Zestaw norm i standardów, które opisują różne aspekty rozwiązań stosowanych w PKI.

Standardy i normy polskie oraz międzynarodowe – (ISO, ECBS, UE):

- **DIRECTIVE 1999/93/EC** **DIRECTIVE** OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures
- **PN-EN ISO 11568-1-6:** - Bankowość. Zarządzanie kluczami w bankowości detalicznej
- PrPN-ISO 13492 – Bankowość Elementy danych związane z zarządzaniem kluczami (detal)
- **PN-ISO/IEC 13888-1do3:1999** - Technika informatyczna. Techniki zabezpieczeń. Niezaprzeczalność
- **PN-ISO/IEC 11770-1do3:** Techniki zabezpieczeń. Zarządzanie kluczami
- **PN-ISO/IEC 10118-1do3:**1996 Technika informatyczna - Techniki zabezpieczeń. Funkcje skrótu
- **ISO/DIS 15782-1** Certificate management for financial services - Part 1: Public Key Certificates
- **ISO 15782-2** Banking - Certificate management - Part 2: Certificate extensions
- **ISO/IEC 10181-4:1997** Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework
- **ISO 8732,** "Banking - Key management (wholesale)",
- **ISO 11166,** "Banking - Key management by means of asymmetric algorithms - Part 1 and 2
- **ISO 8731,** "Banking - Approved Algorithms for message Authentication - Part 1and 2
- **ISO/IEC TR 14516 | ITU-T X.842** Wytyczne dla użytkowania i zarządzania usługami Zaufanej Trzeciej Strony.
- **ISO/IEC 9797**, "Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm",
- **ISO 8372,** "Information processing - Modes of operation for a 64-bit block cipher algorithm",
- **ISO/IEC 14888-1-3** - Information technology - Security techniques - Digital signatures
- American National Standard for Financial Services **ANS X9.79-1:2001 Part 1: PKI Practices and Policy Framework**
- **ITU-T –X500 OSI** The Directory: Overview of concept, models and services
- **ECBS-TC4, TR402** Technical Report 402 "Certification authorities",
- **ECBS-TC4, TR405** Technical Report 405 "Key recovery in financial systems", 1998
- **ECBS-TC4, TR406** Technical Report 406 "Guidelines on algorithms usage and key management"

- **Standardy i normy organizacji międzynarodowych i korporacyjnych**

ETSI -European Telecommunications Standards Institute

Identyfikator	Nazwa standardu	Rodzaj
EG 201 057 V1.1.2 (1997-07)	Telecommunications Security; Trusted Third Parties (TTP);	ETSI Guide

	Requirements for TTP services	
ETSI TS 101 456 V1.1.1 (2000-12)	Policy requirements for certification authorities issuing qualified certificates	Technical Specification
ETSI TS 101 862 V1.2.1 (2001-06)	Qualified certificate profile	Technical Specification
ETSI ES 101 733 V1.2.2 (2000-12)	Electronic signature formats	ETSI Standard
TR 101 xxx V0.4.2 (1998-11)	Telecommunications Security; Electronic signature standardization report	Technical Report
ETSI TS 101 861 V1.1.1 (2001-08)	Time Stamping Profile	Technical Specification
Draft ETSI TS xxxx STF 178-T1 draft I 3/11/2001	Policy requirements for time-stamping authorities	Technical Specification
ETSI TR X XV0.0.2 (2001-08)	XML Format for Signature Policies	Technical Report
TR 101 xxx V0.4.2 (1998-11)	Telecommunications Security; Electronic signature standardization report	Technical Report

CEN/ISSS Workshop on Electronic Signatures (WS/E-Sign), EESSI - European Electronic Signature Standardization Initiative,

Numer	Nazwa	Data publikacji, status
N 161 14167-1:	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures	Berlin/2001-08-01 Draft CWA Version: 0.17 Issued: 2001-07-17
Area G2: N 140 CWA14171	"Procedures for electronic signature verification"	CWA Berlin/2001-03-14 Version 1.0.5 March 13, 2001
Area G1 N 141	"Security Requirements for Signature Creation Systems"	CWA: Berlin/2001-03-14 Version: 3.9 Issued: 2001-03-12
N143	Conformity Assessment Guidance. Part 1 – General	EESSI 2001-03-15
N144	Conformity Assessment Guidance. Part 2 – Certification Authority and Process	EESSI 2001-03-15
N 164 14172-3	Conformity Assessment Guidance. Part 3 - Trustworthy systems managing certificates for electronic signatures	Berlin/2001-09-04 Draft Version: 0.6 Issued: 2001-09-03
N 165 CWA 14172-4	EESSI Conformity Assessment Guidance. Part 4 – Signature creation applications and procedures for electronic signature verification	EESSI Issued: 2001-09-04
N 166 14172-5	Conformity Assessment Guidance. Part 5 - Secure signature creation	EESSI Issued: 2001-09-04

	devices	
Area F N 136	Workshop Agreement Group F - B- *EAL* 4	Berlin/2001-03-01
Area F N 137	Workshop Agreement Group F- A- *EAL* 4.	Berlin/2001-03-01

Rodzaj dokumentu **RFC** -Request for Comments

Uwaga: niektóre standardy RFC zawierają inne (np. **PKCS** RSA Laboratories) wymienione w zestawieniach ujętych przy innych organizacjach standaryzujących – dla zachowania kompletu pozostawiono te standardy w tym zestawieniu

Nr RFC	**Tytuł standardu**	**Firmy opracowujące**	**Wydane / ważność**
1319 Updates: RFC 1115	The MD2 Message-Digest Algorithm	RSA Laboratories	April 1992
1321.	The MD5 Message-Digest Algorithm	MIT Laboratory for Computer Science and RSA Data Security, Inc	April 1992
1422 Obsoletes : 1114	Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management	BBN IAB IRTF PSRG, IETF PEM	February 1993
1423 Obsoletes : 1115	Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers	IRTF PSRG, IETF PEM WG	February 1993
1424	Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services	RSA Laboratories	February 1993
1519 Obsoletes : 1338	Classless Inter-Domain Routing (CIDR):an Address Assignment and Aggregation Strategy	BARRNet; cisco, MERIT; OARnet	September 1993
1738	Uniform Resource Locators (URL)	CERN, Xerox Corporation, University of Minnesota	December 1994
1778 Obsoletes : 1488	The String Representation of Standard Attribute Syntaxes	University of Michigan; ISODE Consortium; Performance Systems International; NeXor Ltd.	March 1995
1883	Internet Protocol, Version 6 (IPv6) Specification	Xerox PARC Networks	December 1995
2104	HMAC: Keyed-Hashing for Message Authentication	IBM; UCSD	February 1997
2119	Key words for use in RFCs to Indicate Requirement Levels	Harvard University Best Current Practice	March 1997
2277	IETF Policy on Character Sets and Languages	UNINETT Best Current Practice	January 1998
2279	UTF-8, a transformation format of	Alis Technologies	January

Obsoletes : 2044	ISO 10646		1998
2311	S/MIME Version 2 Message Specification	RSA Data Security Internet Mail Consortium; Netscape Category: Informational	March 1998
2312	S/MIME Version 2 Certificate Handling	Internet Mail Consortium; RSA Data Security; Netscape Category: Informational	March 1998
2313	PKCS #1: RSA Encryption Version 1.5	RSA Laboratories East Category: Informational	March 1998
2314	PKCS #10: Certification Request Syntax Version 1.5	RSA Laboratories East Category: Informational	March 1998
2315	PKCS #7: Cryptographic Message Syntax Version 1.5	RSA Laboratories, East Category: Informational	March 1998
2321	RITA -The Reliable Internetwork Troubleshooting Agent	Cohesive Network Systems Category: Informational	1 April 1998
2459	Internet X.509 Public Key Infrastructure Certificate and CRL Profile	SPYRUS; VeriSign; NIST; Citicorp	January 1999
2510	Internet X.509 Public Key Infrastructure Certificate Management Protocols	Entrust Technologies; SSE	March 1999
2511	Internet X.509 Certificate Request Message Format	VeriSign; DoD Entrust Technologies	March 1999
2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	CygnaCom Solutions, Inc. VeriSign, Inc. Category: Informational	March 1999
2528	Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates	SPYRUS; NIST Category: Informational	March 1999
2559 Updates: 1778	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2	Entrust; Netscape: Xcert	April 1999
2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP	VeriSign; CertCo; ValiCert; Entrust Technologies	June 1999
2585	Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP	SPYRUS; IMC	May 1999
2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema	Entrust; Netscape; Xcert	June 1999
2630	Cryptographic Message Syntax	SPYRUS	June 1999
2631	Diffie-Hellman Key Agreement Method	RTFM Inc.	June 1999

- Typ dokumentu **- PKIX** (Public-Key Infrastructure X.509), organizacja - **IETF** – (Internet Engineering Task Force)

Identyfikator	**Nazwa**	Wydany
draft-ietf-pkix-ac509prof-09.txt	An Internet Attribute Certificate Profile for Authorization	8th June 2001
draft-ietf-pkix-cmc-archive-00.txt	CMC Extensions: Server Side Key Generation and Key Archival< >	July 13, 2001
draft-ietf-pkix-dpv-dpd-00.txt	Delegated Path Validation and Delegated Path Discovery Protocols	July, 2001
draft-ietf-pkix-ipki-new-rfc2527-00.txt	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	July 12, 2001
draft-ietf-pkix-ipki-pkalgs-03.txt	Algorithms and Identifiers for theInternet X.509 Public Key Infrastructure Certificate and CRL Profile	July, 2001
draft-ietf-pkix-new-part1-08	Internet X.509 Public Key Infrastructure Certificate and CRL Profile	July 2001
draft-ietf-pkix-pi-02.txt	Target category: Standard Track Internet X.509 Public Key Infrastructure Permanent Identifier	October, 2001
draft-ietf-pkix-proxy-01.txt	Internet X.509 Public Key Infrastructure Proxy Certificate Profile	August 2001
draft-ietf-pkix-rfc2510bis-04.txt	S. Farrell Internet X.509 Public Key Infrastructure Certificate Management Protocols	May, 2001
draft-ietf-pkix-rfc2511bis-02.txt	Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)	May 2001
draft-ietf-pkix-rfc2797-bis-01.txt	Certificate Management Messages over CMS	July 2001
draft-ietf-pkix-scvp-06.txt	Simple Certificate Validation Protocol (SCVP)	Paul Hoffman

- Typ dokumentu **-PKCS (**Public Key Cryptography Standard – a set of commonly applied data cryptography standards developed by RSA Data Security Inc.)

Identyfikator	Tytuł	Firma opracowująca	Wydany / ważność
#1 v2.1:	RSA Cryptography Standard	RSA Laboratories	January 5, 2001
#3 Version 1.4	Diffie-Hellman Key-Agreement Standard	RSA Laboratories	November 1, 1993
#6 Version 1.5	Extended-Certificate Syntax Standard	RSA Laboratories	November 1, 1993*
#10	Certification Request Syntax Standard	RSA Laboratories	Version 1.0 November

			1, 1993
#11 v2.11	Cryptographic Token Interface Standard	RSA Laboratories	November 2000
#15	Conformance Profile Specification	RSA Laboratories	August 1, 2000

Normy i standardy stosowane w systemach zarządzania bezpieczeństwem.

- **Normy określające zasady budowy struktur i polityk bezpieczeństwa**

- **ISO/TR 13569:**1997(E) Banking and related financial services Information security guidelines
- **PN - I -13335-1:1999** Wytyczne do zarządzania bezpieczeństwem systemów informatycznych
- **ISO9807:1991** Banking and related financial services – Requirements for message authentication (retail).
- **PN-ISO/IEC 9798-1-3:1996** Technika informatyczna - Techniki zabezpieczeń. Mechanizmy uwierzytelniania podmiotów.
- **ISO 17799 (BS 7799)**: Information security management Arkusz l. Code of practice for information security management systems Arkusz 2. Specification for information security management systems

RFC 2196 (RFC1224) - Site Security Handbook

- **Normy związane z zarządzaniem bezpieczeństwem Systemów Sieciowych**

- **ECBS-TC4,** 401 Technical Report 401 "Secure banking over the Internet", 1997
- **PN-92/T-20001.02** Systemy przetwarzania informacji. Współdziałanie systemów otwartych (OSI). Podstawowy model odniesienia. Architektura zabezpieczeń.
- **ISO/IEC 9594-8** (X.509), Information technology — Open Systems Interconnection — The Directory.
- **ISO 10164-7** Information technology - Open Systems Interconnection - Systems Management: Security Alarm Reporting Function
- **ISO/IEC 10164-8**:1993 Information technology -- Open Systems Interconnection -- Systems Management: Security audit trail function
- **ISO 10164-9**. Information technology - Open Systems Interconnection - Systems Management: Objects and Attributes for Access Control
- **ISO/IEC 10181-1**, "Information technology - Open Systems Interconnection - Security frameworks for open systems - Part 1: Overview", 1995 (equivalent to ITU-T Rec X 810, 1995)

- **ISO/IEC 10181-2**, "Information technology - Open Systems Interconnection - Security frameworks for open systems - Part 2: Authentication framework", 1995 (equivalent to ITU-T Rec X 811, 1995)
- **ISO/IEC 10181-3**, "Information technology - Open Systems Interconnection - Security frameworks for open systems - Part 3: Access control framework", Draft 1995
- **ISO/IEC 10181-4**, "Information technology - Open Systems Interconnection - Security frameworks for open systems - Part 4: Non-repudiation framework", Draft 1995
- **ISO/IEC 10181-5,** "Information technology - Open Systems Interconnection - Security frameworks for open systems - Part 5: Integrity framework", Draft 1995
- **ISO/IEC 10181-6**, "Information technology - Open Systems Interconnection - Security frameworks for open systems - Part 6: Confidentiality framework", Draft 1995
- **ISO/IEC 10181-7**:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework
- **ISO/IEC 11586-1**:1996 Information technology -- Open Systems Interconnection -- Generic upper layers security: Overview, models and notation
- **ISO/IEC 11586-2**:1996 Information technology -- Open Systems Interconnection -- Generic upper layers security: Security Exchange Service Element (SESE) service definition
- **ISO/IEC 11586-3**:1996 Information technology -- Open Systems Interconnection -- Generic upper layers security: Security Exchange Service Element (SESE) protocol specification
- **ISO/IEC 11586-4**:1996 Information technology -- Open Systems Interconnection -- Generic upper layers security: Protecting transfer syntax specification
- **ISO/IEC 11586-5**:1997 Information technology -- Open Systems Interconnection -- Generic upper layers security: Security Exchange Service Element (SESE) Protocol Implementation Conformance Statement (PICS) proforma
- **ISO/IEC 11586-6**:1997 Information technology -- Open Systems Interconnection -- Generic upper layers security: Protecting transfer syntax Protocol Implementation Conformance Statement (PICS) proforma

Normy związane z zarządzaniem bezpieczeństwem przy użyciu kart

- **ISO 7816**. Smart Cards
- **ISO/IEC 7812-1:1993,** *Identification cards - , Identification of issuers – Part1: Numbering system*
- **ISO/IEC 7812-2:1993**, *Identification cards - Identification of issuers – Part 2:Application and registration procedures.*
- **ISO/IEC 7816-8**:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands
- **ISO 8583:1993**, Financial transaction card originated messages – Interchange message specifications.
- **PN-EN ISO 10202** - Karty transakcji finansowych. Architektura zabezpieczenia systemów obsługujących transakcje finansowe za pomocą kart elektronicznych.

- **PN-EN 30202-1:2000** Karty transakcji finansowych. Architektura zabezpieczeń systemów obsługujących transakcje finansowe za pomocą kart elektronicznych. Cykl życia karty.
- **ISO 10202-2**:1996 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 2: Transaction process
- **PN-EN ISO 10202-3:1999** Karty transakcji finansowych. Architektura zabezpieczeń systemów obsługujących transakcje finansowe za pomocą kart elektronicznych. Powiązania przez klucz kryptograficzny.
- **ISO 10202-4**:1996 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 4: Secure application modules
- **ISO 10202-5**:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 5: Use of algorithms
- **ISO 10202-6**:1994 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 6: Cardholder verification
- **ISO 10202-7**:1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 7: Key management
- **ISO 10202-8:**1998 Financial transaction cards -- Security architecture of financial transaction systems using integrated circuit cards -- Part 8: General principles and overview

Inne normy związane z zarządzaniem bezpieczeństwem

- **ISO/IEC 15408-1**:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
- **ISO/IEC 15408-2**:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements
- **ISO/IEC 15408-3**:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements
- **ISO 8649** Information technology - Open Systems Interconnection - Service definision for the Association Control Service Element
- **ISO 8730.** Banking - Requirements for Message Authentication (Wholesale)
- **ISO 8731**. Banking - Approved Algorithms for Message Authentication
- **ISO /IEC 9797**, Information technology — Security techniques — Data integrity mechanism using a cryptographic check function employing a block cipher algorithm.
- **ISO/IEC 13491** Banking - Secure cryptographic devices (retail)
- **CCITT Recommendation X.800** – Security Architecture for Open System Interconnection for CCITT Applications

FIPS PUB- FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Identyfikator	Nazwa	Data publikacji
FIPS PUB 31	Guidelines FOR AUTOMATIC DATA PROCESSING PHYSICAL SECURITY AND RISK MANAGEMENT	1974 JUNE
FIPS 46-3	Data Encryption Standard	
FIPS PUB 73	Guidelines for SECURITY OF COMPUTER APPLICATION	1980 JUNE 30
FIPS PUB 87	Guidelines for ADP Contingency Planning	1981 MARCH 27

FIPS 113	Authentication	
FIPS 112	Password Usage	
FIPS PUB 140-1	SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES	1994 January 11
FIPS PUB 140-2	SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES (Supersedes FIPS PUB 140-1, 1994 January 11)	Issued 1999
FIPS PUB 180-1	SECURE HASH STANDARD	1995 April 17

American National Standards Institute (ANSI)

- **ANSI X3.92** - 1981. The Data Encryption Algorithm (DEA)
- **ANSI X3.105** - 1983. Data Link Encryption
- **ANSI X3.106** - 1983. Data Encryption Algorithm - Modes of operation for the DEA
- **ANSI NCITS.118** - 1998. Personal Identification Number - PIN Pad
- **ANSI X9.1** - 1991. Bank Cards - Magnetic Stripe Data Content (Track 3)
- **ANSI X9.2** - 1980. Interchange Message Specification for Debit and Credit Card Message Exchange among Financial Institution
- **ANSI X9.8** - 1982. Banking - Personal Identification Number Management and Security
- **ANSI X9.9** - 1986. Financial Institution Message Authentication
- **ANSI X9.17** - 1985. Financial Institution Key Management (Wholesale)
- **ANSI X9.19** - 1996. Financial Institution Retail Message Authentication
- **ANSI X9.23**. 1988. Financial Institution Encryption for Wholesale Financial Messages
- **ANSI X9.24**. Financial Services - Key Management Using the DEA
- **ANSI X9.30**.1-1995, Public Key Cryptography for the Financial Services Industry - Part1: The Digital Signature Algorithms (DSA).
- **ANSI X9. 30.2**-1997, Public Key Cryptography for Financial Services Industry- The Secure Hash Algorithm (SHA-1) - Part 2
- **ANSI X9.57**:1997 - Public Key Cryptography for the Financial Services Industry: Certificate Management.
- **ANSI X12.58**- Electronic Data Interchange Security Services X12.58 (version 2)