

Norbert Pohlmann
Helmut Reimer (Hrsg.)

Trusted Computing

**Ein Weg zu neuen
IT-Sicherheitsarchitekturen**

Mit 49 Abbildungen

Inhaltsverzeichnis

Einleitung	1
Trusted Computing – eine Einführung	3
Norbert Pohlmann · Helmut Reimer	
Grundlagen	13
Die Trusted Computing Group	15
Thomas Rosteck	
Trusted Computing Grundlagen	21
Hans Brandl	
TPM Virtualization: Building a General Framework	43
Vincent Scarlata · Carlos Rozas · Monty Wiseman · David Grawrock · Claire Vishik	
Trusted Computing und die Umsetzung in heutigen Betriebssystemen	57
Sebastian Rohr	
Sicherheitsbausteine für Anwendungen	71
Mehr Vertrauenswürdigkeit für Anwendungen durch eine Sicherheitsplattform	73
Markus Linnemann · Niklas Heibel · Norbert Pohlmann	
Die Sicherheitsplattform Turaya	86
Ammar Alkassar · Christian Stüble	
Trusted Network Connect – Vertrauenswürdige Netzwerkverbindungen	97
Marian Jungbauer · Norbert Pohlmann	
Interaktionen TPM und Smart Card	110
Florian Gawlas · Gisela Meister · Axel Heider · Sebastian Wallner	

Anwendungsszenarien	123
Enterprise Security – Informationsschutz im Unternehmen	125
Michael Hartmann · Gunter Bitz	
Unternehmensweites TPM Key Management	140
Bernhard Weiss	
Trusted Computing im Hochsicherheitsbereich	156
Peter Kraaibeek · Hans Marcus Krüger · Kai Martius	
Trusted Computing für automobile IT-Systeme	170
Andrey Bogdanov · Thomas Eisenbarth · Christof Paar · Marko Wolf	
Trusted Computing in mobiler Anwendung: Von Zugangskontrolle zu Identitäten	187
Andreas U. Schmidt · Nicolai Kuntze	
Datenschutz- und rechtliche Aspekte	207
Auswirkungen von Trusted Computing auf die Privatsphäre	209
Markus Hansen · Marit Hansen	
Rechtliche Chancen und Risiken des „Trusted Computing“	221
Andreas Neumann	
Biographien der Autoren	237
Glossar	243
Stichwortverzeichnis	249