1. Record Nr. UNINA9910484966003321

Titolo	Public Key Infrastructure : Third European PKI Workshop: Theory and Practice, EuroPKI 2006, Turin, Italy, June 19-20, 2006, Proceedings / / edited by Andrea S. Atzeni, Antonio Lioy
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-35152-3
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XII, 264 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 4043
Altri autori (Persone)	AtzeniAndrea S LioyAntonio <1958->
Disciplina	004.6
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	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 Revisited -- Authentication 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 Phishing -- Cryptography -- 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 Revisited -- Applications -- 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 System -- Authentication 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 Impersonation -- Short Contributions -- A PKI System for Detecting the Exposure of a User’s Secret Key -- A Guide to the Nightmares of the Certification Service Provider -- A High-Level 3G Wireless PKI Solution for Secure Healthcare Communications -- Identity-Based Strong Multi-Designated Verifiers Signatures.

Sommario/riassunto

Today, PKIs have come of age and they support the security of several large networked systems, such as company-wide document management systems,- governmentapplicationsandsecureVPN. However,despitethissuccess,the?eld has not yet reachedits full scienti?c maturity and there is still room for research in this area. For example, open issues exist in the e?cient management of large PKI (especially with respect to certi?cate validation), better performance could be attained by improved cryptographic techniques and innovative applications are continuously proposed. To discuss progress in the PKI ?eld, the European PKI workshop series was established in 2004, following similar initiatives in Asia and the USA. The ?rst two events of this series took place on the Island of Samos, Greece (EuroPKI 2004), and in Canterbury, UK (EuroPKI 2005). This book contains the proceedings of the Third European PKI Workshop (EuroPKI 2006), held at the Politecnico di Torino, Italy, on June 19-20, 2006. In response to the Call for Papers, about 50 submissions were received. All submissions werereviewed by at least two reviewers(external or members of the Program Committee) and most of them got three reviews. At the end of this process, 22 papers were selected, 18 in their full form and 4 as short papers. These papers led to a lively workshop, with a good mixture between theory and application, continuing the success of the previous workshops in the series.