Zmiany w zał. (Dz.U. z 2017 r. poz. 385) — zaznaczone na czerwono — weszły w życie dnia **01.03.2017 r.**

SPOSÓB OPATRYWANIA DEKLARACJI I PODAŃ KWALIFIKOWANYM PODPISEM ELEKTRONICZNYM

Przyjmuje się następujące zasady opatrywania kwalifikowanym podpisem elektroniczny:

1) Deklaracje i podania 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 deklaracji lub podania wykorzystano standardową metodę wyspecyfikowaną w standardzie XMLDSIG oraz treść podpisywanej deklaracji lub podania została umieszczona w elemencie ds:Object. Atrybut Id dla elementu ds:Object zawierającego deklarację lub podanie musi przyjmować wartość „Dokument”,
   b) dokument PKCS#7 Cryptographic Message Syntax Standard wydany przez RSA Security;
2) Algorytmem kwalifikowanego 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;

4a) Zostanie wykorzystany kwalifikowany certyfikat;

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

6) (uchylony);

7) Formaty, o których mowa w pkt 1, zawierają w szczególności:
   a) dla pkt 1 lit. a parametry identyfikujące jednoznacznie kwalifikowany certyfikat 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,
   b) dla pkt 1 lit. b jako podpisany atrybut, „certyfikat podpisującego”, na który składa się treść kwalifikowanego certyfikatu X.509, służącego do weryfikacji kwalifikowanego podpisu elektronicznego osoby składającej deklarację lub podanie.