1.	Record Nr.	UNINA9910298976903321
	Autore	Proudler Graeme
	Titolo	Trusted Computing Platforms : TPM2.0 in Context / / by Graeme Proudler, Liqun Chen, Chris Dalton
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2014
	ISBN	3-319-08744-4
	Edizione	[1st ed. 2014.]
	Descrizione fisica	1 online resource (393 p.)
	Disciplina	004 005.8 005.82 621.382
	Soggetti	Computer security Data encryption (Computer science) Electrical engineering System safety Systems and Data Security Cryptology Communications Engineering, Networks Security Science and Technology
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Description based upon print version of record.
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Introduction to Trusted Computing -- Futures for Trusted Computing -- Basics of Trusted Platforms -- Trusted Platform Architecture -- TPM2 Requirements -- TPM2 Operation -- Initialising TPM2 -- Managing TPM2 -- Accessing Keys and Data in TPM2 -- Customer Configuration of TPM2 and Its Host Platform -- Starting to Use TPM2 -- Direct Anonymous Attestation (DAA) in More Depth -- Machine Virtualisation, Virtual Machines, and TPMs -- Index.
	Sommario/riassunto	In this book the authors first describe the background of trusted platforms and trusted computing, and speculate about the future. They then describe the technical features and architectures of trusted platforms from several different perspectives, finally explaining

second-generation TPMs, including a technical description intended to supplement the Trusted Computing Group's TPM2 specifications. The intended audience is IT managers and engineers, and graduate students in information security.