1. Record Nr. UNINA9910855395803321

Autore	Johnston David
Titolo	Designing to FIPS-140 : A Guide for Engineers and Programmers
Pubbl/distr/stampa	Berkeley, CA : , : Apress L. P., , 2024 ©2024
ISBN	9798868801259
Edizione	[1st ed.]
Descrizione fisica	1 online resource (224 pages)
Altri autori (Persone)	FantRichard
Disciplina	005.8/24
Soggetti	Data encryption (Computer science) Cryptography Computer security - Standards
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
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 toget 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.