1. Record Nr. UNINA9910809345803321

Autore	Feng Dengguo
Titolo	Trusted computing : principles and applications / / Dengguo Feng [and three others]
Pubbl/distr/stampa	Berlin, [Germany] ; ; Boston, [Massachusetts] : , : De Gruyter : , : Tsinghua University Press, , 2018 ©2018
ISBN	3-11-047609-6
Descrizione fisica	1 online resource (314 pages) : illustrations
Collana	Advances in Computer Science, , 2509-7253 ; ; Volume 2
Disciplina	005.8
Soggetti	Information technology - Security measures Information technology - Management
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Frontmatter -- Preface -- Contents -- 1. Introduction -- 2. Trusted Platform Module -- 3. Building Chain of Trust -- 4. Trusted Software Stack -- 5. Trusted Computing Platform -- 6. Test and Evaluation of Trusted Computing -- 7. Remote Attestation -- 8. Trust Network Connection -- Appendix A: Foundations of Cryptography -- References -- Index
Sommario/riassunto	The book summarizes key concepts and theories in trusted computing, e.g., TPM, TCM, mobile modules, chain of trust, trusted software stack etc, and discusses the configuration of trusted platforms and network connections. It also emphasizes the application of such technologies in practice, extending readers from computer science and information science researchers to industrial engineers.