Biuletynu Informacji Publicznej Ministerstwa Finansów.

§ 4. 1. Zgłoszenia są opatrzone bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu w rozumieniu ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz. 262).

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

§ 5. Traci moc rozporządzenie Ministra Finansów z dnia 30 grudnia 2010 r. w sprawie sposobu przesyłania zgłoszeń oraz rodzajów podpisu elektronicznego, którymi powinny być opatrzone (Dz. U. Nr 259, poz. 1768).

§ 6. Rozporządzenie wchodzi w życie z dniem 1 lipca 2013 r.

Minister Finansów: *wz. J. Cichoń*

¹⁾ Minister Finansów kieruje działem administracji rządowej – finanse publiczne, na podstawie § 1 ust. 2 pkt 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2011 r. w sprawie szczegółowego zakresu działania Ministra Finansów (Dz. U. Nr 248, poz. 1481).

Załącznik do rozporządzenia Ministra Finansów
z dnia 25 czerwca 2013 r. (poz. 753)

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

Przyjmuje się następujący sposób 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 przez 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 przez 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 przez 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:
 - a) dla lit. a 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 przez następujący znacznik: SigningCertificate oraz treść kwalifikowanego certyfikatu X.509 jest umieszczona w elemencie ds:X509Data, zawartym w elemencie KeyInfo,
 - b) dla lit. b jako podpisany atrybut, „certyfikat podpisującego”, na który składa się treść kwalifikowanego certyfikatu X.509, służącego do weryfikacji bezpiecznego podpisu elektronicznego osoby składającej zgłoszenia.