

Bibliografía

- [1] M. Abadi. On SDSI's linked local name spaces. *Journal of Computer Security*, 6(1-2):3–21, 1998.
- [2] M. Abadi and R. Needham. Prudent engineering practice for cryptographic protocols. *IEEE Transactions on Software Engineering*, 1(22):6–15, January 1996.
- [3] A. Abdul-Rahman and S. Hailes. A distributed trust model. In *New Security Paradigms*, pages 48–60, 1997.
- [4] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. G. Neumann, R. L. Rivest, J. I. Schiller, and B. Schneier. The Risks Of Key Recovery, Key Escrow, And Trusted Third-Party Encryption, 1998.
- [5] M. D. Abrams. Renewed understanding of access control policies. In *Proceedings 16th National Computer Security Conference*, pages 87–95, 1993.
- [6] C. Adams, P. Cain, D. Pinkas, and R. Zuccherato. *Time-Stamp Protocol (TSP)*, 2001. Request For Comments (RFC) 3161.
- [7] C. Adams and S. Farrell. *Internet X.509 Public Key Infrastructure Certificate Management Protocols*, 1999. Request For Comments (RFC) 2510.
- [8] S. Ajmani, D. E. Clarke, C. Moh, and S. Richman. ConChord: Cooperative SDSI Certificate Storage and Name Resolution. In *Proceedings of 1st International Workshop on Peer-to-peer Systems*, volume 2429 of *Lecture Notes in Computer Science*, pages 141–154. Springer, March 2002.
- [9] A. O. Alan, P. Freier, and P. C. Kocher. *The SSL Protocol Version 3.0*, 1996. Internet Draft.
- [10] P. Alterman, R. Weiser, M. Gettes, K. Stillson, D. Blanchard, J. Fisher, R. Brentrup, and E. Norman. Report: EDUCAUSE NIH PKI Interoperability Pilot Project. In *Proceedings of 1st Annual PKI Research Workshop*, pages 177–193, April 2002.
- [11] American Bankers Association. *X9.55-199x: Enhanced management controls using digital signatures and attribute certificates*, June 1997.

- [12] American National Standards Institute. *ANSI X9.57: American National Standard, Public Key Cryptography for the Financial Services Industry: Certificate Management*, 1997.
- [13] R. Anderson and R. Needham. Robustness principles for public key protocols. In *Proceedings International Conference on Advances in Cryptology (CRYPTO 95)*, volume 963 of *Lecture Notes in Computer Science*, pages 236–247. Springer, 1995.
- [14] T. Aura. Fast access control decisions from delegation certificate databases. In *Proceedings of 3rd Australasian Conference on Information Security and Privacy ACISP'98*, volume 1428 of *Lecture Notes in Computer Science*, pages 284–295. Springer, July 1998.
- [15] T. Aura. On the structure of delegation networks. In *Proc. 11th IEEE Computer Security Foundations Workshop*, pages 14–26, 1998.
- [16] T. Aura. Distributed access-rights managements with delegations certificates. In *Secure Internet Programming: Security Issues for Distributed and Mobile Objects*, volume 1603 of *Lecture Notes in Computer Science*, pages 211–235. Springer, 1999.
- [17] T. Aura and C. Ellison. Privacy and Accountability in Certificate Systems. Technical Report HUT-TCS-A61, Helsinki University of Technology, 2000.
- [18] T. Austin. *PKI: A Wiley Tech Brief*. John Wiley and Sons, 2001.
- [19] O. Bandmann, M. Dam, and B. Sadighi. Constrained Delegations. In *Proceedings of 2002 IEEE Symposium on Security and Privacy*, pages 131–142, 2002.
- [20] O. Bandmann, B. Sadighi, and O. Olsson. *Decentralized management of access control*. Swedish Institute of Computer Science, 2001. Internal Project Report.
- [21] M. Barbacci, M. Klein, T. H. Longstaff, and C. B. Weinstock. Quality attributes. Technical Report CMU/SEI-95-TR-021, Carnegie Mellon University, 1995.
- [22] D. Bell and L. LaPadula. Secure computer systems: unified exposition and multics interpretation. Technical Report ESD-TR-75-306, The Mitre Corporation, 1976.
- [23] A. Belokosztolszki and K. Moody. Meta-Policies for Distributed Role-Based Access Control Systems. In *Proceedings of 3rd International Workshop on Policies for Distributed Systems and Networks*. IEEE Press, June 2002.
- [24] S. Bennett, S. McRobb, and R. Farmer. *Object-Oriented Systems Analysis and Design*. McGraw Hill, 1999.
- [25] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis. *The KeyNote Trust Management System Version 2*, September 1999. Request For Comments (RFC) 2704.

- [26] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis. The role of trust management in distributed systems security. In *Secure Internet Programming: Security Issues for Distributed and Mobile Objects*, volume 1603 of *Lecture Notes in Computer Science*, pages 185–210. Springer, 1999.
- [27] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized Trust Management. In *Proceedings of the Symposium on Security and Privacy*, pages 164–173, 1996.
- [28] M. Blaze, J. Feigenbaum, and P. Resnick. Managing Trust in an Information Labeling System. In *Proceedings of European Transactions on Telecommunications*, pages 491–501, 1997.
- [29] M. Blaze, J. Feigenbaum, and M. Strauss. Compliance Checking in the PolicyMaker Trust Management System. In *Proceedings of the Financial Cryptography'98*, volume 1465 of *Lecture Notes in Computer Science*, pages 254–274. Springer, 1998.
- [30] M. Blaze, J. Ioannidis, and A. D. Keromytis. Trust management and network layer security protocols. In *Security Protocols Workshop*, pages 103–118, 1999.
- [31] T. Bray, J. Paoli, and C. M. Sperberg. *Extensible Markup Language (XML) 1.0*, February 1998. W3C Recommendation.
- [32] A. Buldas and P. Laud. New Linking Schemes for Digital Timestamping. In *Proceedings of First International Conference on Information Security and Cryptology*, pages 3–14, 1998.
- [33] J. A. Bull, L. Gong, and K. R. Sollins. Towards security in an open systems federation. In *European Symposium on Research in Computer Security (ESORICS)*, pages 3–20, 1992.
- [34] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM Transactions on Computer Systems*, 1(8):18–36, February 1990.
- [35] A. Caja, O. Cánovas, F. J. García, J. Gil, A. F. Gómez, E. Martínez, and G. Martínez. Experiencia piloto de certificación en la Universidad de Murcia. *Boletín de la Red Nacional de I+D, RedIris*, (46):39–45, December 1998.
- [36] A. Caja, O. Cánovas, F. J. García, J. Gil, A. F. Gómez, E. Martínez, and G. Martínez. Providing security to university environment communications. In *Proceedings of the TERENA NORDUnet Networking Conference '99*, Lund (Sweden), June 1999.
- [37] J. Callas, L. Donnerhake, H. Finney, and R. Thayer. *OpenPGP Message Format*, 1998. Request For Comments (RFC) 2440.
- [38] CCITT. *Recommendation X.500: The directory-overview of concepts, models and services*, 1988.

- [39] CEN. *Inter-sector Electronic Purse, Part 2: Security Architecture*, 1546 edition, January 1996.
- [40] D. W. Chadwick and A. Otenko. RBAC Policies in XML for X.509 Based Privilege Management. In *Proceedings of IFIP SEC 2002*, pages 39–53, May 2002.
- [41] D. W. Chadwick and A. Otenko. The PERMIS X.509 Role Based Privilege Management Infrastructure. In *Proceedings of SACMAT 2002*, pages 135–140. ACM, June 2002.
- [42] P. Cheng and R. Glenn. *Tests Cases for HMAC-MD5 and HMAC-SHA-1*, September 1997. Request For Comments (RFC) 2202.
- [43] S. Chokhani and W. Ford. *Certificate Policy and Certification Practices Framework*, March 1999. Request For Comments (RFC) 2527.
- [44] Y. Chu, J. Feigenbaum, B. LaMacchia, P. Resnick, and M. Strauss. REFEREE: Trust management for Web applications. *Computer Networks and ISDN Systems*, 29(8–13):953–964, 1997.
- [45] Dwaine Clarke. SPKI/SDSI HTTP Server and Certificate Chain Discovery in SPKI/SDSI . Master’s thesis, M.I.T., September 2001.
- [46] O. Cánovas, F. J. García, A. F. Gómez, and G. Martínez. Aplicación de la firma dual para la corrección de exámenes en el entorno web. *Boletín de la red nacional de I+D, Rediris*, (54):65–69, November 2000.
- [47] O. Cánovas and A. F. Gómez. AMBAR Protocol: Access Management Based on Authorization Reduction. In *Proceedings of the International Conference on Information and Communications security (ICICS 2001)*, volume 2229 of *Lecture Notes in Computer Science*, pages 376–380. Springer Verlag, November 2001.
- [48] O. Cánovas and A. F. Gómez. A Distributed Credential Management System for SPKI-Based Delegation Systems. In *Proceedings of 1st Annual PKI Research Workshop*, pages 65–76, 2002.
- [49] O. Cánovas and A. F. Gómez. Gestión Distribuida de Certificados Digitales SPKI. In *Actas de la VII Reunión Española de Criptología y Seguridad de la Información*, pages 137–150, September 2002.
- [50] O. Cánovas, A. F. Gómez, G. López, and G. Martínez. Dynamic Virtual Private Networks. In *Proceedings of EUROMEDIA 2000*, pages 317–321, 2000.
- [51] O. Cánovas, A. F. Gómez, and G. Martínez. A PKI Scenario for High-Security Communications: Re-issued Certificates. In *Proceedings of the e-Business and e-Work 2000 Conferences*, pages 225–231, 2000.

- [52] O. Cánovas, A. F. Gómez, and G. Martínez. A system for self-revocation of digital certificates. In *Proceedings of the Second International Network Conference*, pages 289–296, 2000.
- [53] O. Cánovas, A. F. Gómez, and G. Martínez. PISCIS: Comercio Electrónico Basado en Infraestructuras de Certificación Avanzadas y Sistemas de Tarjeta Inteligente. In *Actas del I Simposio Español de Negocio Electrónico*, pages 201–216, 2001.
- [54] O. Cánovas, A. F. Gómez, H. Martínez, and G. Martínez. Different Smartcard-based Approaches to Physical Access Control. In *Proceedings of Infrastructure Security Conference 2002*, volume 2437 of *Lecture Notes in Computer Science*, pages 214–226. Springer Verlag, October 2002.
- [55] Wedgetail Communications. *JCSI - Java Crypto and Security Implementation*. World Wide Web, <http://www.wedgetail.com/jcsi/index.html>, 2002.
- [56] Intel Corporation. *Common Data Security Architecture (CDSA)*. World Wide Web, <http://developer.intel.com/ial/security>, 2002.
- [57] E. Dawson, J. López, J. A. Montenegro, and E. Okamoto. A new design of Privilege Management Infrastructure for organizations using outsourced PKI. In *Proceedings of Information Security Conference 2002*, volume 2433 of *Lecture Notes in Computer Science*, pages 136–149. Springer, 2002.
- [58] Fábrica Nacional de Moneda y Timbre. *Proyecto CERES*. World Wide Web, <http://www.cert.fnmt.es>, 2002.
- [59] T. Dierks and C. Allen. *The TLS Protocol Version 1.0*, January 1999. Request For Comments (RFC) 2246.
- [60] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.
- [61] D. D. Downs, J. R. Rub, K. C. Kung, and C. S. Jordan. Issues in discretionary access control. In *Proceedings of IEEE Symposium on Security and Privacy*, pages 208–218. IEEE Press, April 1985.
- [62] J. Dávila and L. F. Pardo. Diseño y realización de un servicio de sellado digital de tiempo. *Boletín de la Red Nacional de I+D, Rediris*, (46):31–38, November 1998.
- [63] J. G. Dyer, M. Lindemann, R. Perez, R. Sailer, L. van Doorn, S. W. Smith, and S. Weingart. Building the IBM 4758 Secure Coprocessor. *IEEE Computer*, 34(10):57–66, 2001.
- [64] D. Eastlake and O. Gudmundsson. *Storing Certificates in the Domain Name System (DNS)*, March 1999. Request For Comments (RFC) 2538.

- [65] G. Elcock. Web-based user interface for a Simple Distribute Security Infrastructure (SDSI). Master's thesis, M.I.T., June 1997.
- [66] J. E. Elien. Certificate discovery using SPKI/SDSI 2.0 certificates. Master's thesis, M.I.T., May 1998.
- [67] C. Ellison. Improvements on Conventional PKI Wisdom. In *Proceedings of 1st Annual PKI Research Workshop*, pages 165–176, April 2002.
- [68] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen. *Simple Public Key Certificate*. IETF Internet Draft, draft-ietf-spki-cert-structure-06.txt edition, July 1999.
- [69] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen. *SPKI certificate theory*, September 1999. Request For Comments (RFC) 2693.
- [70] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen. *SPKI Examples*. IETF Internet Draft, draft-ietf-spki-cert-examples-01.txt edition, March 1999.
- [71] C. Ellison and B. Schneier. Ten risks of PKI: What you're not being told about public key infrastructure. *Computer Security Journal*, 16(1):1–7, 2000.
- [72] EuroPKI. *EuroPKI Top Level Certification Authority*. World Wide Web, <http://www.europki.org>, 2002.
- [73] S. Farrel. *TLS extensions for AttributeCertificate based authorization*. IETF Internet Draft, draft-ietf-tls-attr-cert-00.txt edition, February 1998.
- [74] S. Farrel and R. Housley. *An Internet Attribute Certificate Profile for Authorization*, April 2002. Request for Comments (RFC) 3281.
- [75] D. F. Ferraiolo, J. A. Cugini, and D. R. Kuhn. Role-Based Access Control (RBAC): Features and Motivations. In *Proceedings Annual Security Applications Conference*, pages 241–248. IEEE Press, 1995.
- [76] J. Ferrari, S. Poh, R. Mackinnon, and L. Yatawara. *Smart Cards: A Case Study*. IBM RedBooks, <http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg245239.pdf>, October 1998.
- [77] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, and T. Berners-Lee. *Hypertext Transfer Protocol – HTTP/1.1*, January 1997. Request for Comments (RFC) 2068.
- [78] IAIK Institute for applied information processing and communication. *IAIK JCE*. World Wide Web, <http://jce.iaik.tugraz.at/>, 2002.
- [79] W. Ford and M. S. Baum. *Secure Electronic Commerce*. Prentice Hall, second edition, 2001.

- [80] B. Fox and B. LaMacchia. Online certificate status checking in financial transactions: the case for re-issuance. In *Proceedings of Financial Cryptography '98*, volume 1648 of *Lecture Notes in Computer Science*, pages 104–117. Springer-Verlag, 1998.
- [81] M. Fredette. An implementation of SDSI-the Simple Distributed Security Infrastructure. Master's thesis, M.I.T., May 1997.
- [82] D. Gambetta. Can we trust trust? In *Trust: Making and Braking Cooperative Relations*, pages 213–237, 1990.
- [83] B. Gassend, G. E. Suh, D. Clarke, M. van Dijk, and S. Devadas. Caches and merkle trees for efficient memory authentication. In *Proceedings of Ninth International Symposium on High Performance Computer Architecture*, 2003. To be published.
- [84] M. Gil and F. Pereñíguez. Extension de una PKI para dar soporte a certificados de atributo X.509. Master's thesis, Universidad de Murcia, June 2002.
- [85] A. F. Gómez, G. Martínez, and O. Cánovas. New Security Services based on PKI. *Future Generations Computer Systems*, 2003. To be published.
- [86] Open Group. *The Open Group Home Page*. World Wide Web, <http://www.opengroup.org>, 2002.
- [87] The Open Group. *Common Security: CDSA and CSSM, Version 2*, c914 edition, May 2000.
- [88] The Open Group. *CDSA Explained*. World Wide Web, <http://www.opengroup.org/products/publications/catalog/g905.htm>, 2001.
- [89] C. A. Gunter and T. Jim. Policy-directed certificate retrieval. In *Proceedings of Software - Practice and Experience*, pages 1609–1640, 2000.
- [90] P. Gutmann. PKI: It's not dead, just resting. *IEEE Computer*, 35(8):41–49, 2002.
- [91] K. Gutzmann. Access Control and Session Management in the HTTP Environment. *IEEE Internet Computing*, 5(1):26–35, 2001.
- [92] A. Hagstrom, S. Jajodia, F. Parisi, and D. Wijesekera. Revocation: a classification. In *Proceedings of the 14th IEEE Computer Security Foundation Workshop*, pages 44–58. IEEE Press, 2001.
- [93] J. Y. Halpern and R. van der Meyden. A logic for SDSI's linked local name spaces. In *Proceedings of the 12th Computer Security Foundations Workshop*, pages 111–122. IEEE Computer Society Press, 1999.
- [94] D. Harkins and D. Carrel. *The Internet Key Exchange (IKE)*, 1998. Request For Comments (RFC) 2409.

- [95] T. Hasu and Y. Kortesniemi. *Implementing an SPKI Certificate Repository within the DNS*, Poster Paper Collection of the Theory and Practice in Public Key Cryptography (PKC 200) edition, January 2000.
- [96] M. Hendry. *Smart Card Security and Applications*. Artech House, April 2001.
- [97] A. Herzberg, Y. Mass, J. Michaeli, D. Naor, and Y. Ravid. Access Control Meets Public Key Infrastructure, Or: Assigning Roles to Strangers. In *Proceedings of IEEE Symposium on Security and Privacy*, pages 2–14, April 2000.
- [98] R. Housley. *Cryptographic Message Syntax*, July 1999. Request for Comments (RFC) 2630.
- [99] R. Housley, T. Polk, W. Ford, and D. Solo. *Internet Public Key Infrastructure, Part I: X.509 Certificate and CRL Profile*, April 2002. Request for Comments (RFC) 3280.
- [100] ICE-CAR. *European ICE-CAR Project*. World Wide Web, <http://ice-car.darmstadt.gmd.de/>, 1999.
- [101] ICE-TEL. *European ICE-TEL Project*. World Wide Web, <http://www.darmstadt.gmd.de/ice-tel/>, 1997.
- [102] Identrus. *Identrus Home Page*. World Wide Web, <http://www.identrus.com>, 2002.
- [103] IETF. *PKIX Working Group*. World Wide Web, <http://www.ietf.org/html.charters/pkix-charter.html>, 2002.
- [104] S. Ioannidis, A. D. Keromytis, S. M. Bellovin, and J. M. Smith. Implementing a distributed firewall. In *ACM Conference on Computer and Communications Security*, pages 190–199, 2000.
- [105] ITU-T. *ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*, 1995. Recommendation X.690.
- [106] ITU-T. *ISO/IEC 9594-8, The Directory: Authentication Framework*, 2001. Recommendation X.509.
- [107] A. Jain, R. Bolle, and S. Pankanti, editors. *BIOMETRICS: Personal Identification in Networked Society*. Kluwer Academic, 1999.
- [108] A. Josang. The right type of trust for distributed systems. In *Proceedings of New Security Paradigms '96*, pages 119–131, 1996.
- [109] S. Kent. *Privacy enhancement for Internet electronic mail - part II: Certificate-based key management*. Request For Comments (RFC) 1422, February 1993.

- [110] S. Kent and R. Atkinson. *IP Authentication Header*. Request For Comments (RFC) 2402, November 1998.
- [111] S. Kent and R. Atkinson. *IP Encapsulating Security Payload*. Request For Comments (RFC) 2406, November 1998.
- [112] J. Knudsen. *Java Cryptography*. O' Reilly, 1998.
- [113] P. Kocher. On certificate validation and revocation. In *Proceedings of Financial Cryptography 98*, volume 1465 of *Lecture Notes in Computer Science*, pages 172–177. Springer-Verlag, 1998.
- [114] J. Kohl and C. Neumann. *The Kerberos network authentication service*. Request For Comments (RFC) 1510, September 1993.
- [115] L. Kohnfelder. *Toward a Practical Public-Key Cryptosystem*. M.I.T., 1978. Bachelor's Thesis.
- [116] J. Koponen, P. Nikander, J. Rasanen, and J. Paajarvi. Internet access through WLAN with XML encoded SPKI certificates. In *Proceedings of NordSec'00*, October 2000.
- [117] Y. Kortensniemi, T. Hasu, and J. Sars. Validity Management in SPKI. In *Proceedings of 1st Annual PKI Research Workshop*, pages 27–36, April 2002.
- [118] RSA Laboratories. *PKCS#7: Cryptographic Message Syntax Standard Ver 1.5*, May 1997.
- [119] RSA Laboratories. *PKCS#5: Password-Based Cryptography Standard*, March 1999.
- [120] RSA Laboratories. *PKCS#10: Certification Request Syntax Standard Ver 1.7*, May 2000.
- [121] RSA Laboratories. *PKCS#11: Cryptographic Token Interface Standard Ver 2.10*, December 2000.
- [122] X. Lai. *On the design and security of block ciphers*, volume 2. ETH Series in Information Processing, 1992.
- [123] T. Lampinen. Using SPKI Certificates for Authorization in CORBA based Distributed Object-Oriented Systems. In *Proceedings of NordSec'99*, pages 61–81, November 1999.
- [124] B. W. Lampson. A note on the confinement problem. *Communications of the ACM*, 16(10):613–615, October 1973.
- [125] B. W. Lampson. Protection. *Operating Systems Review*, 8(1):18–24, January 1974.

- [126] N. Li. Local Names in SPKI/SDSI. In *Proceedings of the 13th IEEE Computer Security Foundations Workshop*, pages 2–15. IEEE Press, June 2000.
- [127] D. Lie, C. Thekkath, M. Mitchell, P. Lincoln, D. Boneh, J. Mitchell, and M. Horowitz. Architectural support for copy and tamper resistant software. In *Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS-IX)*, pages 169–177, November 2000.
- [128] The Cryptix Foundation Limited. *Cryptix*. World Wide Web, <http://www.cryptix.org>, 2002.
- [129] J. Liu and Y. Ye, editors. *E-Commerce Agents, Marketplace Solutions, Security Issues, and Supply and Demand*, volume 2033 of *Lecture Notes in Computer Science*. Springer, 2001.
- [130] V. Lortz, M. Wischy, M. Hondo, and T. Nixon. *Universal Plug-and-Play Security Requirement*. UPnP Forum, July 2001.
- [131] G. López and O. Cánovas. *PISCIS PKI: Documentación técnica*. Universidad de Murcia, December 2001.
- [132] J. López. Infraestructuras de autenticación y autorización. *Seguridad en Informática y Comunicaciones (SIC)*, (50):56–60, June 2002.
- [133] H. S. Madhusudhana and V. R. Ramachandran. *SPKI Certificate Integration with Transport Layer Security*. IETF Internet Draft, draft-ietf-tls-spki-00.txt edition, July 2001.
- [134] A. Malpani, R. Housley, and T. Freeman. *Simple Certificate Validation Protocol (SCVP)*, 2002. IETF PKIX Work in progress.
- [135] S. Marsh. *Formalising Trust as a Computational Concept*. PhD thesis, University of Stirling, 1994.
- [136] H. Martínez, F. García, G. López, J. Tavira, J. P. Cánovas, and B. Ubeda. TICA: Dispositivo de Control de Acceso mediante Java y Tarjetas Inteligentes. *Boletín de la Red Nacional de I+D, RedIris*, (55):73–76, January 2001.
- [137] MasterCard and Visa. *SET secure electronic transaction specification, version 1.0. Book 1: Business Description, Book 2: Programmer's Guide, Book 3: Formal Protocol Definition*, May 1997.
- [138] A. Maywah. An implementation of a secure web client using SPKI/SDSI Certificates. Master's thesis, M.I.T., May 2000.
- [139] C. J. McCollum, J. R. Messing, and L. A. Nortagiaco. Beyond the pale of MAC and DAC: Defining new forms of access control. In *Proceedings IEEE Symposium on Research in Security and Privacy*, pages 190–200. IEEE Press, May 1990.

- [140] S. Micali. Enhanced certificate revocation. Technical Report MIT/LCS/TM-542, MIT Laboratory for Computer Science, 1995.
- [141] S. Micali. NOVOMODO: Scalable Certificate Validation and Simplified PKI Management. In *Proceedings of 1st Annual PKI Research Workshop*, pages 15–26, 2002.
- [142] S. Micali and R. L. Rivest. Micropayments revisited. In *Proceedings of the Cryptographer's Track at the RSA Conference 2002*, volume 2271 of *Lecture Notes in Computer Science*, pages 149–163. Springer, 2002.
- [143] Sun Microsystems. *XDR: External Data Representation Standard*, June 1987. Request for Comments (RFC) 1014.
- [144] Sun Microsystems. *Java Card 2.1.1 Application Programming Interface*. World Wide Web, <http://java.sun.com/products/javacard/javacard21.html>, May 2000.
- [145] J. C. Mitchell, V. Shmatikov, and U. Stern. Finite-State Analysis of SSL 3.0. In *7th USENIX Security Symposium*, pages 201–215, 1998.
- [146] D. Mitton, S. Barkley, D. Nelson, B. Patil, M. Stevens, and B. Wolff. *Authentication, Authorization, and Accounting: Protocol Evaluation*. Request For Comments (RFC) 2904, June 2001.
- [147] A. Morcos. A Java implementation of Simple Distributed Security Infrastructure. Master's thesis, M.I.T., 1998.
- [148] M. Myers. Revocation: Options and challenges. In *Proceedings of Financial Cryptography 98*, volume 1465 of *Lecture Notes in Computer Science*, pages 165–171. Springer-Verlag, 1998.
- [149] M. Myers, C. Adams, D. Solo, and D. Kemp. *Internet X.509 Certificate Request Message Format*, March 1999. Request For Comments (RFC) 2511.
- [150] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. *OCSP: Online Certificate Status Protocol*, June 1999. Request For Comments (RFC) 2560.
- [151] M. Myers, X. Liu, J. Schaad, and J. Weinstein. *Certificate Management Messages over CMS*, 2000. Request For Comments (RFC) 2797.
- [152] P. H. Myrvang. *An Infrastructure for Authentication, Authorization and Delegation*. PhD thesis, Department of Computer Science, University of Tromsø, May 2000.
- [153] M. Naor and K. Nissim. Certificate revocation and certificate update. In *Proceedings 7th USENIX Security Symposium*, pages 561–570, January 1998.
- [154] G. Navarro, S. Robles, and J. Borrell. SPKI para el control de acceso a recursos en entornos de agentes móviles. In *Actas de la VII Reunión Española sobre Criptología y Seguridad de la Información*, pages 671–683, September 2002.

- [155] Netscape. *Certificate Management System*. World Wide Web, <http://wp.netscape.com/cms/v4.0/>, 2002.
- [156] P. Nikander. *An Architecture for Authorization and Delegation in Distributed Object-Oriented Agent Systems*. PhD thesis, Helsinki University of Technology, March 1999.
- [157] H. Nwana, J. Rosenschein, T. Sandholm, C. Sierra, P. Maes, and R. Guttman. Agent-mediated electronic commerce: Issues, challenges, and some viewpoints. In *Proceedings of the Second International Conference on Autonomous Agents (Agents'98)*, pages 189–196, May 1998.
- [158] OASIS. *XML-Based Security Services TC (SSTC)*. World Wide Web, <http://www.oasis-open.org/committees/security/index.shtml>, 2002.
- [159] Institute of Electrical and Electronic Engineers. *IEEE Standard Computer Dictionary: A compilation of IEEE Standard Computer Glossaries*. IEEE Press, 1990.
- [160] University of Murcia. *KRONOS Project*. World Wide Web, <http://ants.dif.um.es/kronos>, 2002.
- [161] Helsinki University of Technology. *Telecommunications Software Security Architecture*. World Wide Web, <http://www.tcm.hut.fi/Research/TeSSA/>, 2002.
- [162] R. Oppliger, G. Pernul, and C. Strauss. Using attribute certificates to implement role-based authorization and access control. In *Proceedings of the 4th Fachtagung Sicherheit in Informationssystemen (SIS 200)*, pages 169–184, October 2000.
- [163] J. Partanen and P. Nikander. Adding SPKI certificates to JDK 1.2. In *Third Nordic Workshop on Secure IT Systems (Nordsec'98)*, Trondheim, Norway, 1998.
- [164] N. Perwaiz and I. Sommerville. Structured management of role-permission relationships. In *Proceedings of SACMAT 2001*, pages 163–169. ACM, 2001.
- [165] D. Pinkas and R. Housley. *Delegated Path Validation and Delegated Path Discovery Protocol Requirements*.
- [166] O. Prnjat, I. Liabotis, T. Olukemi, L. Sacksand M. Fisher, P. McKee, K. Carlberg, and G. Martinez. Policy-based Management for ALAN-Enabled Networks. In *Proceedings of 3rd International Workshop on Policies for Distributed Systems and Networks*. IEEE Press, June 2002.
- [167] OpenSSL Project. *OpenSSL library*. World Wide Web, <http://www.openssl.org>, 2002.
- [168] B. Ramsdell. *S/MIME Version 3 Message Specification*, 1999. Request For Comments (RFC) 2633.

- [169] P. Resnick and J. Miller. PICS: Internet Access Controls Without Censorship. *Communications of the ACM*, 39(10):87–93, 1996.
- [170] R. Rivest and B. Lampson. *SDSI: A simple distributed security infrastructure*.
- [171] R. L. Rivest. *The MD5 Message-Digest Algorithm*, April 1992. Request For Comments (RFC) 1321.
- [172] R. L. Rivest. Can We Eliminate Certificate Revocations Lists. In *Proceedings of Financial Cryptography '98*, volume 1465 of *Lecture Notes in Computer Science*, pages 178–183. Springer-Verlag, 1998.
- [173] J. P. Rubio and F. J. Sáez. DKRONOS: Gestión distribuida de Control de Acceso Físico. Master's thesis, Universidad de Murcia, December 2001.
- [174] A. Ruiz, G. Martinez, O. Canovas, and A. F. Gomez. SPEED Protocol: Smartcard-Based Payment with Encrypted Electronic Delivery. In *Proceedings of 4th Information Security Conference*, volume 2200 of *Lecture Notes in Computer Science*, pages 446–461. Springer, 2001.
- [175] B. Sadighi and M. Sergot. Revocation Schemes for Delegated Authorities. In *Proceedings of IEEE 3rd International Workshop on Policies for Distributed Systems and Networks*, 2002.
- [176] B. Sadighi, M. Sergot, and O. Bandmann. Using Authority Certificates to Create Management Structures. In *Proceeding of Security Protocols, 9th International Workshop*, April 2001.
- [177] B. Sadighi and L. van der Torre. Towards a formal analysis of control systems. In *Proceedings of 18th European Conference on Artificial Intelligence*, pages 317–318. John Wiley and Sons, 1998.
- [178] R. S. Sandhu, E. Coyne, H. Feinstein, and C. Youman. Role-based access control models. *IEEE Computer*, 29(2):38–47, February 1996.
- [179] K. Seamons, M. Winslett, and T. Yu. Limiting the Disclosure of Access Control Policies during Automated Trust Negotiation. In *Proceedings of Network and Distributed System Security Symposium*, April 2001.
- [180] RSA Security. *RSA BSAFE*. World Wide Web, <http://www.rsasecurity.com/products/bsafe/>, 2002.
- [181] R. E. Smith. *Internet Cryptography*. Addison Wesley, 1997.
- [182] Sourceforge.net. *Project: Common Data Security Architecture*. World Wide Web, <http://sourceforge.net/projects/cdsa>, 2002.

- [183] F. Stajano. *Security for Ubiquitous Computing*. John Wiley and Sons, 2002.
- [184] M. Thompson, W. Johnston, S. Mudumbai, G. Hoo, K. Jackson, and A. Essiari. Certificate-Based Access Control for Widely Distributed Resources. In *Proceedings of the 8th USENIX Security Symposium*, pages 215–227, August 1999.
- [185] Trolltech. *QT. The cross-platform GUI Toolkit*. World Wide Web, <http://www.trolltech.com>, 2002.
- [186] J. Vollbrecht, P. Calhoun, S. Farrell, L Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, and D. Spence. *AAA Authorization Framework*. Request For Comments (RFC) 2904, August 2000.
- [187] D. Wagner and B. Schneier. Analysis of the SSL 3.0 protocol. *2nd USENIX Workshop on Electronic Commerce*, pages 29–40, November 1996.
- [188] M. Wahl, T. Howes, and S. Kille. *Lightweight Directory Access Protocol (v3)*, December 1997. Request for Comments (RFC) 2251.
- [189] P. Zimmermann. *The Official PGP User's Guide*. MIT Press, 1995.