SPOSÓB OPATRYWANIA KSIĄG KWALIFIKOWANYM PODPISEM ELEKTRONICZNYM WERYFIKOWANYM PRZY POMOCY WAŻNEGO KWALIFIKOWANEGO CERTYFIKATU

Przyjmuje się następujące zasady opatrywania kwalifikowanym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu ksiąg:

1) księgi opatruje się podpisem elektronicznym z wykorzystaniem formatu określonego przez specyfikację techniczną ETSI TS 103 171 XML Advanced Electronic Signatures (XAdES Basic Electronic Signature, w skrócie XAdES-BES) wydaną przez European Telecommunications Standards Institute, w którym do przygotowania formy kanonicznej księgi wykorzystano standardową metodę wyspecyfikowaną w standardzie XMLDSIG oraz treść podpisywanej księgi została umieszczona w elemencie ds:Object;

2) algorytmem kwalifikowanego 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) pkcs-1(1) sha1-with-rsa-signature(5);

3) algorytmem kwalifikowanego podpisu elektronicznego jest Sha256WithRSAEncryption, którego specyfikacja techniczna jest jednoznacznie określona przez następujący identyfikator obiektu: identyfikator iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11);

4) 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;

5) 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) hashAlgorithmIdentifier(26);

6) funkcją skrótu jest SHA-256, którego specyfikacja techniczna jest jednoznacznie określona przez następujący identyfikator obiektu: identyfikator joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1);

7) kwalifikowany certyfikat zawiera w polu identyfikatora podmiotu „subject" przynajmniej następujące atrybuty: nazwa kraju, nazwisko, imię (imiona) lub pseudonim, numer seryjny;

8) wykorzystany zostanie certyfikat kwalifikowany;

9) format, o którym mowa w pkt 1, zawiera w szczególności parametry identyfikujące jednoznacznie certyfikat kwalifikowany podmiotu podpisującego (nazwa wystawcy certyfikatu i jego numer seryjny oraz wartość skrótu SHA-1 lub SHA-256 z certyfikatu), którego używa się podczas weryfikacji podpisu, jest umieszczony 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.