



Automotive, Industrial & Multimarket

Release Notes (Version 03.00.1325.00)

TPM Driver Package

Version: 1.8

Date: 30th April 2007

FOR INTERNAL USE ONLY

Dev. / Step Code:		Sales Code:	
Status:	For Internal Use Only	Date:	30th April 2007
Document:	ReleaseNotes_TPM Driver Package3.0_SP2_IFX	Created with:	Microsoft Office Word
Author:	IFIN SW ADS	TEL.	
Document path:			

REVISION HISTORY

VERSION	DATE	CHANGE MADE BY	SECTION NUMBER	DESCRIPTION OF CHANGE
1.0	11/12/04	M. Palatzky	all	First version
1.1	2005-04-08	M. Groeschel	2.1.7, 2.1.8	Version 01.70.0154.03
1.2	2005-06-13	M. Palatzky	2.1.7, 2.1.8	Version 01.80.0001.00
1.3	2005-11-08	M. Palatzky	2.1.8	Version 01.80.0002.00
1.4	2006-06-27	Arpita Datta	2.1.8, 2.1.10	Version 01.80.0004.00
1.5	2006-08-25	Arpita Datta	2.1.3, 2.1.8	Version 01.80.0004.01 (RC2 release)
1.6	2006-10-19	Arpita Datta	2.1.3, 2.1.7, 2.1.8	Version 03.00.1095.00
1.7	2007-02-05	Arpita Datta	2.1.3, 2.1.7, 2.1.8	Version 03.00.1239.00
1.8	2007-04-30	Arpita Datta	2.1.3, 2.1.8	Version 03.00.1325.00



FOR INTERNAL USE ONLY

Contents

1	Introduction	4
2	Release Notes	5
2.1.1	Purpose of the build	5
2.1.2	Descriptive Name of Deliverable	5
2.1.3	Vendor Version Number	5
2.1.4	Short Description	5
2.1.5	Supported Languages	5
2.1.6	Supported Platforms	5
2.1.6.1	Operating System	5
2.1.6.2	Hardware Requirements	5
2.1.7	Known Observations from Test Report	6
2.1.8	Observations Fixed in this Release	6
2.1.9	Installation Instructions	6
2.1.10	Files Installed or Changed	6
2.1.10.1	Installed Files	6
2.1.11	Co-requisite hardware or software	7
2.1.11.1	BIOS Requirements	7
2.1.11.2	Security Platform Chip	7
3	Debug Versions	8

FOR INTERNAL USE ONLY

1 Introduction

This document provides information about the release of the TPM Driver Package.

FOR INTERNAL USE ONLY

2 Release Notes

2.1.1 Purpose of the build

Version 3.00 Driver Package (Driver only Setup) Service Pack

2.1.2 Descriptive Name of Deliverable

TPM Driver Package

2.1.3 Vendor Version Number

Package Version : 03.00.1325.00

Driver Version : 02.00.0000.00

2.1.4 Short Description

The TPM Driver Package SW is required to install the kernel device driver for your Security Platform Chip.

2.1.5 Supported Languages

English

2.1.6 Supported Platforms

2.1.6.1 Operating System

- Microsoft Windows 2000 Professional Service Pack 4 with Microsoft Internet Explorer 5 or higher
- Microsoft Windows 2000 Server Service Pack 4 with Microsoft Internet Explorer 5 or higher
- Microsoft Windows XP Professional or higher
- Microsoft Windows XP Home Edition or higher
- Microsoft Windows XP Professional x64
- Microsoft Windows Server 2003
- Microsoft Windows Vista

2.1.6.2 Hardware Requirements

A PC capable to run one of the mentioned operating systems and equipped with an Infineon Security Platform Chip TPM SLD 9630 TT1.1 or SLB 9635 TT1.2.

FOR INTERNAL USE ONLY

2.1.7 Known Observations from Test Report

- tpm00005233 On Windows XP systems, the Driver Only SetUp fails when done using "Add Hardware Wizard".

2.1.8 Observations Fixed in this Release

- Added support for new version of TPM Driver (version 02.00.0000.00)

2.1.9 Installation Instructions

The module <Setup.exe> installs the Infineon TPM kernel device driver.

Installation of the driver requires administrative rights.

2.1.10 Files Installed or Changed

2.1.10.1 Installed Files

File Name	Installation Directory	Comment
Readme.txt	%INSTALLDIR%	Readme file

Following files will be temporarily installed during the installation process and will be removed after the installation process finished:

File Name	Installation Directory	Comment
IfxDrvSetupAppl32.exe	%SUPPORTDIR%	Installation Helper EXE
IfxDrvSetupAppl64.exe	%SUPPORTDIR%	Installation Helper EXE
IfxInstHlp.dll	%SUPPORTDIR%	Installation Helper DLL

Installation Directory:

Abbreviation	Windows 2000 / XP	Comment
%DRIVER%	%OS%\System32\Drivers	
%INSTALLDIR%	<Program Files>\Infineon\ Security Platform Software	Default installation directory, but user may change it



FOR INTERNAL USE ONLY

Abbreviation	Windows 2000 / XP	Comment
%OS%	<Windows>	Directory of operating system
%SUPPORTDIR%		Dynamically created by Windows Installer on start of a installation process. It is automatically removed on process finish.

2.1.11 Co-requisite hardware or software

2.1.11.1 BIOS Requirements

BIOS ACPI plug and play support for the Security Platform Chip.

2.1.11.2 Security Platform Chip

TPM SLD 9630TT1.1 with firmware version 1.05 or greater.

or

TPM SLB 9635 TT1.2 with firmware version 1.00 or greater.

FOR INTERNAL USE ONLY

3 Debug Versions

Debug Event log entries will not expose any confidential information but allows to follow up internal PSD processing for support purposes.