Automotive, Industrial & Multimarket

Release Notes (V2.5 RTM RC1)

Infineon TPM Professional Package

Version: 1.1

Date: 10 November 2005

Dev. / Step Code:	**Sales Code:**
Status:	**Date:** 10 November 2005
Document: IFX TPM Professional Package - Release Notes.doc	**Created with**: Microsoft Office Word
Author: AIM CC TI	**TEL.**
Document path:	

REVISION HISTORY

VERSION	DATE	CHANGE MADE BY	SECTION NUMBER	DESCRIPTION OF CHANGE
1.1	09/19/05	AIM CC TI	all	Beta
1.1	11/10/05	AIM CC TI	2.1.7 2.1.8	RTM RC 1

Contents

1 Introduction

This document provides a comprehensive overview of the system, using a number of different concept/design views to depict different aspects of the system. It is intended to capture and convey the significant decisions which have been made on the system.

2 Release Notes

2.1.1 Purpose of the build

Version V2.5 RTM RC1

2.1.2 Descriptive Name of Deliverable

Infineon TPM Professional Package

2.1.3 Vendor Version Number

Build: 02.50.0734.03

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
SP - Spanish
US - English

2.1.6 Supported Platforms

2.1.6.1 Operating Systems

- 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
- Microsoft Windows 2000 Professional Service Pack 4 with Microsoft Internet Explorer 5 or higher

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

Known Bugs and Limitations

2.1.7.1 Not supported functionality

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

2.1.7.2 Setup

- 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.

- tpm00003367 License Agreement window is not closed by clicking on next, another window will merge on top of the License Agreement window making the Lincense Agreement window not to go away during the installation process. It will disappear at the Finish Window (issue on Windows 2000, fixed for Windows XP)

2.1.7.3 Encrypting File System

- tpm00003360 Reconfiguration of EFS on Windows 2003 Server
  Reconfiguration gets active after user has logged on again
- tpm00003414 1 minute delay during log off on W2K after using EFS

2.1.7.4 PSD

- tpm00000912 No data in PSD but warning to delete it
- tpm00002404 Delete PDS 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.
- 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.

2.1.7.5 Dictionary Attack

- tpm00003550 Upgrade from HSW 2.0 with IFX TPM1.2 to HSW 2.5:
  TPM_AT_DELAY_DOUBLE_LOCK mode not set
  If a PC system with IFX 1.2 TPM is initially used with HSW 2.0, the TPM chip is not initialized with TPM_AT_DELAY_DOUBLE_LOCK mode while upgrading to HSW 2.5. If the user upgrades to HSW 2.5, it does not behave the same as if he initialized with HSW 2.5. TPM is still in TPM_AT_DELAY_DOUBLE 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 wizards 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 RSASecurID

- tpm00001051 cannot import token file to ifxtpmck.dll through double click. Button “Transfer Tokens Smart Card” does not appear.
  Status: a service request at RSA Inc. has been started and clarification is in progress.
- 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.
- tpm00002103 If the Platform is disabled and the user tries to import a token through the RSA SecurID Software Token the User Authentication Screen appears. When user enters the right password an error message "Token Import Failed: PKCS 11 Error:Error writing PKCS 11 Object" appears.

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

- tpm00003386 TNA does not offer EFS logout when EFS certificate is used which is no 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”.
- tpm00003568 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.

2.1.7.10 User Documentation

- tpm00003381 / tpm00003382 / tpm00003374 / tpm00003376 Layout of tables
  If window displaying the online help is not large enough, the table layout is not properly aligned (e.g. French, Japanese)

2.1.7.11 TSS 1.2 compatibility

- The definition of TSS flags are changed to be consistent with TCG approved TSS 1.2 header files

This has the following impact:
- Applications developed with current IFX TSS SDK header files may fail in case they are using these flags running on top of new TSS Stack
- Applications developed with new flag definitions may only run on new TSS Stack in case they are using these flags
- Applications may choose to determine the version of TSS stack installed and use the appropriate flag values to achieve compatibility with different versions.

2.1.7.12 Miscellaneous

- tpm00002791 Initialization of guest user account
  Information: Initialization of guest user account can be done successfully. But after log off OS deletes the user hive so that user is not initialized again after log in.
- tpm00003340 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

Same fixes as in V2.0 SP2.

- tpm00002654 Validation of password
  Information: While taking the system backup and restore a user on a new clean system without TPM owner present and user not initialized before, the user is asked for a BUK password. Password cannot be validated at the time the password is requested. Later on wizard will show failure information on finish page.
- tpm00002914 "Unspecified error" when driver for SC reader is not installed
  User Wizard ends up with “Unspecified error” if Platform initialized including enhanced auth but no SC reader is installed on system

Fixes with RTM

- tpm00003336 Core service startup strategy with hidden TPM not implemented.
- tpm00003359 Certificate request still possible after the Basic User Key was deleted (via management provider API).
  Background: the CSP and its keys (BUK) remain loaded as long as the application was not closed.
- tpm00003367 License Agreement window is not closed by clicking on next, another window will merge on top of the License Agreement window making the Lincense Agreement window not to go away during the installation process. It will disappear at the Finish Window (fixed for Windows XP)
- tpm00003468 Concurrent system backup of more than one system into one backup file on a server share is not supported.
- tpm00003485 Strings which were modified or added new after the first package was sent to translation service will appear in English in resource files.
- tpm00003489 no hint if SC reader disconnected.

- tpm00003491 TNA Info page is not getting updated to show temp. disabled after entering DA defense mode
- tpm00003523 No balloon pops up after the TPM was disabled.
- tpm00003526 Certificate Viewer does not display all PKCS#11 certificate properties correctly
- tpm00003552 Error Dialogue not modal with respect to Owner Password change Window.
- tpm00003553 Policy is not getting added in WIN 2K French
- tpm00003562 Event log entry from "Spupgrade" caused by missing registry key.
  Hint: The problem is self-healing; the solution will create the registry key at first subsequent use.
- tpm00003579 Balloon "cannot access backup archive ..." when initializing new platform and user on Windows XP Media Center Edition
- tpm00003582 License.txt still shows V2.0 in all languages except English

2.1.9 Installation Instructions

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

Installing Infineon TPM Professional Package Software requires administrative rights.

2.1.10 WHQL Certification State

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

2.1.11 Files Installed or Changed

2.1.11.1 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_%S.txt	%INSTALLDIR%\%MUI%	License text
Logo.gif	%INSTALLDIR%\%MUI%	Online Help for BIOS information
MS_Help.css	%INSTALLDIR%\%MUI%	Online Help for BIOS information
Readme.txt	%INSTALLDIR%\%MUI%	Release Notes
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%	MMC template: Security Policy – System
SpPolUsr.msc	%INSTALLDIR%	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
IfxSpCustomGlue.dll	%INSTALLDIR%	Helper Dll for launching the Security Platform Mgt.
IfxSpPol.adm	%POL%	Administrative Template for Group Policy Editor
IFXTPM.sys	%DRIVER%	TPM Kernel Device Driver
CapiCom.dll	%SYS32%	CAPI COM support; Redistributable from Microsoft
IfxSpMgt.cpl	%SYS32%	Security Platform Control Panel Applet
IfxSpMgt.dll	%SYS32%	Security Platform Management Provider
IfxSpMgt.exe	%SYS32%	Security Platform Management Service
IfxSpMps.dll	%SYS32%	Security Platform Management ServiceProxy/Stub
IFXTCS.exe	%SYS32%	TSS Core Service

File Name	Installation Directory	Comment
IFXTCSps.dll	%SYS32%	TSS Core Service Proxy/Stub
IFXTPM.dll	%SYS32%	TSS Device Driver Library
IfxTPMCK.dll	%SYS32%	IFX PKCS#11 Provider
IFXTPMCP.dll	%SYS32%	TPM Cryptographic Provider
IFXTSP.dll	%SYS32%	TSS Service Provider
IfxUAGUI.exe	%SYS32%	IFX User Authorization Server
IfxUAGps.dll	%SYS32%	IFX User Authorization Server Proxy/Stub
IfxSPArc.dll	%SYS32%	Security Platform Archive Access Component
IfxWlxEN.dll	%SYS32%	WinLogon Event Notification DLL
IfxXmlRs.dll	%SYS32%	XML Resource DLL

Personal Secure Drive Integration:

File Name	Installation Directory	Comment
Psd.dll	%INSTALLDIR%	Personal Secure Drive Middleware module
PSDCFGWZ.ocx	%INSTALLDIR%	Personal Secure Drive Configuration Wizard Pages
PSDCFGWZ%MUI%.dll	%INSTALLDIR%	Personal Secure Drive Language Ressource DLL's for Wizard Pages
PSDMsg.dll	%INSTALLDIR%	Personal Secure Drive Message Library for Event Logging
PSDRecovery%MUI%.dll	%INSTALLDIR%	Personal Secure Drive Language Ressource DLL's for Recovery Tool.
PSDrt.exe	%INSTALLDIR%	Personal Secure Drive Runtime Application
PSDrt%MUI%.dll	%INSTALLDIR%	Personal Secure Drive Language Ressource DLL's for Runtime Application.
PSDShExt.dll	%INSTALLDIR%	Personal Secure Drive Explorer Shell Extension
PSDShExt%MUI%.dll	%INSTALLDIR%	Personal Secure Drive Language Ressource DLL's for Explorer Shell Extension.
PSDSrvc.exe	%INSTALLDIR%	Personal Secure Drive Windows Service
PSD.sys	%DRIVER%	Personal Secure Drive Disk driver
PSDRecovery.exe	%SYS32%	Personal Secure Drive Recovery Tool

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

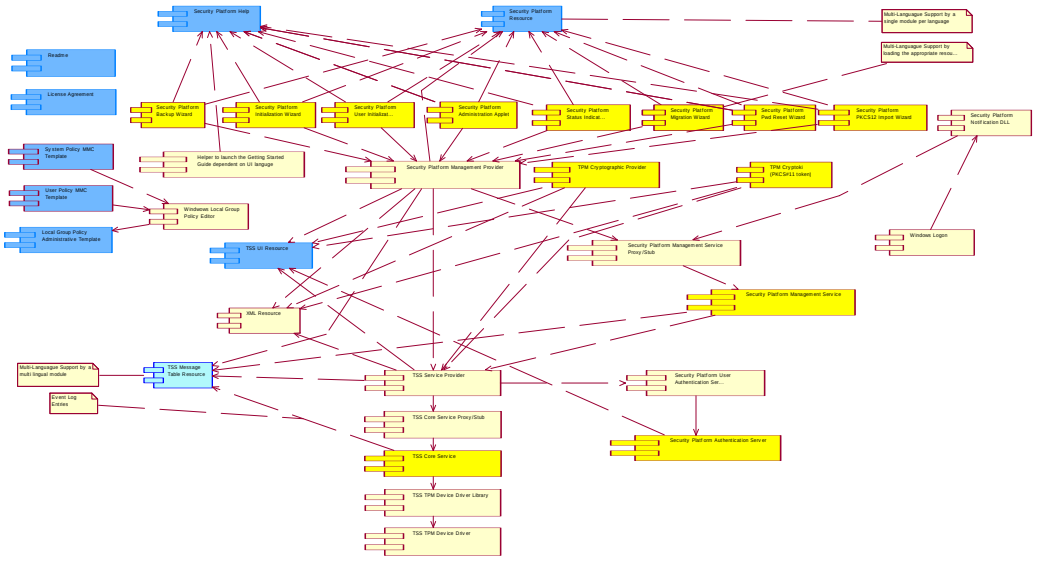
File Name	Installation Directory	Comment
IfxInstDrv.dll	%SUPPORTDIR%	Driver Installation Helper DLL

File Name	Installation Directory	Comment
IfxInstHlp.dll	%SUPPORTDIR%	Installation Helper DLL
License_%S.txt	%SUPPORTDIR%	Licence text displayed in License Agreement Dialog

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	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	

2.1.12 Component dependencies



2.1.13 Co-requisite hardware or software

2.1.13.1 BIOS Requirements

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

2.1.13.2 Security Platform Chip

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

2.1.14 Memory requirements

2.1.15 Known conflicting components

3 Test Results

4 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 PSDsrvc.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".

5 FTP drop box