<<   >>

<<   >>

13   ISBN   9783540351511

10   ISBN   3540351515

         2007-8

         Atzeni, Andrea S.; Lioy, Antonio;

         259

                            PDF

                http://www.tushu007.com

Page 2

This book constitutes the refereed proceedings of the Third European Public Key Infrastructure Workshop: Theory and Practice, EuroPKI 2006, held in Torino, Italy, in June 2006. The 18 revised full papers and 4 short papers presented were carefully reviewed and selected from about 50 submissions. The papers are organized in topical sections on PKI management, authentication, cryptography, applications, and short contributions.

Page 3

PKI Management   Use of a Validation Authority to Provide Risk Management for the PKI Relying Party   Modeling and Evaluation of Certification Path Discovery in the Emerging Global PKI   Distributing Security-Mediated PKI RevisitedAuthentication I   An Improved Lu-Cao's Remote User Authentication Scheme Using Smart Card   Forward Secure Password-Enabled PKI with Instant Revocation   Separable Identity-Based Deniable Authentication: Cryptographic Primitive for Fighting PhishingCryptography   Breaking Yum and Lee Generic Constructions of Certificate-Less and Certificate-Based Encryption Schemes   On the Security of Multilevel Cryptosystems over Class Semigroups of Imaginary Quadratic Non-maximal Orders   Short Linkable Ring Signatures RevisitedApplications   An Infrastructure Supporting Secure Internet Routing   Fighting E-Mail Abuses: The EMPE Approach   DomainKeys Identified Mail Demonstrates Good Reasons to Re-invent   the Wheel   Towards Secure Electronic Workflows   An Access Control System for Multimedia Content Distribution   Efficient Conjunctive Keyword Search on Encrypted Data Storage   SystemAuthentication II   Enhanced Forward-Secure User Authentication Scheme with Smart Cards   Pseudonymous PKI for Ubiquitous Computing   An Efficient POP Protocol Based on the Signcryption Scheme for the WAP PKI   On the Resilience of Key Agreement Protocols to Key Compromise ImpersonationShort ContributionsAuthor Index

PDF