LITERATURE ON TRUSTED COMPUTING

The usual problem to face with advanced technologies like Trusted Computing is the gap between the application scenarios and the standardized Trusted Computing specifications. The application scenarios define the system, the integration possibilities and the security requirements on a high level for the whole system, e.g. system integrity protection. Using Trusted Computing as a solution for these security requirements, the Trusted Computing concepts need to be integrated into the whole system and architecture.
The Trusted Computing technology is defined and specified in the Trusted Computing standards. They define the low level set of functions, which the TPM or a Trusted Computing Software Stack provides, however they do not explain in depth how these functions are applied and integrated into a system for specific application scenarios.

For the integration of the Trusted Computing technology into such system, a deeper understanding of the Trusted Computing concepts, the standardized TPM functions and their respective application scenarios is required. These topics are explained in a number of books, which have been written mostly by authors of the specifications. These books introduce the Trusted Computing technologies and offer an informative overview of the specifications for newcomers. It is recommended to read at least one of the books before working with the TCP specification, because it will save a lot of time and resources during the concept and development phase.

The following list of books gives an overview of available literature without any claim of being complete. It also does not contain any judgment about the quality, the didactic or the specific content of the books.

Have fun with reading.

Title:

Trusted Computing Platforms

Author:
Siani Pearson

Publisher:
Hewlet-Packard Company

ISBN:
0-13-009220-7

Fig. 1

Title:

A Practical Guide to Trusted Computing

Authors:
David Challener, Kent Yoder, Ryan Catherman, David Safford and Leendert Van Doorn

Publisher:
IBM Press

ISBN-13:
0-13-239842-7

Fig. 2

Title:

Trusted Computing Platforms

Author:
Sean W. Smith

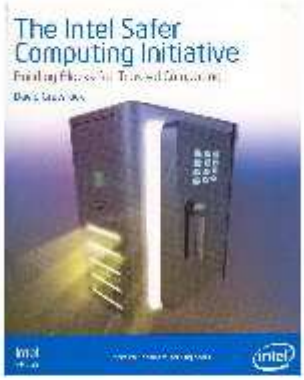
Publisher:
Springer

ISBN:
0-387-23916-2

Fig. 3

Title:

The Intel Safer Computing Initiative



Author:
David Grawrock

Publisher:
Intel Press

ISBN:
0-9764832-6-2

Fig. 4

Title:

Trusted Module Platform Basics - Using TPM in Embedded Systems

Author:
Steven Kinney

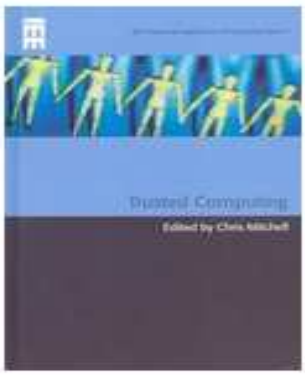
Publisher:
Newnes

ISBN:
0-7506-7960-3

Fig 5

Title:

Trusted Computing



Author:
Chris Mitchell

Publisher:
IEE

ISBN:
0-86341-525-3

Fig 6:

Title:

Trusted Computing: Ein Weg zu neuen IT-Sicherheitsarchitekturen

(only available in German)

Authors:
Norbert Pohlmann, Helmut Reimer

Publisher:
Vieweg+Teubner

ISBN-13:
978-3834803092

Fig. 7

Title:

Trusted Computing Systeme: Konzepte und Anforderungen

(only available in German)

Authors:
Thomas Müller

Publisher:
Springer

ISBN-13:
978-3540764090

Fig. 8