1. Record Nr. UNINA9910483497803321

Titolo	Public Key Infrastructure : Second European PKI Workshop: Research and Applications, EuroPKI 2005, Canterbury, UK, June 30- July 1, 2005, Revised Selected Papers / / edited by David Chadwick, Gansen Zhao
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XII, 272 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 3545
Altri autori (Persone)	ChadwickDavid <1951-> ZhaoGansen
Disciplina	005.8
Soggetti	Computer networks Cryptography Data encryption (Computer science) Algorithms Information storage and retrieval systems Application software Computers and civilization Computer Communication Networks Cryptology Information Storage and Retrieval Computer and Information Systems Applications Computers and Society
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Authorisation -- A Multipurpose Delegation Proxy for WWW Credentials -- Secure Role Activation and Authorization in the Enterprise Environment -- Towards a Unified Authentication and Authorization Infrastructure for Grid Services: Implementing an Enhanced OCSP Service Provider into GT4 -- Interoperability -- A Heterogeneous Network Access Service Based on PERMIS and SAML -- Interoperation Between a Conventional PKI and an ID-Based Infrastructure -- XKMS Working Group Interoperability Status Report -- Evaluating a CA -- An

Innovative Policy-Based Cross Certification Methodology for Public Key Infrastructures -- Modeling Public Key Infrastructures in the Real World -- Classifying Public Key Certificates -- ID Based Ring Signatures -- Identity Based Ring Signature: Why, How and What Next -- Practical Implementations -- Development of a Flexible PERMIS Authorisation Module for Shibboleth and Apache Server -- CA-in-a-Box -- New Protocols -- A Lower-Bound of Complexity for RSA-Based Password-Authenticated Key Exchange -- Recoverable and Untraceable E-Cash -- Risks and Attacks -- A Method for Detecting the Exposure of OCSP Responder's Session Private Key in D-OCSP-KIS -- Installing Fake Root Keys in a PC -- Long Term Archiving -- Provision of Long-Term Archiving Service for Digitally Signed Documents Using an Archive Interaction Protocol -- Legal Security for Transformations of Signed Documents: Fundamental Concepts.

Sommario/riassunto

This book contains the proceedings of the 2nd EuroPKI Workshop — EuroPKI 2005, held at the University of Kent in the city of Canterbury, UK, 30 June–1 July 2005. The workshop was informal and lively, and the university setting encouragedactive exchangesbetween the speakersand the audience. Theworkshopprogramcomprisedakeynotespeechfrom Dr. CarlisleAdams, followedby18refereedpapers, withaworkshopdinnerinandguidedtouraround the historic Dover Castle. Dr. Adams is well known for his contributions to the CAST family of s-metric encryption algorithms, to international standards from the IETF, ISO, and OASIS, authorship of over 30 refereed journals and conference papers, and co-authorship of Understanding PKI: Concepts, Standards, and Deployment Considerations (Addison-Wesley). Dr. Adams keynote speech was entitled 'PKI: Views from the Dispassionate "I",' in which he presented his thoughts on why PKIhas been availableas an authentication technology for many years now,but has only enjoyed large-scale success in fairly limited contexts to date. He also presented his thoughts on the possible future(s) of this technology, with emp- sis on the major factors hindering adoption and some potential directions for future research in these areas. In response to the Call for Papers, 43 workshop papers were submitted in total. All papers were blind reviewed by at least two members of the Program Committee, the majority having 3 reviewers, with a few borderline papers h- ing 4 or more reviewers; 18 papers were accepted for presentation in 8 sessions.