

# Standardy techniczne podpisu elektronicznego

<http://ipsec.pl/standardy-normy/standardy-techniczne-podpisu-elektronicznego.html>

ITU-T X.509

Standard X.509 jest rozwijany przez ITU-T (dawniej CCIT) i jest podstawowym standardem definiującym format, zawartość oraz znaczenie pól w certyfikacie X.509 oraz CRL.

- <http://www.itu.int/rec/T-REC-X.509/en> X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks - strona główna standardu X.509 w ITU-T
- <http://www.itu.int/rec/T-REC-X.509/en> wersja X.509v1 opublikowana 1993 roku (dostępna za darmo)
- <http://www.itu.int/rec/T-REC-X.509/recommendation.asp?lang=en&parent=T-REC-X.509-200508-I> wersja X.509v3 opublikowana w 2005 roku (płatna)
- [erraty do X.509v3 publikowane w latach 2007 i 2008](#)
- <http://www.itu.int/rec/T-REC-X.509-200811-I/en> zatwierdzona w listopadzie 2008

PKIX

X.509 zostało także zaadaptowane przez IETF i jest rozwijane przez grupę roboczą PKIX. Główne standardy opublikowane przez tę grupę to m.in.:

- [RFC 5280](http://tools.ietf.org/html/rfc5280) - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile - opisujący certyfikaty X.509v3 i CRLv2 (odpowiada X.509v3)
- [RFC 4158](http://tools.ietf.org/html/rfc4158) - Internet X.509 Public Key Infrastructure: Certification Path Building
- [RFC 3161](http://tools.ietf.org/html/rfc3161) - Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)
- [RFC 3029](http://tools.ietf.org/html/rfc3029) - Internet X.509 Public Key Infrastructure: Data Validation and Certification Server Protocols (DVCS)
- [RFC 2560](http://tools.ietf.org/html/rfc2560) - X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol - OCSP

X.509v3 zostało także opublikowane jako:

- [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=43793](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43793) > *ISO/IEC 9594-8:2005* { *Polska Norma* <http://www.pkn.pl/?a=show&m=katalog&id=535004&page=1> > *PN-ISO/IEC 9594-8:2006* < /a > (*nabazie ISO/IEC 9594-8:2001 z poprawkami z 2002*)
- [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=39876](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39876) > *ISO/IEC 10118-3:2004* - *Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions - RIPEMD-160, RIPEMD-128, SHA-1, SHA-256, SHA-512, SHA-384, WHIRLPOOL*
- [http://csrc.nist.gov/publications/fips/fips180-3/fips180-3\\_final.pdf](http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf) > *NIST FIPS 180-3* - *Secure Hash Standard - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512*



- [RFC 3280](http://tools.ietf.org/html/rfc3280) "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" (X.509v3, 2002)
  - [RFC 3739](http://tools.ietf.org/html/rfc3739) "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile"
  - [/podpis\\_elektroniczny/ts102280v010101p.pdf](/podpis_elektroniczny/ts102280v010101p.pdf) > *ETSITS102280* "X.509V.3CertificateProfileforCertificate" </a>, *aktualnieobowiazujacyprofileuropejskiegocertyfikatakwalifikowanego, przyczynedodyskusjiot Repudiationmoznałączynymiczyinie*. {< ahref = "/podpis\_elektroniczny/cwa14365-01-2004-Mar.pdf" > *CWA14365-1March2004* "GuideontheUseofElectronicSignatures-Part1: LegalandTechnicalAspects" </a>
  - [/podpis\\_elektroniczny/cwa14169.pdf](/podpis_elektroniczny/cwa14169.pdf) > *CWA14169* "SecureSignature-CreationDevicesEAL4+" </a>, 2002, 212str., *technicznwymaganiabezpieczenstwadla"bezpiecznegourzadzeniadoskladaniapodpisu"* (Proahref = "/podpis\_elektroniczny/cwa14171-00-2004-May.pdf" > *CWA14171* "Generalguidelinesforelectronicsignature" </a>
  - [/podpis\\_elektroniczny/cwa14170-00-2004-May.pdf](/podpis_elektroniczny/cwa14170-00-2004-May.pdf) > *CWA14170* "Securityrequirementsforsignature" </a> {< ahref = "/podpis\_elektroniczny/cwa14172-04-2004-Mar.pdf" > *CWA14172-4* "EESSTConformityAssessmentGuidance-Part4: Signaturecreationapplicationsandgeneralguidelinesforelectronic" </a> < ul > < li > < ahref = "http://www.cenorm.be/cenorm/businessdomains/businessdomains/iss/cwa/electronic/signatures.asp" > *CenormCWA14167-14890* </a> *innepropozycjestandardowtechnicznych, zwlaszczaSSCD* </li>
  - [/podpis\\_elektroniczny/ts101862v131.pdf](/podpis_elektroniczny/ts101862v131.pdf) > *ETSITS101862V1.3.2* "QualifiedCertificateprofile" (2004-06) </a> {< ahref = "/podpis\_elektroniczny/tr102438v010101p.pdf" > *ETSITR102438V1.1.1* "ElectronicSignature" </a> </li>
- [/podpis\\_elektroniczny/tr102044v010101p.pdf](/podpis_elektroniczny/tr102044v010101p.pdf) > *ETSITR102044V1.1.1* "ElectronicSignaturesandInfrastructure" </a> < ul > < li > < ahref = "/podpis\_elektroniczny/tr102605v010101p.pdf" > *ETSITR102605V1.1.1* "ElectronicSignatureMail" (2007-09) </a>

[/podpis\\_elektroniczny/tr102047v010201p.pdf](/podpis_elektroniczny/tr102047v010201p.pdf) > *ETSITR102047V1.2.1* "InternationalHarmonizationofElectronic" </a> < ul > < li > < ahref = "/podpis\_elektroniczny/tr102458v010101p.pdf" > *ETSITR102458V1.1.1* "ElectronicSignatureMappingComparisonMatrixbetweentheUSFederalBridgeCACertificatePolicyandtheEuropeanQualifiedCertificate" </a> </li>

[RFC 3125](http://tools.ietf.org/html/rfc3125), "Electronic Signature Policies"

[RFC 3126](http://tools.ietf.org/html/rfc3126), "Electronic Signature Formats for long term electronic signatures" (ETSI TS 101 733 V.1.2.2)

[RFC 2560](http://tools.ietf.org/html/rfc2560) "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP"

[RFC 3029](http://tools.ietf.org/html/rfc3029) "Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols"

[Internet Draft](http://tools.ietf.org/html/draft-ietf-pkix-scvp-32) "Server-based Certificate Validation Protocol (SCVP)"

[RFC 3376](http://tools.ietf.org/html/rfc3379) "Delegated Path Validation and Delegated Path Discovery Protocol Requirements" (DPV, DPD)

[RFC 4210](http://tools.ietf.org/html/rfc4210) "Internet X.509 Public Key Infrastructure: Certificate Management Protocol (CMP)"

[RFC 3161](http://tools.ietf.org/html/rfc3161): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)"

{ja href="http://tools.ietf.org/html/rfc3281" }RFC 3281 "An Internet Attribute Certificate Profile for Authorization"i/a\_i

{ja href="http://tools.ietf.org/wg/pkix/" }IETF: Public-Key Infrastructure (X.509) (Active WG)i/a\_i

{ja href="http://www.itu.int/rec/T-REC-X.500/en" }X.500i/a\_i

{ja href="http://www.itu.int/rec/T-REC-X.509/en" }X.509i/a\_i wszystkie wersje (ja href="http://www.itu.int/rec/T-REC-X/e" }inne z serii Xi/a\_i)

{ja href="http://www.itu.int/ITU-T/asn1/index.html" }ASN.1i/a\_i

{ja href="http://asn1.elibel.tm.fr/en/standards/encoding" }BER, DER, PER, CER, XER, ECNi/a\_i - kodowania ASN.1

{ja href="http://www.itu.int/ITU-T/studygroups/com17/languages/X.693-0112.pdf" }X.693 "XML Encoding Rules"i/a\_i (kodowanie ASN.1 do XML)

{ja href="/podpis\_elektroniczny/ISIS-MTT\_Corespecification\_v1.1.pdf" } > ISIS-MTTspecyfikacja1.1 < /a >, < ahref = "http://www.teletrust.de/index.php?id = 395" } ISIS-MTT(specyfikacjaze stronyprojektu) < /a >, < ahref = "http://www.teletrust.de/index.php?id = 364" } ISIS-MTT(stronaglowna) < /a >, komentarz < ahref = "/podpis\_elektroniczny/ISIS-MTT-PreSpec-FinalDraft.pdf" } ISIS-MTT" Long-TermSignatureConservation" < /a > { < ahref = "https://www.eema.org//index.cfm" } EEMA(EuropeanAssociationfore - IdentityandSecurity) < /a >

{ja href="http://www.esstandardisation.eu/index.php" }eSignatures Standardisation Surveyi/a\_i (publikacja w listopadzie 2007)

{ja href="http://www.ietf.org/html.charters/ltans-charter.html" }IETF WG - Long-Term Archive and Notary Services (ltans)i/a\_i

{ja href="http://www.bundesnetzagentur.de/enid/5f4fd603029657429043d7befe0b0214,0/Areas/ElectronicSignature/Niemieckieprzepisyopodpisielektronicznym(SigG, SigV), poangielsku < /a > { < ahref = "http://www.cs.dartmouth.edu/pki02/Micali/paper.pdf" } NOVOMODO(X.509v3) < /a > , proponowanowametodaweryfikacjiwazności certyfikatów konkurencyjną do CRL/OCSP

{Bridge CA

li\_i {ja href="http://www.bridge-ca.org/eb-ca2/" }European Bridge CAi/a\_i {ja href="http://www.certipath.com/" } Bridge CA (CBCA)i/a\_i

i/li\_i

- {ja href="http://www.tscp.org/resources.htm" }Transglobal Secure Collaboration Program (TSCP)i/a\_i

{ja href="http://www.oasis-open.org/specs/index.phpdssv1.0" }OASIS: Digital Signature Services v1.0i/a\_i

{ja href="http://www.oasis-open.org/committees/tc\_home.php?wg\_abrev = securitysamlv20" } > OASIS : SecurityAssertionMarkupLanguage(SAML) < /a > < /ul >

{strong\_i SPKIi/strong\_i

- {ja href="http://world.std.com/cme/html/spki.html" }SPKI/SDSI Certificatesi/a\_i

{strong\_i Inne linkii/strong\_i

- {ja href="http://tools.ietf.org/html/rfc4270" }RFC 4270 "Attacks on Cryptographic Hashes in Internet Protocols"i/a\_i (w tym także na PKI)

- [Wikipedia : Preimage resistance](http://pl.wikipedia.org/wiki/Preimage_resistance) < /a > – *odporność kryptograficznych funkcji skrótuna fałszerstwa* {< a href = "http : //tools.ietf.org/html/rfc2898" PKCS5 : Password – Based Cryptography Specification Version 2.0" < /a > (mechanizmy przetwarzania hasel w aplikacjach kryptograficznych)
- [Przykład Elektronicznej Skrzynki Podawczej](http://muw.e-bip.pl/upo/UPOService.aspx) /a;
  - {i**PN ISO/IEC**i/strongi
  - {i**ISO/IEC 27001:2005**i/strongi - norma Systemu Zarządzania Bezpieczeństwem Informacji
  - {i**ISO/IEC 17799:2005**i/strongi - zalecenia i najlepsze praktyki
  - {i**Standardy de facto**i/strongi
    - [OWASP \(Open Web Application Security Project\)](http://www.owasp.org/index.php/Main_Page) < /a > {< a href = "http : //www.isecom.org/osstmm/" > OSSTMM (Open Source Security Testing Methodology)
    - [The Standard of Good Practice for Information Security](http://www.isfsecuritystandard.com/index_n.s.htm) /a > {< a href = "http : //openid.net/wiki/index.php/RelyingPartyBestPractices" > OpenID Relying Party Best Practices
  - {i**Zalecenia NIST**i/strongi
    - [NIST 800](http://csrc.nist.gov/publications/nistpubs/index.html) /a;