1. Record Nr. UNISA996465493403316

Titolo	Public key infrastructure : 4th European PKI Workshop : theory and practice, EuroPKI 2007, Palma de Mallorca, Spain, June 28-30, 2007, proceedings / / Javier Lopez, Pierangela Samarati, Josep L. Ferrer (editors)
Pubbl/distr/stampa	Berlin ; ; Heidelberg ; ; New York : , : Springer, , [2007] ©2007
ISBN	1-280-97013-8 9786610970131 3-540-73408-2
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XI, 380 p.)
Collana	Lecture notes in computer science ; ; 4582
Disciplina	005.8
Soggetti	Public key infrastructure (Computer security)
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	Authorization Architectures for Privacy-Respecting Surveillance -- Privacy-Preserving Revocation Checking with Modified CRLs -- E-Passports as a Means Towards the First World-Wide Public Key Infrastructure -- An Interdomain PKI Model Based on Trust Lists -- One-More Extension of Paillier Inversion Problem and Concurrent Secure Identification -- An Efficient Signcryption Scheme with Key Privacy -- Direct Chosen-Ciphertext Secure Hierarchical ID-Based Encryption Schemes -- Certificate-Based Signature: Security Model and Efficient Construction -- Time Capsule Signature: Efficient and Provably Secure Constructions -- A New Variant for an Attack Against RSA Signature Verification Using Parameter Field -- AutoPKI: A PKI Resources Discovery System -- Bootstrapping a Global SSO from Network Access Control Mechanisms -- Anonymous k-Show Credentials -- On Partial Anonymity in Secret Sharing -- Anonymous Identification and Designated-Verifiers Signatures from Insecure Batch Verification -- OpenHSM: An Open Key Life Cycle Protocol for Public Key Infrastructure's Hardware Security Modules -- Two Worlds, One Smart Card: An Integrated Solution for Physical Access and Logical

Security Using PKI on a Single Smart Card -- On the Robustness of Applications Based on the SSL and TLS Security Protocols -- Using WebDAV for Improved Certificate Revocation and Publication -- Reducing the Computational Cost of Certification Path Validation in Mobile Payment -- Security-by-Contract: Toward a Semantics for Digital Signatures on Mobile Code -- Applicability of Public Key Infrastructures in Wireless Sensor Networks -- Spatial-Temporal Certification Framework and Extension of X.509 Attribute Certificate Framework and SAML Standard to Support Spatial-Temporal Certificates -- Electronic Payment Scheme Using Identity-Based Cryptography -- Undeniable Mobile Billing Schemes -- Universally Composable Signcryption -- Chord-PKI: Embedding a Public Key Infrastructure into the Chord Overlay Network -- Privacy Protection in Location-Based Services Through a Public-Key Privacy Homomorphism -- A Critical View on RFC 3647.

Sommario/riassunto

These proceedings contain the papers accepted at the 2007 European PKI Workshop: Theory and Practice (EuroPKI 2007), held in Palma de Mallorca, Spain, during June 28–30, and hosted by the Computer Science Department of the University of Balearic Islands (UIB) with the support of the Balearic Islands Government and the Private Law Department at UIB. This year’s event was the fourth event in the EuroPKI Workshops series. Previous events of the series were held in: Samos, Greece (2004); Kent, UK (2005); and Turin, Italy, (2006). In response to the call for papers, 77 papers were submitted to this year’s workshop, setting a record of the highest number of papers submitted to an EuroPKI event so far and confirming an increased interest in PKI research and in the EuroPKI event. Each paper was reviewed by three members of the Program Committee, and evaluated on the basis of its significance, novelty, technical quality and relevance to the workshop. The paper selection process was very competitive: of the papers submitted, only 21 full papers and 8 short papers were selected for presentation at the workshop and inclusion in this volume.