



Automotive, Industrial & Multimarket

Release Notes (V3.0.2.2 SP2 HF2)

Infineon TPM Professional Package

Version: 2.3

Date: 4th February 2008

Dev. / Step Code:	Sales Code:
Status:	Date: 4th February 2008
Document: IFX_ReleaseNotes_3.0.2.2.doc	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	03/07/06	IFIN SW ADS	all	Beta 1
1.2	11/08/06	IFIN SW ADS		Beta2
1.3	28/09/06	IFIN SW ADS		RC
1.5	25/10/06	IFIN SW ADS		RC2
1.55	16/11/06	IFIN SW ADS		RC3 (Preliminary)
1.7	24/11/06	IFIN SW ADS		RC3
1.75	11/12/06	IFIN SW ADS		RTM HF1
1.8	05/02/07	IFIN SW ADS		SP1 RC1
1.9	27/02/07	IFIN SW ADS		SP1 RC2
2.1	20/07/07	ADS SEC SW		SP2
2.3	04/02/08	ADS SEC SW		SP2 HF2

Contents

1	Introduction	5
2	Release Notes	6
2.1.1	Purpose of the build	6
2.1.2	Descriptive Name of Deliverable	6
2.1.3	Vendor Version Number	6
2.1.4	Short Description	6
2.1.5	Supported Languages	6
2.1.6	Supported Platforms	6
2.1.6.1	Operating Systems	6
2.1.6.2	Compatibility requirements	7
2.1.6.3	Hardware Requirements	7
2.1.7	Known Observations from Test Report	7
2.1.7.1	Not supported functionality	7
2.1.7.2	Setup	7
2.1.7.3	Encrypting File System	8
2.1.7.4	PSD	8
2.1.7.5	Dictionary Attack	8
2.1.7.6	Entrust	9
2.1.7.7	RSASecurID	9
2.1.7.8	Enhanced Authentication	9
2.1.7.9	TNA	9
2.1.7.10	Miscellaneous	10
2.1.8	Observations Fixed in this Release	10
2.1.9	Obsolete Observations	11
2.1.10	Installation Instructions	11
2.1.11	WHQL Certification State	11
2.1.12	Files Installed or Changed	11
2.1.12.1	Installed Files	12
2.1.13	Component dependencies	16



2.1.14	Co-requisite hardware or software	17
2.1.14.1	BIOS Requirements	17
2.1.14.2	Security Platform Chip	17
3	Debug Versions.....	18

1 Introduction

This document provides information about the released version of the Infineon TPM Professional Package.

2 Release Notes

2.1.1 Purpose of the build

Version V3.0.2.2 SP2 HF2

2.1.2 Descriptive Name of Deliverable

Infineon TPM Professional Package

2.1.3 Vendor Version Number

Build: 03.00.1413.05

2.1.4 Short Description

The Infineon TPM Professional Package Software is required to use your Security Platform Chip.

The Infineon TPM Professional Package Software is a TCG-compliant security solution for PCs.

2.1.5 Supported Languages

BR	- Brazilian Portuguese
CH	- Chinese simplified
CHT	- Chinese Traditional
FR	- French
GR	- German
IT	- Italian
JP	- Japanese
KR	- Korean
RU	- Russian
SP	- Spanish
US	- English

2.1.6 Supported Platforms

2.1.6.1 Operating Systems

- Microsoft Windows Vista (prepared for SP1)
- Microsoft Windows XP Professional Service Pack 2
- Microsoft Windows XP Home Edition Service Pack 2
- Microsoft Windows XP Media Center Edition 2005
- Microsoft Windows XP Tablet PC Edition 2005
- Microsoft Windows Server 2003 Service Pack 1

2.1.6.2 Compatibility requirements

- On a Windows 2000 based platform the Internet Explorer versions 5.0 and 6.0 (for SSL client side authentication via Infineon TPM User CSP) and the related versions of the Outlook Express (for S/MIME utilizing the Infineon TPM User CSP).
- Microsoft Office applications Microsoft Office 2000 SR-1, Microsoft Office XP, Microsoft Office 2003 (for S/MIME and SSL client side authentication via Infineon TPM User CSP).
- Netscape Communicator application Netscape Communicator 4.7.9, Netscape Communicator 7.2 (for S/MIME and SSL client side authentication via TPM Cryptoki Token).
- RSA SecurID
RSA SecurID Software Token Software V3.0
RSA SecurID ACE/Agent Software V5.0 for web access authentication
RSA SecurID ACE/Agent Software V5.5 (plus patch: sdeap.dll V5.5.0.133) for remote access authentication
- Checkpoint
Check Point VPN-1 SecuRemote/SecureClient NG with Application Intelligence (R55)
Check Point VPN-1/FireWall-1 NG with Application Intelligence (R55)
- Entrust
Entrust Desktop Solutions 7.0:
Entrust Entelligence Desktop Manager (Entrust/Entelligence)
Entrust Entelligence E-mail plug-in for Outlook (Entrust/Express)
Entrust Entelligence File Plug-in (Entrust/ICE)
Entrust Entelligence TrueDelete (Entrust/TrueDelete)
- Adobe
Acrobat 6.0 Professional for digitally signing of PDF documents as well as encryption.

2.1.6.3 Hardware Requirements

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

2.1.7 Known Observations from Test Report

2.1.7.1 Not supported functionality

- Server awareness of client
- Archive with emergency recovery / password reset public key not selectable by Security Platform admin in platform init wizard

2.1.7.2 Setup

- tpm00004826 If the software is installed on an operating system which does not support policies (e.g. XP Home), then the policies are missing after an upgrade to an

operating system which supports this feature (e.g Vista Business Edition) and cannot be enabled by repair/modify of the installation. The software has to be uninstalled and reinstalled to enable the policies. This is mentioned in the Readme.txt

- tpm00000761 If the user changes the “Language for non-Unicode programs” in Control Panel, Regional settings, the Setup will run in that language and the shortcuts in the Start menu are created in the same language.

2.1.7.3 Encrypting File System

- tpm00004960 UAC and BUP dialogs pop up when administrative user logs on if OS is upgraded from XP to Vista. Workaround mentioned in the Readme.txt file.
- tpm00004293 Reconfiguration of EFS on Windows 2003 Server
Reconfiguration gets active after user has logged on again
- tpm00004244 Key Set Problem while configuring the EFS when the system time is changed. The Readme.txt mentions the workaround for this by restarting the system
- tpm00003414 (SMS00000749) 1 minute delay during log off on W2K after using EFS.

2.1.7.4 PSD

- tpm00003566 PSD TNA Load
If PSD is configured to “Load at logon” and user does not provide Basic User Password (BUP) during that process but chooses to load PSD additionally from TNA an error message “Personal Secure Drive is in use by another process” pops up. PSD can still be loaded by providing BUP in first BUP dialog.
- tpm00002404 Delete PSD with save of content
More space than really required is requested since calculation of required space for copy contains also space used by file system and system volume information of PSD drive.

2.1.7.5 Dictionary Attack

- tpm00005227 When the limit for the dictionary attack is set to 1, the TPM is not deactivated even if the count of the dictionary attack reaches this limit.
- tpm00003550 Upgrade from Infineon TPM Professional Package 2.0 with IFX TPM1.2 to Infineon TPM Professional Package 3.0:
TPM_AT_DELAY_DOUBLE_LOCK mode not set
If a PC system with IFX 1.2 TPM is initially used with Infineon TPM Professional Package 2.0, the TPM chip is not initialized with TPM_AT_DELAY_DOUBLE_LOCK mode while upgrading to Infineon TPM Professional Package 3.0.
If the user upgrades to Infineon TPM Professional Package 3.0, it does not behave the same as if he initialized with Infineon TPM Professional Package 3.0. TPM is still in TPM_AT_DELAY mode.
This issue is mentioned in Readme file with according workaround.

- tpm00003623 No event log entry after entering DA defense mode
- tpm00003749 Reset of DA if Platform is in state "Initialized with Other OS" state
Calling the Platform Initialization wizard with command line parameter /resetAttack to reset DA defense measures has no effect. TPM wizard ignores parameter and wants to initialize the platform.

2.1.7.6 Entrust

- tpm00002158
 - Creation of an Entrust profile for a user id that is not TPM-initialized
Error displayed from the Entrust software - "Cryptoki device returned an unknown error value"
 - Creation of an Entrust profile for a user id that is TPM-initialized, but the platform is disabled
Error displayed from the Entrust software - "This profile must be a token profile"
- tpm00002497 Basic User Password dialog pops up twice
 - After login (entrust login is started automatically), the BUP dialog comes up twice, then the Entrust dialog "Enter pin ..." once.
 - While creating Entrust Profile BUP dialog comes up twice, in between the entrust dialog ("enter pin ...") pops up.

2.1.7.7 RSA SecurID

- tpm00001061 Remote access authentication from Windows logon screen
In the Windows logon screen the PKCS#11 module does not support the option "Log on using dial-up connection".
Workaround: Log on to the system and start the remote access connection from the Control Panel, Network Connections.

2.1.7.8 Enhanced Authentication

- tpm00002809 Switch to "Enhanced Authentication" when BUK password has expired
If BUK password has expired the BUK password has to be changed first before enhanced authentication can be enabled

2.1.7.9 TNA

- tpm00004357 Wrong tooltip in TNA if platform is temp disabled due to dictionary attack. TNA tooltip says "Ready to use" even when TPM 1.2 chip goes into defense state and DA mode of TPM 1.2 is configured to TPM_AT_DELAY_DOUBLE_LOCK.
- tpm00003386 TNA does not offer EFS logout when EFS certificate is used which is not yet valid. When user decrypts a file which is encrypted by a certificate which is not yet valid TNA does not show "Logout from Encrypting File System" menu because EFS state is set to "needs reconfiguration".

2.1.7.10 Miscellaneous

- tpm00005457 After installation of HSW, the warning event, 3004 from Windows Defender, is found in the system event log. This is a behaviour of Microsoft Windows Defender and a service request is pending at Microsoft regarding this issue.
- tpm00005451 Warning 1517 of application event log is recorded on every reboot.
- tpm00005450 Warning 1524 of application event log is recorded after EFS access.
- tpm00005420 Warning 541 of TBS is recorded when the system resume from S3 and / or S4
- tpm00004837 WLAN is not supported on Windows Vista systems.
- tpm00004714 Error events when accessing encrypting file after key is purged.
- tpm00004527 Status update in Security Platform Control panel is missing in case the BitLocker is managed from Vista BitLocker Control Panel.
- tpm00004526 Status update in TNA and the Security Platform Control panel is missing in case the TPM is managed from Vista TPM console/wizard. A possible workaround for Owner state : Restart system.
- tpm00004272 (SMSPS00000328)Basic User Password Dialog prevents Shutdown/Restart
When the Basic User Key password is present, the user cannot perform Shutdown or Restart. However Standby and Hibernate can be performed.

2.1.8 Observations Fixed in this Release

Fixed with SP2 HF2

- tpm00006558 Migration failure with EFS configured on source and target
Root cause: Old basic user key is used/cached by CSP
Fix: Release basic user key before importing new basic user key
- tpm00006557 System hangs on shutdown after resume from standby
Root cause: Raise condition in TPM driver. Driver waits for an event that is never signaled (deadlock)
Fix: Workaround in TCS by resetting the event during shutdown
- tpm00006415 Certificate enrollment via MMC does not work on Vista SP1
Root cause: CSP returns failure on CryptSetKeyParam(param=KP_CERTIFICATE) since certificate storage is not supported.
Fix: CSP returns Success on CryptSetKeyParam(param=KP_CERTIFICATE) but doesn't not store certificate
- tpm00005837 After S3 resumes, the TPM utility cannot be used intermittently.
Root cause: The time delay for waiting for the TPM to resume was not sufficient.
Fix: Increased the time period to wait for TPM to resume

2.1.9 Obsolete Observations

- tpm00004784 Counter of failed attempts does not appear on screen for changing user password.

Reason : This was not reproducible by development team and also received confirmation from customer that it was not reproducible by them either,

2.1.10 Installation Instructions

The module <Setup.exe> installs the Infineon TPM Professional Package Software.

Installing Infineon TPM Professional Package Software requires administrative rights.

2.1.11 WHQL Certification State

Guardionic Solutions has a signed contingency from Microsoft for its PSD.SYS driver that WHQL is not applicable to this driver. Contingency No: 622

2.1.12 Files Installed or Changed

2.1.12.1 Installed Files

File Name	Installation Directory	Comment
CustomBIOS.htm	%INSTALLDIR%\%MUI%	Online Help for BIOS information
FooterLine.gif	%INSTALLDIR%\%MUI%	Online Help for BIOS information
SecurityPlatform.chm	%INSTALLDIR%\%MUI%	Security Platform Help
License_%.rtf	%INSTALLDIR%\%MUI%	License text
Logo.gif	%INSTALLDIR%\%MUI%	Logo
Readme.txt	%INSTALLDIR%\%MUI%	Release Notes
ReadmeUpgrade.txt	%INSTALLDIR%\%MUI%	Release Notes for upgrade
IfxSpURs%MUI.dll	%INSTALLDIR%	Common UI resource DLL
IFXTRs%MUI%.dll	%INSTALLDIR%	IFX TSS Resource DLL
IFXTRsMs.dll	%INSTALLDIR%	IFX TSS Message Table Resource DLL
SpPolSys.msc	%INSTALLDIR%\%TARGET_OS%\%MUI%	MMC template: Security Policy – System
SpPolUsr.msc	%INSTALLDIR%\%TARGET_OS%\%MUI%	MMC template: Security Policy - User
SpMigWz.exe	%INSTALLDIR%	Security Platform Migration Wizard
SpMUIHlp.exe	%INSTALLDIR%	MUI Helper for launching the Getting Started Guide
SpTna.exe	%INSTALLDIR%	Security Platform TNA
SpTPMWz.exe	%INSTALLDIR%	Security Platform Initialization Wizard
SpUserWz.exe	%INSTALLDIR%	Security Platform User Initialization Wizard
SpP12Wz.exe	%INSTALLDIR%	Security Platform PKCS#12 Import Wizard
SpPwdResetWz.exe	%INSTALLDIR%	Security Platform Password Reset Wizard
SpBackupWz.exe	%INSTALLDIR%	Security Platform Backup Wizard
SpUpgrade.exe	%INSTALLDIR%	Tool for upgrading from V1.70 to this version
IfxSpPol.adm	%POL%	Administrative Template for Group Policy Editor
IFXTPM.sys	%DRIVER%	TPM Kernel Device Driver
CapiCom.dll	%SYS32%	CAPICOM support; Redistributable from Microsoft
IfxSpMgt.cpl	%SYS32%	Security Platform Control Panel Applet

File Name	Installation Directory	Comment
IfxSpMgt.dll	%SYS32%	Security Platform Management Provider
IfxSpMgt.exe	%SYS32%	Security Platform Management Service
IfxSpMps.dll	%SYS32%	Security Platform Management ServiceProxy/Stub – 32 bit
IfxSpMps.dll	%SYS64%	Security Platform Management ServiceProxy/Stub – 64 bit
IFXTCS.exe	%SYS32%	TSS Core Service
IFXTCSps.dll	%SYS32%	TSS Core Service Proxy/Stub – 32 bit
IFXTCSps.dll	%SYS64%	TSS Core Service Proxy/Stub – 64 bit
IFXTPM.dll	%SYS32%	TSS Device Driver Library
IfxTPMCK.dll	%SYS32%	IFX PKCS#11 Provider – 32 bit
IfxTPMCK.dll	%SYS64%	IFX PKCS#11 Provider – 64 bit
IFXTPMCP.dll	%SYS32%	TPM Cryptographic Provider – 32 bit
IFXTPMCP.dll	%SYS64%	TPM Cryptographic Provider – 64 bit
IFXTSP.dll	%SYS32%	TSS Service Provider – 32 bit
IFXTSP.dll	%SYS64%	TSS Service Provider – 64 bit
IfxUAGUI.exe	%SYS32%	IFX User Authorization Server
IfxUAGps.dll	%SYS32%	IFX User Authorization Server Proxy/Stub – 32 bit
IfxUAGps.dll	%SYS64%	IFX User Authorization Server Proxy/Stub – 64 bit
IfxSPArc.dll	%SYS32%	Security Platform Archive Access Component – 32 bit
IfxSPArc.dll	%SYS64%	Security Platform Archive Access Component – 64 bit
IfxXmlRs.dll	%SYS32%	XML Resource DLL

Personal Secure Drive:

File Name	Installation Directory	Comment
Psd.dll	%INSTALLDIR%	Personal Secure Drive Middleware module
PSDCFGWZ.ocx	%INSTALLDIR%	Personal Secure Drive Configuration Wizard Pages
PSDRs%MUI%.dll	%INSTALLDIR%	Personal Secure Drive Language Ressource DLL's
PSDMsg.dll	%INSTALLDIR%	Personal Secure Drive Message Library for Event Logging
PSDrt.exe	%INSTALLDIR%	Personal Secure Drive Runtime Application
PSDShExt.dll	%SYS32%	Personal Secure Drive Explorer Shell Extension –

File Name	Installation Directory	Comment
		32 bit
PSDShExt.dll	%SYS64%	Personal Secure Drive Explorer Shell Extension – 64 bit
IfxPsdSv.exe	%SYS32%	Personal Secure Drive Windows Service
PSD.sys	%DRIVER%	Personal Secure Drive Disk driver
PSDRecovery.exe	%OS%	Personal Secure Drive Recovery Tool

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

File Name	Installation Directory	Comment
IfxInstDrv.dll	%SUPPORTDIR%	Driver Installation Helper DLL
IfxInstHlp.dll	%SUPPORTDIR%	Installation Helper DLL
License_%S.rtf	%SUPPORTDIR%	Licence text displayed in License Agreement Dialog
IfxDrvSetupAppl32.exe	%SUPPORTDIR%	Driver Installation Helper Exe
IfxDrvSetupAppl64.exe	%SUPPORTDIR%	Driver Installation Helper Exe

Installation Directory:

Abbreviation	Windows 2000 / XP	Comment
%DRIVER%	<Windows>\System32\Drivers	
%HELP%	<Windows>\Help	
%INSTALLDIR%	<Program Files>\Infineon\Tpm Software	Default installation directory, but user may change it
%MUI%	US, FR, GR, SP, IT, JP, CH, CHT, KR, RU	Abbreviation for MUI support identifying a certain language
%OS%	<Windows>	
%POL%	<Windows>\inf	
%SUPPORTDIR%		Dynamically created by Windows Installer on start of a installation process. It is automatically removed on process finish.
%SYS32%	<Windows>\System32 <Windows>\SysWow64	On a 32 bit operating system On a 64 bit operating system



Abbreviation	Windows 2000 / XP	Comment
%SYS64%	<Windows>\System32	On a 64 bit operating system
%TARGET_OS%	WXP, W2K, Vista	Abbreviation for the target OS

[illegible]

2.1.14 Co-requisite hardware or software

2.1.14.1 BIOS Requirements

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

2.1.14.2 Security Platform Chip

- Security Platform Chip: TPM SLD 9630TT1.1
Firmware: Version 1.05
- Security Platform Chip: SLB 9635TT1.2
Firmware: Version 1.00

3 Debug Versions

PSD supports event logging also for debugging purposes.

The PSD event logging is controlled via registry entries at
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\App Paths\PSDapp

The event log level is set by the value 'EventLogging' as REG_DWORD, this value is set at install time.

Following values are defined:

- No event log

0 No event log

1 Only error events

2 Error and warning events (**default** at installation)

3 Error, warning and information events

4 Error, warning, information and debug events (EventDebugging value)

In case of debug events, an additional value 'EventDebugging' controls with module posts debug events as REG_DWORD, one or more values can combined (added) together.

0x00000001 PSD.dll

0x00000002 PSDrt.exe

0x00000004 PSDsvc.exe

0x00000008 PSDCFGWZ.ocx

0x00000010 PSDShExt.dll

0x00000040 PSDrecovery.exe

0x00000100 unmount.exe (only visible at uninstall time)

Note:

Enabling debug events for all modules will fill up the eventlog very fast.

Therefore the recommendation is to change the event log properties.

Increase the log size and enable the option "overwrite events as needed".

