Primul grup de standarde

- RFC 4210 Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP). C. Adams, S. Farrell, T. Kause, T. Mononen. September 2005
- RFC 4211 Certificate Request Protocol
  Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF). J. Schaad. September 2005.
- RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu. November 2003.
- RFC 3494 Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status. K. Zeilenga. March 2003.
- RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams. June 1999.
- RFC 2585 Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP. R. Housley, P. Hoffman.May1999.
- RFC 2587 Internet X.509 Public Key Infrastructure LDAPv2 Schema. S. Boeyen, T. Howes, P. Richard. June 1999.
- RFC 2797 Certificate Management Messages over CMS. M. Myers, X. Liu, J. Schaad, J. Weinstein. April 2000.
- RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms. H. Prafullchandra, J. Schaad. July 2000.
- RFC 3029 Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols. C. Adams, P. Sylvester, M. Zolotarev, R. Zuccherato. February 2001.
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile. S. Santesson, M. Nystrom, T. Polk. March 2004.
- RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). C. Adams, P. Cain, D. Pinkas, R. Zuccherato. August 2001.
- RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. L. Bassham, W. Polk, R. Housley. April 2002.
- RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. R. Housley, W. Polk, W. Ford, D. Solo. April 2002.
- RFC 3281 An Internet Attribute Certificate Profile for Authorization. S. Farrell, R. Housley. April 2002.

Al doilea grup de standarde

- CWA 14167-1:2003 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
- CWA 14167-2:2003 Cryptographic module for CSP signing operations with backup -Protection profile - CMCSOB PP
- CWA 14167-3:2004 Cryptographic module for CSP key generation services protection profile CMCKG-PP
- CWA 14167-4:2004 Cryptographic module for CSP signing operations – Protection profile - CMCSO PP
- CWA 14170:2003 Security requirements for signature creation applications
- CWA 14171:2004 General guidelines for electronic signature verification
- CWA 14172-1:2003 EESSI Conformity Assessment Guidance - Part 1: General introduction
- CWA 14172-2:2003 EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes
- CWA 14172-3:2003 EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures
- CWA 14172-4:2004 EESSI Conformity Assessment Guidance - Part 4: Signature creation applications and general guidelines for electronic signature verification
- CWA 14172-5:2004 EESSI Conformity Assessment Guidance - Part 5: Secure signature-creation devices
- CWA 14172-6:2004 EESSI Conformity Assessment Guidance - Part 6: Signature creation device supporting signatures other than qualified
- CWA 14172-7:2004 EESSI Conformity Assessment Guidance - Part 7:
  Cryptographic modules used by Certification Service Providers for signing operations and key generation services
- CWA 14172-8:2004 EESSI Conformity Assessment Guidance - Part 8: Timestamping Authority services and processes

- CWA 14355:2004 Guidelines for the implementation of Secure Signature-Creation Devices
- CWA 14890-1:2004 Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements
- CWA 14890-2:2004 Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services

Al treilea grup de standarde

- ISO/IEC 9796-2:2002 Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms
- ISO/IEC 9796-3:2000 Information technology - Security techniques - Digital signature schemes giving message recovery - Part 3: Discrete logarithm based mechanisms
- ISO/IEC 10118-1:2000 Information technology - Security techniques - Hash-functions - Part 1: General
- ISO/IEC 10118-2:2000 Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an n-bit block cipher
- ISO/IEC 10118-3:2004 Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions
- ISO/IEC 10118-4:1998 Information technology - Security techniques - Hash-functions - Part 4: Hash-functions using modular arithmetic
- ISO/IEC 14888-1:1998 Information technology - Security techniques - Digital signatures with appendix - Part 1: General
- ISO/IEC 14888-2:1999 Information technology - Security techniques - Digital signatures with appendix - Part 2: Identity-based mechanisms
- ISO/IEC 14888-3:1998 Information technology - Security techniques - Digital signatures with appendix - Part 3: Certificate-based mechanisms
- ISO/IEC 18033-1:2005 Information technology - Security techniques - Encryption algorithms - Part 1: General
- ISO/IEC 18033-3:2005 Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers
- ISO/IEC 18033-4:2005 Information technology - Security techniques - Encryption algorithms - Part 4: Stream ciphers

Al patrulea grup de standarde

- PKCS#1 RSA Cryptography Standard
- PKCS #3 Diffie-Hellman Key Agreement Standard
- PKCS #5 Password-Based Encryption Standard
- PKCS #6 Extended-Certificate Syntax Standard
- PKCS#7 Cryptographic Message Syntax Standard
- PKCS #8 Private-Key Information Syntax Standard
- PKCS #9 Selected Object Classes and Attribute Types.
- PKCS #10 Certification Request Syntax Standard
- PKCS#ll Cryptographic Token Interface Standard
- PKCS #12 Personal Information Exchange Syntax Standard
- PKCS #13 Elliptic Curve Cryptography Standard

Al cincilea grup de standarde

S/MIME

- RFC 2311 S/MIME Version 2 Message Specification. S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade, L. Repka. March 1998.
- RFC 2312 S/MIME Version 2 Certificate Handling. S. Dusse, P. Hoffman, B. Ramsdell, J. Weinstein. March 1998.
- RFC 2630 Cryptographic Message Syntax. R. Housley. June 1999.
- RFC 2632 S/MIME Version 3 Certificate Handling. B. Ramsdell, Ed.. June 1999.
- RFC 2633 S/MIME Version 3 Message Specification. B. Ramsdell, Ed.. June 1999.
- RFC 2634 Enhanced Security Services for S/MIME. P. Hoffman, Ed.. June 1999.

- RFC 2785 Methods for Avoiding the "Small-Subgroup" Attacks on the Diffie-Hellman Key Agreement Method for S/MIME. R. Zuccherato. March 2000.

S/HTTP TLS

- RFC 2246 The TLS Protocol Version 1.0. T. Dierks, C. Allen. January 1999.
- RFC 2659 Security Extensions For HTML. E. Rescorla, A. Schiffman. August 1999.
- RFC 2660 The Secure HyperText Transfer Protocol. E. Rescorla, A. Schiffman. August 1999.
- RFC 2817 Upgrading to TLS Within HTTP/1.1. R. Khare, S. Lawrence. May 2000.
- RFC 2818 HTTP Over TLS. E. Rescorla. May 2000.

IPSec

- RFC2401 Security Architecture for the Internet Protocol. S. Kent, R. Atkinson. November 1998.
- RFC 2402 IP Authentication Header. S. Kent, R. Atkinson. November 1998.
- RFC 2406 IP Encapsulating Security Payload (ESP). S. Kent, R. Atkinson. November 1998.
- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP). D. Maughan, M. Schertler, M. Schneider, J. Turner. November 1998.

DNS

- RFC 3007 Secure Domain Name System (DNS) Dynamic Update. B. Wellington. November 2000.
- RFC 2535 Domain Name System Security Extensions. D. Eastlake 3rd. March 1999.
- RFC 2536 DSA KEYs and SIGs in the Domain Name System (DNS). D. Eastlake 3rd. March 1999.
- RFC 3110 RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS). D.Eastlake 3rd. May 2001.
- RFC 2538 Storing Certificates in the Domain Name System (DNS). D. Eastlake 3rd, O. Gudmundsson. March 1999.
- RFC 2539 Storage of Diffie-Hellman Keys in the Domain Name System (DNS). D.Eastlake 3rd. March 1999.
- RFC 2540 Detached Domain Name System (DNS) Information. D. Eastlake 3rd. March 1999.
- RFC 2541 DNS Security Operational Considerations. D. Eastlake 3rd. March 1999.