| | | |
|---|---|---|
| 1. | Record Nr. | UNISALENTO991001152979707536 |
| | Autore | Course and Workshop on physics of mirrors, reversed field pinches, and compact tori |
| | Titolo | Physics of mirrors, reversed field pinches, and compact tori : proceedings of the course and workshop held at Villa Monastero, Varenna, Italy, September 1-11, 1987 / edited by S. Ortolani, E. Sindoni |
| | Pubbl/distr/stampa | Bologna : Editrice Compositori, 1988 |
| | ISBN | 8877940107 |
| | Descrizione fisica | 3 v. : ill. ; 25 cm. |
| | Classificazione | 53.0.66<br>53.0.67<br>53.0.671<br>53.4.6<br>53.6.5<br>530.44<br>QC717.6 |
| | Altri autori (Persone) | Ortolani, S.<br>Sindoni, Elio |
| | Altri autori (Enti) | SIF<br>International school of plasma physics Piero Caldirola |
| | Soggetti | Magnetic mirrors - Congresses |
| | Lingua di pubblicazione | Inglese |
| | Formato | Materiale a stampa |
| | Livello bibliografico | Monografia |
| | Note generali | Includes bibliographies and index.<br>Papers from the Course and Workshop on Physics of Mirrors, Reversed Field Pinches, and Compact Tori of the International School of Plasma Physics "Piero Caldirola." |

| | |
|---|---|
| 2. Record Nr. | UNINA9910855395803321 |
| Autore | Johnston David |
| Titolo | Designing to FIPS-140 : A Guide for Engineers and Programmers / / by David Johnston, Richard Fant |
| Pubbl/distr/stampa | Berkeley, CA : , : Apress : , : Imprint : Apress, , 2024 |
| ISBN | 9798868801259 |
| Edizione | [1st ed. 2024.] |
| Descrizione fisica | 1 online resource (224 pages) |
| Disciplina | 005.8 |
| Soggetti | Data protection<br>Data and Information Security |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Includes index. |
| Nota di contenuto | Chapter 1: FIPS140 -- Chapter 2: FIPS Technical Details -- Chapter 3: Security Levels (1,2,3,4) -- Chapter 4: Subordinate Specs -- Chapter 5: Working with Accredited Certification Labs -- Chapter 6: Documentation Requirements -- Chapter 7: Algorithm Validation -- Chapter 8: Industry Forums. |
| Sommario/riassunto | This book provides detailed and practical information for practitioners to understand why they should choose certification. It covers the pros and cons, and shows how to design to comply with the specifications (FIPS-140, SP800 documents, and related international specs such as AIS31, GM/T-0005-2021, etc.). It also covers how to perform compliance testing. By the end of the book, you will know how to interact with accredited certification labs and with related industry forums (CMUF, ICMC). In short, the book covers everything you need to know to make sound designs. There is a process for FIPS-140 (Federal Information Processing Standard) certification for cryptographic products sold to the US government. And there are parallel certifications in other countries, resulting in a non-trivial and complex process. A large market of companies has grown to help companies navigate the FIPS-140 certification process. And there are accredited certification labs you must contract to get the certification. Although this was once a fairly niche topic, it is no longer so. Other industries— banking, military, healthcare, air travel, and more—have adopted FIPS certification for cryptographic products. The demand for these services |

has grown exponentially. Still, the available skills pool has not grown. Many people are working on products with zero usable information on what to do to meet these standards and achieve certification or even understand if such certification applies to their products. What You Will Learn What is FIPS-140? What is the SP800 standard? What is certification? What does it look like? What is it suitable for? What is NIST? What does it do? What do accredited certification labs do? What do certification consultants do? Where and when is certification required? What do FIPS-140 modules look like? What are the sub-components of FIPS-140 modules (RNGs, PUFs, crypto functions)? How does certification work for them? What are the physical primitives (RNGs, PUFs, key stores) and how do you handle the additional complexity of certifying them under FIPS? What are the compliance algorithms (AES, SP800-90 algos, SHA, ECDSA, key agreement, etc.)? How do you design for certification (BIST, startup tests, secure boundaries, test access, zeroization, etc.)? How do you get CAVP certificates (cert houses, ACVTs)? How do you get CMVP certifications (cert houses, required documents, design information, security policy, etc.)?