Bibliography

[Akl83] S. Akl: *Digital Signatures: A Tutorial Survey*, IEEE Computer Magazine, Feb. 1983, pp. 15-24

[AKS90] A. Ahtiainen, J. Keskinen, J. Simolin, K. Tarpila, I. Turunen, *Protocol Software Engineering Tools for Implementation of a General Purpose OSI Stack*, in Computer Networking (L. Csaba et all., editors), Elsevier Science Publishers, BV (North Holland), presented in IFIP conference, Budapest, May 1990

[ANS81] ANSI X3.92, *Data Encryption Algorithm*, American National Standards Institute, New York, 1981

[ANS83] ANSI X3.106, *Data Encryption Algorithm – Modes of Operation*, American National Standards Institute, New York, 1983

[BAN89] M. Burrows, M. Abadi, R. Needham: *A Logic of Authentication*, ACM Operating Systems Review, Vol. 23, No. 5, 1989

[Bar90] R. Barrett, *Security in Wide Area Networks – Some Baseline Requirements*, Computer Fraud & Security Bulletin, Dec. 1990, pp. 14-18

[BDH88] D. Branstad, J. Dorman, R. Housley, *SP4: A Transport Encapsulation Security Protocol*, 1988

[Bel89] S. Bellowin, *Security Problems in the TCP/IP Protocol Suite*, ACM Computer Communication Review, Vol. 19, No. 2, April 1989, pp. 32-48

[BG89] T. Beth, D. Gollmann, *Algorithm Engineering for Public Key Algorithms*, IEEE Journal on Selected Areas in Communications, Vol. 7, No. 4, May 1989, pp. 458-466

[BI89] F. Burg, N. Di Iorio, *Networking of Networks: Interworking According to OSI*, IEEE Journal on Selected Areas in Communications, Vol. 7, No. 7, September 1989, pp. 1131-1142

[Bib77] K. Biba, *Integrity Considerations for Secure Computer Systems*, ESD-TR-76-372, MITRE MTR-3153 NTIS AD A039324, Bedford, Mass., April 1977

 © Arto Karila, 1991

[Bir85] A. Birrell, *Secure Communications Using Remote Procedure Calls*, ACM Transactions on Computer Systems, Vol. 3, No. 1, Feb. 1985, pp. 1-14

[BM90] J. Burns, C. Mitchell, *A Security Scheme for Resource Sharing over a Network*, Computers & Security, Vol. 9, No. 1, Feb. 1990, pp. 67-75

[BO88] E. Brickell, A. Odlyzko, *Cryptanalysis: A Survey of Recent Results*, Proceedings of the IEEE, Vol. 76, No. 5, May 1988, pp. 578-593

[BP74] D. Bell, E. LaPadula, *Secure Computer Systems: Mathematical Foundations and Model*, M74-244, Vol. 2, MITRE Corp., Bedford, Mass., Oct. 1984

[BS90] E. Biham, A. Shamir, *Differential Cryptanalysis of DES-Like Cryptosystems*, Proceedings of Crypto'90, June 1990

[BVA90] T. Beth, S. Vanstone, G. Agnew, *What One Should Know about Public Key Algorithms – Today!*, proceedings of SECURICOM 90, Paris, March 1990

[CEN90] *Report on Taxonomy for Security Standardisation*, prepared for the ITSTC by the CEN/CENELEC Security Group, CSecG/49/90, Sep. 1990

[CG90] P.-C. Cheng, V. Gligor, *On the Formal Specification and Verification of a Multiparty Session Protocol*, Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, May 7-9, 1990, pp. 216-233

[CGV90] R. Cocino, M.T. Grillo, F. Vaschetto, *Draft Specification for a Secure Tranport Protocol Class 0*, 4th version, a contribution to COST-225, ISO/IEC JTC1/SC6/WG4, December 1990

[Cha85] D. Chaum, *Security without Identification: Transaction Systems to Make Big Brother Obsolete*, Communications of the ACM, Vol. 28, No. 10, Oct. 1985, pp. 1030-1044

[Cla88] D. Clark, *The Design Philosophy of the DARPA Internet Protocols*, ACM Computer Communication Review, Vol. 18, No. 4, Aug. 1988, pp. 106-114

[Com89] Commission of the European Communities, *EDI in Perspective*, EUR 11883 EN, Brussel – Luxembourg, 1989

[Com90] Commission of the European Communities, *Proposal for a Decision of the Council in the Field of Information Security* (INFOSEC), COM(90) 314 final, Brussel, July 3, 1990

[COS90] Security Mechanisms for Computer Networks, *Extended OSI Security Architecture*, COST-11 Ter Project Report, Volume II, Draft, Oct. 1990

[CP88] J. Crowcroft, K. Paliwoda, *A Multicast Transport Protocol*, ACM Computer Communication Review, Vol. 18, No. 4, Aug. 1988, pp. 247-256

[CPW89] L. Cassel, C. Partridge, J. Westcott, *Network Management Architectures and Protocols: Problems and Approaches*, IEEE Journal on Selected Areas in Communications, Vol. 7, No. 7, September 1989, pp. 1104-1114

[Dav83] D. Davies, *Applying the RSA Digital Signature to Electronic Mail*, IEEE Computer Magazine, Feb. 1983, pp. 55-62

[Dee88] S. Deering, *Multicast Routing in Internetworks and Extended LANs*, ACM Computer Communication Review, Vol. 18, No. 4, Aug. 1988, pp. 55-64

[Den83] D. Denning, *Protecting Public Keys and Signature Keys*, IEEE Computer Magazine, Feb. 1983, pp. 27-35

[DH76] W. Diffie, M. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory,Vol. IT-22, No. 6, Nov. 1976, pp. 644-654

[DH77] W. Diffie, M. Hellman, *Exhaustive Cryptanalysis of the NBS Data Encryption Standard*, Computer, June 1977, pp. 74-78

[DH79] W. Diffie, M. Hellman, *Privacy and Authentication: An Introduction to Cryptography*, Proceedings of the IEEE, Vol. 67, No. 3, Mar. 1979, pp. 397-427

[Dif88] W. Diffie, *The First Ten Years of Public-Key Cryptography*, Proceedings of the IEEE, Vol. 76, No. 5, May 1988, pp. 560-577

[DKK90] F. Dix, M. Kelly, R. Klessig, *Access to a Public Switched Multi-Megabit Data Service Offering*, ACM Computer Communication Review, Vol. 20, No. 3, July 1990, pp. 46-61

[DoD85] *Trusted Computer Systems Evaluation Criteria*, DoD 5200.28-STD, Department of Defense, USA, 1985

[DP84] D. Davies, W. Price, *Security for Computer Networks*, John Wiley & Sons, 1984

[DS81] D. Denning, G. Sacco, *Timestamps in Key Distribution Protocols*, Communications of the ACM, Vol. 24, No. 8, Aug. 1981, pp. 533-536

[ECM88] ECMA, *Security in Open Systems - A Security Framework*, ECMA TR/46, July 1988

[ECM89] ECMA, *Security in Open Systems, Data Elements and Service Definitions*, July 1989

[Far91] Discussions with professsor David Farber in Helsinki, March 1991

[FFS88] U. Feige, A. Fiat, A. Shamir, *Zero-knowledge Proofs of Identity*, Journal of Cryptology, 1, 1988

[FP90] W. Fumy, A. Pfau, *Asymmetric Authentication Schemes for Smart Cards – Dream or reality?*, IFIP TC-11 6th International Conference and Exhibition on Information Security, Espoo, Finland, 1990

[FS87] A. Fiat, A. Shamir, *How to Prove Yourself: Practical Solutions to Identification and Signature Problems*, Proceedings of Crypto'86, Springer, 1987

[Gen90] G. Genilloud, *X.400 MHS: First Steps Towards an EDI Communication Standard*, ACM Computer Communication Review, Vol. 20, No. 2, April 1990, pp. 72-86

[GNY90] L. Gong, R. Needham, R. Yahalom, *Reasoning about Belief in Cryptographic Protocols*, Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, May 7-9, 1990, pp. 234-248

[GOS90] *U.S. Government Open Systems Interconnection Profile* (GOSIP), Draft, Version 2.0, April 1989

[HD89] C. Huitema, A. Doghri, *Defining Faster Transfer Syntaxes for the OSI Presentation Protocol*, ACM Computer Communication Review, Vol. 19, No. 5, Oct. 1989, pp. 44-55

[Hei90] J. Heinänen, *Review of ISO IP*, a contribution to the EC COSINE project, August 13, 1990

[Hei91] J. Heinänen, *Review of Backbone Technologies*, preprint, to be published in the RARE Symposium on High Speed Networking for Research in Europe, Jan. 24, 1991, Brussels

[HKK90] J. Harju, J. Koivisto, J. Kuittinen, J. Lahti, J. Malka, E. Ojanperä, J. Reilly, *C-VOPS Users' Manual*, Technical Research Centre of Finland, Telecommunications laboratory, 1990

[Hou89] R. Housley, *Authentication, Confidentiality, and Integrity Extensions to the XNS Protocol Suite*, ACM Security, Audit & Control Review, Vol. 7, No. 3, Fall 1989, pp. 17-24

[IEE90] Institute of Electrical and Electronic Engineers, Proposed Standard: *DQDB Subnetwork of a Metropolitan Area Network*, IEEE 802.6, P802.6/D14, July 13, 1990

[IM90] C. I'Anson, C. Mitchell, *Security Defects in CCITT Recommendation X.509 – The Directory Authentication Framework*, ACM Computer Communication Review, Vol. 20, No. 2, April 1990, pp. 30-34

[IS7498-1] ISO, Information Processing Systems, *Open Systems Interconnection Reference Model, Part 1: Basic Reference Model*, ISO 7498-1 (CCITT X.200), Geneva 1984

[IS7498-2] ISO, Information Processing Systems, *Open Systems Interconnection Reference Model, Part 2: Security Architecture*, ISO DIS 7498-2, July 19, 1988

[IS7498-3] ISO, Information Processing Systems, *Open Systems Interconnection Reference Model, Part 3: Naming and Addressing*, ISO DIS 7498-3, 1989

[IS7498-4] ISO, Information Processing Systems, *Open Systems Interconnection Reference Model, Part 4: Management Framework*, ISO DIS 7498-4, 1987

[IS7498/A1] ISO, Information Processing Systems, *Open Systems Interconnection, Connectionless Data Transmission*, ISO 7498-1/Add. 1, 1987

[IS7498/A2] ISO, Information Processing Systems, *Open Systems Interconnection, Multipeer Data Transmission*, ISO 7498-1/Add. 2

[IS7498/C1] ISO, Information Processing Systems, *Open Systems Interconnection, Technical Corrigendum 1*, ISO 7498-1/Cor. 1, 1988

[IS7776] *HDLC – Description of the X.25 LAPB-compatible DTE Data Link Procedures*, ISO 7776, 1986

[IS8072/A1] ISO, Information Processing Systems, *Open Systems Interconnection, Transport Service Definition, Addendum 1: Connectionless-mode Transmission*, ISO 8072/Add. 1

[IS8073/A2] ISO, Information Processing Systems, *Open Systems Interconnection, Connection Oriented Transport Protocol Specification, Addendum 2: Class 4 Operation over Connectionless Network Service*, ISO 8073/Add. 2

[IS8073] ISO, Information Processing Systems, *Open Systems Interconnection, Connection Oriented Transport Protocol Specification*, ISO 8073 (CCITT X.224), 1986

[IS8208] ISO, Information Processing Systems, *Open Systems Interconnection, X.25 Packet Level Protocol for Data Terminal, Equipment*, ISO 8208 (CCITT X.25), 1990

[IS8326/A3] ISO, Information Processing Systems, *Open Systems Interconnection, Basic Connection Oriented Session Service Definition, Addendum 3: Connectionless Session Service*, ISO 8326/DAD3, 1988

[IS8348/A1] ISO, Information Processing Systems, *Open Systems Interconnection, Network Service Definition, Addendum 1: Connectionless-mode Transmission*, ISO 8348/AD1, 1987

[IS8348] ISO, Information Processing Systems, *Open Systems Interconnection, Network Service Definition*, ISO 8348 (CCITT X.213), 1987

[IS8372] ISO, Information Technology, Security Techniques, *Modes of Operation for a 64-bit Block Cipher Algorithm*, ISO/IEC, ISO 8372, 1989

[IS8473] ISO, Information Processing Systems, *Open Systems Interconnection, Protocol for Providing the Connectionless-mode Network Service (Internetwork Protocol)*, ISO 8473

[IS8571-1] ISO, Information Processing Systems, *Open Systems Interconnection – File Transfer, Access and Management, Part 1: General Introduction*, ISO 8571-1, Oct. 1988

[IS8571-2] ISO, Information Processing Systems, *Open Systems Interconnection, File Transfer, Access and Management, Part 2: The Virtual Filestore Definition*, ISO 8571-2, Oct. 1988

[IS8571-4] ISO, Information Processing Systems, *Open Systems Interconnection, File Transfer, Access and Management, Part 4: The File Protocol Specification*, ISO 8571-4, Oct. 1988

[IS8602] ISO, Information Processing Systems, *Open Systems Interconnection, Protocol for Providing the Connectionless-mode Transport Service*, ISO 8602, Dec. 1987

[IS8649/A1] ISO, Information Processing Systems, *Open Systems Interconnection, Association Control Service Element, Addendum 1: Authentication*, ISO 8649/DAD1, 1989

[IS8649/A2] ISO, Information Processing Systems, *Open Systems Interconnection, Association Control Service Element, Addendum 2: Connectionless ACSE Service*, ISO 8649/DAD2, 1989

[IS8649/A3] ISO, Information Processing Systems, *Open Systems Interconnection, Association Control Service Element, Addendum 3: A-Context Management Service*, ISO 8649/PDAD3 (working draft), 1990

[IS8649] ISO, Information Processing Systems, *Open Systems Interconnection, Service Definition for the Association Control Service Element (ACSE)*, ISO 8649 (CCITT X.217), 1988

[IS8650/A1] ISO, Information Processing Systems, *Open Systems Interconnection, Peer Entity Authentication During Association Establishment*, ISO 8650/DAD1, 1989

[IS8650/A4] ISO, Information Processing Systems, *Open Systems Interconnection, Application Entity Titles*, ISO 8650/PDAD4 (working draft), 1990

[IS8650] ISO, Information Processing Systems, *Open Systems Interconnection, Protocol Specification for the Association Control Service Element (ACSE)*, ISO 8650 (CCITT X.227), 1988

[IS8802-1] ISO, Information Processing Systems, *Open Systems Interconnection, Local Area Networks, Part 1: Introduction*, ISO 8802-1

[IS8802-2] ISO, Information Processing Systems, *Open Systems Interconnection, Local Area Networks, Part 2: Logical Link Control*, ISO 8802-2

[IS8802-3] ISO, Information Processing Systems, *Open Systems Interconnection, Local Area Networks, Part 3: Carrier Sense Multiple Access with Collision Detection,Access Method and Physical Layer Specifications*, ISO 8802-3, 1989

[IS8802-5] ISO, Information Processing Systems, *Open Systems Interconnection, Local Area Networks, Part 5: Token Ring Access Method and Physical Layer Specifications*, ISO DIS 8802-5, 1990

[IS8807] *LOTOS – A Formal Description Technique Based on the Temporal Ordering of Observational Behaviour*, ISO 8807, 1989

[IS8822/A1] ISO, Information Processing Systems, *Open Systems Interconnection, Connection Oriented Presentation Service Definition, Addendum 1: Connectionless-mode Presentation Service*, ISO 8822/DAD1, 1989

[IS8823] ISO, Information Processing Systems, *Open Systems Interconnection, Connection Oriented Presentation Protocol Specification*, ISO 8823 (CCITT X.226), 1988

[IS8824/A1] ISO, Information Processing Systems, *Open Systems Interconnection, Specification of Abstract Syntax Notation One, Addendum 1: ASN.1 Extensions*, ISO 8824/DAD1 (CCITT X.208), 1988

[IS8824] ISO, Information Processing Systems, O*pen Systems Interconnection, Specification of Abstract Syntax Notation One*, ISO 8824 (CCITT X.208), 1987

[IS8825/A1] ISO, Information Processing Systems, *Open Systems Interconnection, Specification of Basic Encoding Rules for ASN.1, Addendum 1: ASN.1 Extensions*, ISO 8825/DAD1 (CCITT X.209), 1988

[IS8825] ISO, Information Processing Systems, *Open Systems Interconnection, Specification of Basic Encoding Rules for ASN.1*, ISO 8825 (CCITT X.209), 1987

[IS8831] ISO, Information Processing Systems, *Open Systems Interconnection, Job Transfer and Manipulation Concepts and Services*, ISO 8831, 1989

[IS8832] ISO, Information Processing Systems, *Open Systems Interconnection, Specification of the Basic Class Protocol for Job Transfer and Manipulation*, ISO 8832, 1989

[IS9040] ISO, Information Processing Systems, *Open Systems Interconnection, Virtual Terminal Service – Basic Class*, ISO 9040, 1988

[IS9041] ISO, Information Processing Systems, *Open Systems Interconnection, Virtual Terminal Protocol – Basic Class*, ISO 9041, 1989

[IS9066-1] ISO, Information Processing Systems, *Open Systems Interconnection, Reliable Transfer, Part 1: Model and Service Definition*, ISO 9066-1 (CCITT X.218), 1989

[IS9066-2] ISO, Information Processing Systems, *Open Systems Interconnection, Reliable Transfer, Part 2: Protocol Specification*, ISO 9066-2 (CCITT X.228), 1989

[IS9072-1] ISO, Information Processing Systems, *Open Systems Interconnection, Remote Operations, Part 1: Model, Notation and Service Definition*, ISO 9072-1 (CCITT X.219), 1989

[IS9072-2] ISO, Information Processing Systems, *Open Systems Interconnection, Remote Operations, Part 2: Protocol Specification*, ISO 9072-2 (CCITT X.229), 1989

[IS9314-1] *Fiber Distributed Data Interface, Part 1: Physical Layer Protocol*, ISO 9314-1, 1989

[IS9314-2] *Fiber Distributed Data Interface, Part 2: Medium Access Control*, ISO 9314-2, 1989

[IS9314-3] *Fiber Distributed Data Interface, Part 3: Physical Layer Medium Dependent*, ISO DIS 9314-3, 1990

[IS9314-4] *Fiber Distributed Data Interface, Part 3: Single Mode Fiber/Physical Layer Medium Dependent*, ISO DP 9314-4, 1990

[IS9314-5] *Fiber Distributed Data Interface, Part 5: Hybrid Ring Control (FDDI II)*, ISO DP 9314-5, 1990

[IS9545/A1] ISO, Information Processing Systems, *Open Systems Interconnection, Application Layer Structure, Addendum 1: Connectionless Operation*, ISO DIS 9545/PDAD1 (working draft), 1989

[IS9545] ISO, Information Processing Systems, *Open Systems Interconnection, Application Layer Structure*, ISO DIS 9545 (CCITT X.200), 1989

[IS9549] ISO, Information Processing Systems, *Open Systems Interconnection, Connectionless Session Protocol*, ISO DIS 9549, 1988

[IS9576] ISO, Information Processing Systems, *Open Systems Interconnection, Connectionless Presentation Protocol Specification*, ISO DIS 9576, 1989

[IS9579-1] ISO, Information Processing Systems, *Open Systems Interconnection, Remote Database Access, Part 1: General Model, Services and Protocol*, ISO DP 9579, 1990

[IS9579-2] ISO, Information Processing Systems, *Open Systems Interconnection, Remote Database Access, Part 2: SQL Specification*, ISO DP 9579, 1990

[IS9594-1] ISO, Information Processing Systems, *Open Systems Interconnection, The Directory, Part 1: Overview of Concepts, Models and Services*, ISO 9594-1 (CCITT X.500), Dec. 1988

[IS9594-8] ISO, Information processing systems, *Open Systems Interconnection, The Directory, Part 8: Authentication framework*, ISO 9594-8 (CCITT X.509), Dec. 1988

[IS9595] ISO, Information Processing Systems, *Open Systems Interconnection, Common Management Information Service Definition, Part 1: Overview*, ISO DIS 9595, 1989

[IS9596] ISO, Information Processing Systems, *Open Systems Interconnection, Common Management Information Protocol (CMIP) Specification*, ISO DIS 9596, 1989

[IS9796] ISO, Information Technology, Security Techniques, *A Signature Algorithm for Short Messages*, ISO DP 9796, 1990

[IS9797] ISO, Information Technology, Security Techniques, *A Data Integrity Mechanism*, ISO DP 9797, 1990

[IS9798-1] ISO, Information Technology, Security Techniques, *Entity Authentication Mechanisms, Part 1: General Model for Entity Authentication Mechanisms*, ISO/IEC DIS 9798-1, 1990

[IS9798-2] ISO, Information Technology, Security Techniques, *Entity Authentication Mechanisms, Part 2: Entity Authentication Using Symmetric Key Techniques*, ISO/IEC DIS 9798-2, 1990

[IS9798-3] ISO, Information Technology, Security Techniques, *Entity Authentication Mechanisms, Part 3: Entity Authentication Using a Public Key Algorithm*, ISO/IEC CD 9798-3, 1990

[IS9799] ISO, Information Processing Systems, *Peer Entity Authentication Using a Public-Key Algorithm with a Two-Way Handshake*, ISO DP 9799, 1988

[IS10000-1] *International Standardized Profiles, Part 1: Taxonomy Framework*, ISO TR 10000-1, 1990

[IS10000-2] *International Standardized Profiles, Part 2: Taxonomy of Profiles*, ISO TR 10000-2, 1990

[IS10035] ISO, Information Processing Systems, *Open Systems Interconnection, Connectionless ACSE Protocol Specification*, ISO DIS 10035, 1989

[IS10040] ISO, Information Processing Systems, *Open Systems Interconnection, Systems Management Overview*, ISO/IEC DP 10040 (CCITT X.701), 1990, June 16, 1990

[IS10116] ISO, Information Technology, Security Techniques, *Modes of Operation for an N-bit Block Cipher Algorithm*, ISO/IEC DIS 10116, 1990

[IS10118-1] ISO, Information Technology, Security Techniques, *Hash Functions for Digital Signatures, Part 1: General*, ISO/IEC CD 10118-1, June 21, 1990

[IS10118-2] ISO, Information Technology, Security Techniques, *Hash Functions for Digital Signatures, Part 2: Hash Functions using a Symmetric Block Cipher Algorithm*, ISO/IEC CD 10118-2, June 21, 1990

[IS10164-7] ISO, Information Processing Systems, *Open Systems Interconnection, Systems Management, Part 7: Security Alarm Reporting Function*, ISO/IEC DIS 10164-7 (CCITT X.736), Soeul, May 21-22, 1990

[IS10164-8] ISO, Information Processing Systems, *Open Systems Interconnection, Systems Management, Part 8: Security Audit Trail Function*, ISO/IEC DIS 10164-8 (CCITT X.740), Soeul, June 1990

[IS10164-9] ISO, Information Processing Systems, *Open Systems Interconnection, Systems Management, Part 9: Objects and Attributes for Access Control*, ISO/IEC DIS 10164-9 (CCITT X.741), Soeul, June 1990

[IS10165-1] ISO, Information Processing Systems, *Open Systems Interconnection, Structure of Management Information, Part 1: Management Information Model*, ISO/IEC DIS 10165-1 (CCITT X.720), Paris, Jan. 1990

[IS10167] *Guidelines for the Application of Estelle, LOTOS, and SDL*, ISO DTR 8807, 1990

[IS10181-1] ISO, Information Technology, *OSI Security Model, Part 1: Security Framework*, ISO DP 10181-1

[IS10181-2] ISO, Information Technology, *OSI Security Model, Part 2: Authentication Framework*, ISO DP 10181-1

[ISO90a] ISO, Information Processing Systems, *Proposed Draft for End System to End System Security Protocol*, 2nd version, ISO/IEC JTC1/SC6, 27 July, 1990

[ISO90b] ISO, Information Processing Systems, *Appendix B to UK Proposal for Network Layer End System to End System Security Protocol*, ISO/IEC JTC1/SC6, July 27, 1990

[ISO90c] ISO, Information Processing Systems, *OSI Upper Layers Security Model*, fourth working draft, ISO/IEC JTC1/SC21 N5447, ISO/IEC JTC1/SC21/WG6 and CCITT Question 19/VII Collaborative ad hoc Meeting on Security in Berlin, Oct. 30, 1990

[ISO90d] ISO, Information Processing Systems, *Working Draft Integrity Framework*, ISO/IEC JTC1/SC21 N5047, July 1990

[ISO90e] ISO, Information Processing Systems, *Working Draft Non-Repudiation Framework*, ISO/IEC JTC1/SC21 N5046, July, 1990

[ISO90f] D. Kim, Y. Kim, H. Shin, H. Choi, T. Park, *Proposal of a Common Security Service Element in the OSI Application Layer*, ISO/IEC JTC1/SC21 N5002 Attachment, Sep. 1990

[ITS90] *Information Technology Security Evaluation Criteria (ITSEC), Harmonised Criteria of France – Germany – the Netherlands – the United Kingdom*, Draft, May 2, 1990

[Kar86] A. Karila, *Portable Protocol Development and Run-Time Environment*, Licentiate's thesis, Helsinki University of Technology, Apr. 1986

[Kar87] A. Karila, *C-VOPS – A Portable Environment for Protocol Development and Implementation*, Proceedings of IFIP TC6 International Conference on Information Network and Data Communication, Sweden, May 11-14, 1986, North Holland, 1987, pp. 19-34

[Kat90] Dave Katz, *The Use of Connectionless Network Layer Protocols over FDDI Networks*, ACM Computer Communication Review, Vol. 20, No. 3, July 1990, pp. 32-45

[Ken89] S. Kent, *Comments on "Security Problems in the TCP/IP Protocol Suite"*, ACM Computer Communication Review, Vol. 19, No. 3, July 1989, pp. 10-19

[KHA90] A. Karila, J. Harju, I. Airaksinen, M. Sievänen, *Inserting Security Mechanisms into OSI Layers – a Case Study*, Lappeenranta University of Technology, 1990

[KLP83] A. Karila, K. Lång, P. Pulli, Tietoliikennesovittimen toiminta ja rakenne, (*Functional Specification and Structure of a Transport Layer Gateway*, in Finnish), Technical Research Centre of Finland, Research Notes 252, 1983, 94 p.

[KM91] J. Koivisto, J. Malka, *DVOPS – An Object-Oriented Approach to Distributed Computation*, to be presented in the Usenix'91 conference, Technical Research Centre of Finland, January 1991

[Koi87] J. Koivisto, Sovelluskerroksen tietoyksiköiden automaattinen käsittely standardikuvauskielen perusteella, (*Automatic Handling of Application Layer Data Units Based on a Standard Description Language*, in Finnish), Master's Thesis, Helsinki University of Technology, Department of Technical Physics, 1987

[Lan81] C. Landwehr, *Formal Models for Computer Security*, ACM Computing Surveys, Vol. 13, No. 3, Sept. 1981, pp. 247-278

[LLH89] C.-S.Laih, J.-Y. Lee, L. Harn, Y.-K. Su, *Linearly Shift Knapsack Public-Key Cryptosystem*, IEEE Journal on Selected Areas in Communications, Vol. 7, No. 4, May 1989, pp. 534-547

[LS90] W.-P. Lu, M. Sundareshan, *A Model for Multilevel Security in Computer Networks*, IEEE Transactions on Software Engineering, Vol. 16, No. 6, June 1990, pp. 647-659

[LT90] L. Landweber, M. Tasman, *An ISO TP4-TP0 Gateway*, ACM Computer Communication Review, Vol. 20, No. 2, April 1990, pp. 16-21

[Mas88] J. Massey, *An Introduction to Contemporary Cryptology*, Proceedings of the IEEE, Vol. 76, No. 5, May 1988, pp. 533-549

[Mer89] R. Merkle, *One Way Hash Functions and DES*, Proceedings of Crypto'89, Santa Barbara, October, 1989

[MH78] R. Merkle, M. Hellman, *Hiding Information and Signatures in Trapdoor Knapsack*, IEEE Transactions on Information Theory, Vol. IT-24, Sep. 1978, pp. 525-530

[Mit90] C. Mitchell, *OSI and X.400 Security*, Telecommunications, May 1990, pp. 49-54

[MM83] R. DeMillo, M. Merritt, *Protocols for Data Security*, IEEE Computer Magazine, Feb. 1983, pp. 39-51

[MOI90] S. Miyaguchi, K. Ohta, M. Iwata, *128-bit hash function (N-Hash)*, proceedings of SECURICOM90, Paris, March 1990

[Moo88] J. Moore, *Protocol Failures in Cryptosystems*, Proceedings of the IEEE, Vol. 76, No. 5, May 1988, pp. 594-602

[MT79] R. Morris, K. Thompson, *Password Security: A Case History*, Communications of the ACM, Vol. 22, Nov. 1979, pp. 594-597

[MWR89] C. Mitchell, M. Walker, D. Rush, *CCITT/ISO Standards for Secure Message Handling*, IEEE Journal on Selected Areas in Communications, Vol. 7, No. 4, May 1989, pp. 517-524

[NCS87] *Trusted Network Interpretation of the Trusted Computer Systems Evaluation Criteria*, NCSG-TG-005, Version 1, National Computer Security Center, USA July 31, 1987

[Nel88] R. Nelson, *SDNS Services and Architecture*, 1988

[Nes90] D. Nessett: *A Critique of the Burrows, Abadi and Needham Logic*, ACM Operating Systems Review, 1990

[Nok90] *How to Use CASN Compiler for Implementation of a Virtual Task in CVOPS*, Ver. 1.0, Technical Report, Nokia Research Centre, 1990

[NS78] R. Needham, R. Schroeder, *Using Encryption for Authentication in Large Networks of Computers*, Communications of the ACM, Vol. 21, No. 12, Dec. 1978, pp. 993-999

[NS87] R. Needham, R. Schroeder, *Authentication Revisited*, ACM Operating Systems Review, Vol. 21, No. 1, Jan. 1987, p. 7

[NS89] K. Nakao, K. Suzuki, *Proposal on a Secure Communications Service Element (SCSE) in the OSI Application Layer*, IEEE Journal on Selected Areas in Communications, Vol. 7, No. 4, May 1989, pp. 505-516

[OR87] D. Otway, O. Rees, *Efficient and Timely Mutual Authentication*, ACM Operating Systems Review, Vol. 21, No. 1, Jan. 1987, pp. 8-10

[OT89] E. Okamoto, K. Tanaka, *Key Distribution System Based on Identification Information*, IEEE Journal on Selected Areas in Communications, Vol. 7, No. 4, May 1989, pp. 481-485

[Par90] G. Parulkar, *The Next Generation of Internetworking*, ACM Computer Communication Review, Vol. 20, No. 1, Jan. 1990, pp. 18-43

[Pat87] W. Patterson: *Mathematical Cryptology for Computer Scientists and Mathematicians*, Rowman & Littlefield, 1987

[PK79] G. Popek, C. Kline, *Encryption and Secure Computer Networks*, ACM Computing Surveys, Vol. 11, No. 4, Dec. 1979, pp. 331-356

[PK90] D. Piscitello, M. Kramer, *Internetworking Using Switched Multimegabit Data Service in TCP/IP Environments*, ACM Computer Communication Review, Vol. 20, No. 3, July 1990, pp. 62-71

[PSI90] PSI Inc., *ISODE 6.0 Announcement*, Jan. 1990

[QG90] J.-J. Quisquater, L. Guillou, *How to Explain Zero-Knowledge Protocols to Your Children*, 1990

[RFC81a] *Internet Protocol*, RFC 791, Sep. 1981

[RFC81b] *Transmission Control Protocol*, RFC 793, Sep. 1981

[RFC89a] J. Linn, *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encipherment and Authentication Procedures*, RFC 1113, 1989

[RFC89b] S. Kent, J. Linn, *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management*, RFC 1114, 1989

[RFC89c] J. Linn, *Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes and Identifiers*, RFC 1115, 1989

[RHF90] F. Ross, J. Hamstra, R. Fink, *FDDI – A LAN Among MANs*, ACM Computer Communication Review, Vol. 20, No. 3, July 1990, pp. 16-31

[Riv90] R. Rivest, *The MD4 Message Digest Algorithm* (Version 2/17/90, Revised), ISO/IEC JTC1/SC 27/WG20.2 N193, April 4, 1990

[Ros90] M. Rose, *The Open Book, OSI – a Practical Perspective*, Prentice Hall, 1990

[RSA78] R. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, Vol. 21, No. 2, Feb. 1978, pp. 120-126

[Rue90] R. Rueppel, *A Formal Approach to Security Architectures*, preprint of paper to be presented in Eurocrypt'91, April 8 – 11, 1991, Brighton, England, dated Dec. 17, 1990

[Rue91] Lecture by and discussion with Rainer Rueppel at Helsinki University, March 18, 1991

[SDN89a] SDNS, *Secure Data Network Systems, Security Protocol 3 (SP3)*, Specification SDN.301, Revision 1.4, Feb. 28, 1989

[SDN89b] SDNS, *Secure Data Network Systems, Security Protocol 4 (SP4)*, Specification SDN.401, Revision 1.3, May 2, 1989

[SEG90] Security EDIFACT Group, *Security Framework for EDIFACT*, MD4.B, Document 1.19, v. 1.0, (draft), 7 June, 1990

[Sha49] C. Shannon, *Communication Theory of Secrecy Systems*, Bell System Technical Journal, Vol. 28, Oct. 1949, pp. 656-715

[Sha85] A. Shamir, *Identity-Based Cryptosystem and Signature Scheme*, Advances in Cryptology: Proceedings of Crypto'84, Springer, Berlin, 1985, pp. 47-53

[Sim79] G. Simmons, *Symmetric and Asymmetric Encryption*, ACM Computing Surveys, Vol. 11, No. 4, Dec. 1979, pp. 305-330

[Sim84] G. Simmons, *Authentication Theory/Coding Theory*, Advances in Cryptology, Proceedings of Crypto '84, Springer, New York, 1985, pp. 411-431

[Sim88] G. Simmons, *A Survey of Information Authentication*, Proceedings of the IEEE, Vol. 76, No. 5, May 1988, pp. 603-620

[Sim89] G. Simmons, *A Protocol to Provide Verifiable Proof of Identity and Unforgeable Transaction Receipts*, IEEE Journal on Selected Areas in Communications, Vol. 7, No. 4, May 1989, pp. 435-447

[SM87] A. Shimizu, S. Miyaguchi, *Fast Data Encipherment Algorithm FEAL*, Proceedings of Eurocrypt'87, April 1987

[SNC88] J. Steiner, C. Neuman, J. Schiller, *Kerberos: An Authentication Service for Open Network Systems*, Project Athena, MIT, 1988

[TED89] The TEDIS – EDI Security Workshop, *Security in a Multi-Owner System*, Brussels, June 20-21, 1989

[TED90a] *TEDIS Programme 1988-1989*, Activity Report, Brussels, July 25, 1990

[TED90b] *Digital Signatures in EDIFACT*, a TEDIS programme report prepared by CRYPTOMATHIC A/S, final version, Nov. 29, 1990

[TTY88] Kari Lång (editor), Tietotekniikan kehittämisohjelma FINPRIT: Tietotekniikan yhdentäminen, *final report (concise version) of the FINPRIT research program* (in Finnish), TEKES, Helsinki, 1988

[VK83] V. Voydock, S. Kent, *Security Mechanisms in High-Level Network Protocols*, Computing Surveys, Vol. 15, June 1983, pp. 135-171

[Wal89] S. Walker, *Network Security: The Parts of the Sum*, Proceedings of the 1989 IEEE Computer Society Symposium on Security and Privacy, Oakland, 1989, pp. 2-9

[Woo87] C. Wood & al., *Computer Security: A Comprehensive Controls Checklist*, Wiley, New York, 1987

[Woo90] C. Wood, *Principles of Secure Information Systems Design*, Computers & Security, Vol. 9, No. 1, Feb. 1990, pp. 13-24

[X.21] *Interface between data terminal equipment (DTE) and data circuit-terminating-equipment (DCE) for synchronous operation on public data networks*, CCITT Recommendation X.21, Blue Book Vol. VIII, Fascicle VIII.2, Geneva, 1989

[X.25] *Interface between data terminal equipment (DTE) and data circuit-terminating-equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit*, CCITT Recommendation X.25 (see also ISO 7776 and ISO 8208), Blue Book Vol. VIII, Fascicle VIII.2, Geneva, 1989

[X.200] *Reference Model of Open Systems Interconnection for CCITT Applications*, CCITT Recommendation X.200 (ISO 7498), Blue Book Vol. VIII, Fascicle VIII.4, Geneva, 1989

[X.224] *Transport Protocol Specification*, CCITT Recommendation X.224 (ISO 8073), Blue Book Vol. VIII, Fascicle VIII.5, Geneva, 1989

[X.208] *Specification of Abstract Syntax Notation One (ASN.1)*, CCITT Recommendation X.208 (ISO 8824, ISO 8824/AD1), Blue Book Vol. VIII, Fascicle VIII.4, Geneva, 1989

[X.209] *Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*, CCITT Recommendation X.208 (ISO 8825, ISO 8825/AD1), Blue Book Vol. VIII, Fascicle VIII.4, Geneva, 1989

[X.210] *Layer Service Definition Conventions*, CCITT Recommendation X.210 (ISO TR 8509), Blue Book Vol. VIII, Fascicle VIII.4, Geneva, 1989

[X.213] *Network Service Definition for Open Systems Interconnection for CCITT Applications*, CCITT Recommendation X.213 (ISO 8348, ISO 8348/AD2, ISO 8348/AD3), Blue Book Vol. VIII, Fascicle VIII.4, Geneva, 1989

[X.217] *Association Control Service Definition for Open Systems Interconnection for CCITT Applications*, CCITT Recommendation X.217 (ISO 8649), Blue Book Vol. VIII, Fascicle VIII.4, Geneva, 1989

[X.218] *Reliable Transfer: Model and Service Definition*, CCITT Recommendation X.218 (ISO 9066-1), Blue Book Vol. VIII, Fascicle VIII.4, Geneva, 1989

[X.219] *Remote Operations: Model, Notation and Service Definition*, CCITT Recommendation X.219 (ISO 9072-1), Blue Book Vol. VIII, Fascicle VIII.4, Geneva, 1989

 © Arto Karila, 1991

[X.224] *Transport Protocol Specification*, CCITT Recommendation X.224 (ISO 8073), Blue Book Vol. VIII, Fascicle VIII.5, Geneva, 1989

[X.227] *Protocol Specification for the Association Control Service Element*, CCITT Recommendation X.227 (ISO 8650), Blue Book Vol. VIII, Fascicle VIII.5, Geneva, 1989

[X.228] *Protocol Specification for the Reliable Transfer Service Element*, CCITT Recommendation X.228 (ISO 9066-2), Blue Book Vol. VIII, Fascicle VIII.5, Geneva, 1989

[X.229] *Protocol Specification for the Remote Operations Service Element*, CCITT Recommendation X.229 (ISO 9072-2), Blue Book Vol. VIII, Fascicle VIII.5, Geneva, 1989

[X.400] *Message Handling, Part 1: System and Service Overview*, CCITT Recommendation X.400, Blue Book Vol. VIII, Fascicle VIII.7, Geneva, 1989

[X.500] *The Directory – Overview of Concepts, Models, and Services*, CCITT Recommendation X.500 (Melbourne 1988, ISO 9594-1), Blue Book Vol. VIII, Fascicle VIII.8, Geneva, 1989

[X.509] *The Directory, Part 8: Authentication Framework*, CCITT Recommendation X.509 (Melbourne 1988, ISO 9594-1), Blue Book Vol. VIII, Fascicle VIII.8, Geneva, 1989

[Z.100] *Functional Specification and Description Language (SDL)*, CCITT Recommendations Z.100 and Z.110, Blue Book Vol. X, Fascicle X.1, Geneva, 1989

[ZE90] R. Zamparo, G. Endersz, *Architecture and Testbed Realization of Security Services in an OSI Communication Environment*, preprint of presentation at ICCC in Nov. 1990 at New Delhi, Sep. 4, 1990