1.	Record Nr.	UNINA9910482998603321
	Titolo	Public Key Infrastructure : 5th European PKI Workshop: Theory and Practice, EuroPKI 2008 Trondheim, Norway, June 16-17, 2008, Proceedings / / edited by Stig F. Mjølsnes, Sjouke Mauw, Sokratis Katsikas
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2008
	ISBN	3-540-69485-4
	Edizione	[1st ed. 2008.]
	Descrizione fisica	1 online resource (X, 239 p.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 5057
	Altri autori (Persone)	MjlsnesStig F MauwS KatsikasSokratis K
	Disciplina	005.82
	Soggetti	Cryptography Data encryption (Computer science) Computer programming Algorithms Information storage and retrieval systems Application software Computers and civilization Cryptology Programming Techniques 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	Invited Talk -- New PKI Protocols Using Tamper Resistant Hardware -- Certificates -- Validation Algorithms for a Secure Internet Routing PKI -- Instant Revocation -- Optimized Certificates – A New Proposal for Efficient Electronic Document Signature Validation -- Authentication -- An Efficient and Provable Secure Identity-Based Identification Scheme in the Standard Model -- Trust-Rated Authentication for Domain-

Structured Distributed Systems -- Levels of Assurance and Reauthentication in Federated Environments -- Practice -- Current Status of Japanese Government PKI Systems -- A Privacy-Preserving eHealth Protocol Compliant with the Belgian Healthcare System -- Signatures -- Fast Point Decompression for Standard Elliptic Curves -- An Efficient Strong Key-Insulated Signature Scheme and Its Application -- Efficient Generic Forward-Secure Signatures and Proxy Signatures -- Analysis -- Fault Attacks on Public Key Elements: Application to DLP-Based Schemes -- Weaknesses in BankID, a PKI-Substitute Deployed by Norwegian Banks -- Networks -- An Open Mobile Identity Tool: An Architecture for Mobile Identity Management -- PEACHES and Peers.

Sommario/riassunto

This book constitutes the refereed proceedings of the 5th European Public Key Infrastructure Workshop: Theory and Practice, EuroPKI 2008, held in Trondheim, Norway, in June 2008. The 15 revised full papers presented together with 1 invited paper were carefully reviewed and selected from 37 submissions. Ranging from theoretical and foundational topics to applications and regulatory issues in various contexts, the papers focus on all research and practice aspects of PKI and show ways how to construct effective, practical, secure and low cost means for assuring authenticity and validity of public keys used in large-scale networked services.