| | | |
|---|---|---|
| 1. | Record Nr. | UNINA9910698257103321 |
| | Autore | Barker Elaine B. |
| | Titolo | Guideline for implementing cryptography in the federal government / / Elaine B. Barker, William C. Barker, Annabelle Lee |
| | Pubbl/distr/stampa | Gaithersburg, Md. : , : National Institute of Standards and Technology, , 2005 |
| | Edizione | [Second edition.] |
| | Descrizione fisica | 1 online resource (viii, 89 pages) |
| | Collana | NIST special publication |
| | Disciplina | 005.8 |
| | Soggetti | Computer security - Standards |
| | Lingua di pubblicazione | Inglese |
| | Formato | Materiale a stampa |
| | Livello bibliografico | Monografia |
| | Note generali | Title from title screen (viewed on July 20, 2006).<br>"December 2005." |
| | Nota di bibliografia | Includes bibliographical references. |
| | Sommario/riassunto | This Second Edition of NIST Special Publication (SP) 800-21, updates and replaces the November 1999 edition of Guideline for Implementing Cryptography in the Federal Government. Many of the references and cryptographic techniques contained in the first edition of NIST SP 800-21 have been amended, rescinded, or superseded since its publication. The current publication offers new tools and techniques. NIST SP 800-21 is intended to provide a structured, yet flexible set of guidelines for selecting, specifying, employing, and evaluating cryptographic protection mechanisms in Federal information systems?and thus, makes a significant contribution toward satisfying the security requirements of the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347. The current publication also reflects the elimination of the waiver process by the Federal Information Security Management Act (FISMA) of 2002. SP 800-21 includes background information, describes the advantages of using cryptography; defines the role and use of standards and describes standards organizations that are outside the Federal government; describes the methods that are available for symmetric and asymmetric key cryptography; describes implementation issues (e.g., key management); discusses assessments, including the Cryptographic Module Validation Program (CMVP), the Common Criteria (CC), and |

Certification and Accreditation (C&A); and describes the process of choosing the types of cryptography to be used and selecting a cryptographic method or methods to fulfill a specific requirement.