Chipcard & Security

Release Notes (V3.7 RTM)

Infineon TPM Professional Package

Version: 1.1

Date: 2010-02-24

Dev. / Step Code:		Sales Code:	
Status:		Date:	2010-02-24
Document: IFX_ReleaseNotes.doc		Created with: Microsoft Office Word	
Author: CCS TI DM SW PC		TEL.	
Document path:			

REVISION HISTORY

VERSION	DATE	CHANGE MADE BY	SECTION NUMBER	DESCRIPTION OF CHANGE
1.0	2010-02-02	CCS TI DM SW PC		V3.7 RC
1.1	2010-02-24	CCS TI DM SW PC		V3.7 RTM

Infineon

Contents

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 V3.7 RTM

2.1.2 Descriptive Name of Deliverable
Infineon TPM Professional Package

2.1.3 Vendor Version Number
Build: 03.70.2281.00

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

2.1.5.1 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
CS   - Czech

2.1.6 Supported Platforms

2.1.6.1 Operating Systems
Operating Systems (only for 32-bit product version):

- Microsoft Windows XP Professional Service Pack 3

- Microsoft Windows XP Home Edition Service Pack 3

- Microsoft Windows XP Media Center Edition 2005 Service Pack 3

- Microsoft Windows XP Tablet PC Edition 2005 Service Pack 3

- Microsoft Windows Server 2003 Service Pack 2

- Microsoft Windows Vista Service Pack 1 (Home Basic, Home Premium, Business, Enterprise, Ultimate)

- Microsoft Windows Vista Service Pack 2 (Home Basic, Home Premium, Business, Enterprise, Ultimate)

- Microsoft Windows Server 2008 Service Pack 2

- Microsoft Windows 7 (Home Premium, Professional, Enterprise, Ultimate)

Operating Systems (only for 64-bit product version):

- Microsoft Windows XP Professional x64 Edition Service Pack 3 (AMD64)

- Microsoft Windows Server 2003 x64 Edition Service Pack 2 (AMD64)

- Microsoft Windows Vista Service Pack 1 (Home Basic, Home Premium, Business, Enterprise, Ultimate)

- Microsoft Windows Vista Service Pack 2 (Home Basic, Home Premium, Business, Enterprise, Ultimate)

- Microsoft Windows 7 (Home Premium, Professional, Enterprise, Ultimate)

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).

- 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)

- 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

Project Specific Documents

- Infineon Security Platform Chip TPM SLB 9635TT1.2

- Broadcom TPM
  TPM FW-Version: 2.23
  Tested with HPQ Lakeport DC 7600
  TPM FW-Version: 2.30
  Tested with HPQ Castles DC5750

- Winbond TPM
  TPM FW-Version: 2.16
  Tested with Desktop-System from Lenovo

- STMicro TPM
  TPM FW-Version: 4.30
  Tested with Dell-OptiPlex 755 System; BIOS-Version: A04 (11/05/07)

2.1.7 Known Observations from Test Report

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*

- tpm00006568 Norton Antivirus 2005 complains about "malicious script" during installation. This is not seen with latest version of Norton Antivirus as with Norton Antivirus 2006

- tpm00006105 Warning message for unsupported operating systems
  Warning message for unsupported OS appears after the installation of prerequisites. According information is provided readme.txt as "Known Bugs and Limitation".

- tpm00006064 Fatal error during un-installation, If prerequisite package (e.g. VC++ Redistributable) is removed and then TPM software is un-installed. This is mentioned in readme.txt as "Known Bugs and Limitation".

- tpm00006051 InstallShield error 1152: Extracting prq file while passing incorrect parameter during setup.
  InstallShield error 1152 is displayed, if setup is launched with an invalid command line

- 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

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

- 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_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 wizard ignores parameter and wants to initialize the platform.

2.1.7.6 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.

2.1.7.7 Settings Tool

- tpm00006609 The "X" on upper right corner of system message box is shown but does not work.

If platform or user is not initialized, clicking on "User" page will display a dialog informing the user if he wants to initialize now. The "X" on upper right corner is shown but does not work on this dialog. This is only visible systems with Vista and AERO effects enabled and is an operating system issue. SW uses system message box which should handle this. The "x" button is not enabled if the message box has buttons other than "OK", "Cancel". It is by design from MS since Windows 2000.

2.1.7.8 TPM Interoperability

- Potential interoperability issue between ST-Micro TPM v4.30 and other third party TPMs like Intel and Winbond in migration scenarios.
  Migration in "Migrate-Mode" (used in emergency recovery use case while restoring from system backup) and in "Re-Wrap-Mode" (used in migration use case) from STMicro TPM system to other third party TPM system fails, if STMicro TPM did not generated a "full qualified" basic user key (most significant bit is not set).

- tpm00006713 A TPM or TSS error occurs for STMicro TPM if TPM is disabled under Vista
  TPM SW is installed on a clean system and Chip is disabled in BIOS. If user starts the CPL as administrator and clicks any tab different to Info page a "TPM or TSS error occurred (0xe0283002)" message box pops up.

- tpm00006682 Interoperability between ST-Micro (TPM FW v3.11) and other none ST-Micro TPMs
  Migration from a ST-Micro TPM system to another TPM system is not possible. Migration wizard fails with authorization error for basic user password validation during import of migration archive on destination system. This error occurs even if user is migrating from user (a) to user (b) on the same ST-Micro system.
  Not an issue with STMicro TPM FW v4.30

- tpm00006671 Interoperability between ST-Micro and Winbond TPM system
  User initialized on a ST-Micro TPM system does not work in Winbond TPM system if roamed to Winbond system with Trusted Computing Management Server v1.0 in server mode or via emergency recovery restore in standalone mode.

- tpm00006510 Interoperability between ST-Micro and Broadcom TPM system
  User initialized on a ST-Micro TPM system does not work in Broadcom TPM system if roamed to Broadcom system with Trusted Computing Management Server v1.0 in server mode or via emergency recovery restore in standalone mode.

2.1.7.9 Miscellaneous

- tpm00007764 Microsoft VPN connection when using EAP-TLS with certificates
  Issue is mentioned in readme.txt section 5.6.20

- tpm00007538 TPM small icon in control panel is shown without key image.

- tpm00007522 TPM icon 'expansion/compression' problem in Vista control panel
  No support for 'large' & 'Extra large' TPM icons in control panel.

- tpm00006486 F5 to refresh PSD configuration pages does not work
  F5 does not refresh list box on page "Configure your Personal Secure Drive"

- tpm00006093 Volume Shadow Copy Service (VSS) shows issue at Vista, Windows
  Server 2003 and XP when a PSD is loaded.
  With Vista System Restore is not using System Restore service, but is utilizing
  Volume Shadow Copy Service (VSS). As VSS is affected when a PSD is loaded,
  creation of restore points is also affected when PSD is loaded and selected for
  automatic restore points.

- tpm00005457 After installation of SW, the warning event, 3004 from Windows
  Defender, is found in the system event log. This is a behavior 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

- 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 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.

2.1.7.10 RSASecurID

- tpm00006110 RSA SecurID Software Token v3.07 does not load PKCS#11 crypto
  service provider.
  RSA provided a hot fix for Infineon (based on v3.07) that re-enables PKCS#11
  support. But this hot fix does not work with Host Software versions 3.0 and higher.
  Presumably there will not be a version 3.08 of RSA SecurID.

2.1.7.11 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

2.1.8 Observations Fixed in this Release

2.1.8.1 RC 2 / RTM

- tpm00008281 Encryption of a file is done using an obsolete key (only under Vista)
  EFS file access is denied after a certificate change (e.g. migrating TPM User from

source to destination PC). This happens if a user has multiple instances for the same user running (e.g. run as, elevation) which are accessing EFS encrypted files.

2.1.8.2 RC 1

- tpm00008072 TPM EFS encrypt function is lost when first BUP dialog is canceled

- tpm00008228 Missing 'i' icon in PKCS#11 PKI Help

- tpm00008217 Shorten period without displaying any progress dialog during installation

- tpm00008182 Error seen in event log -> Event ID: 12320 - The key cannot be found in the persistent storage database after resetting the TPM to factory default and re-initializing the user

- tpm00008179 Error seen in event log -> Event ID: 12320 - The key cannot be found in the persistent storage database after resetting the TPM to factory default and re-initializing the user

- tpm00008168 Initialization on Windows 7 by Active Directory & local admin user reflects 2 error events in Application log
Event ID : 57 - The "Infineon TPM Key Storage Provider" provider was not loaded because initialization failed.

- tpm00008157 Wizards and CPL don't work on Win2000

- tpm00008129 Microsoft Visual C++ 2005 SP1 ATL Patch Redistributable is installed as a pre-requisite

- tpm00008102 Improvement of Japanese policy name and description for reading NV memory

- tpm00008101 Inconsistent Japanese TNA menu item for PSD Unload all

- tpm00008100 Japanese list of feature in User Init Wizard is inconsistent with US and Help

- tpm00008098 Button in Help for migration is inconsistent with actual dialog

- tpm00008097 Help for PSD Unload dialog is inconsistent with actual dialog

- tpm00008096 Inappropriate Japanese translations in Help file

- tpm00008095 Inconsistent Japanese translation in dialogs and Help for Password Reset

- tpm00008091 Name of button to change certificate during User Init Wizard in Help file is inconsistent

- tpm00008090 Name of Wizard Page Element for EFS in Quick Init Wizard is inconsistent with actual dialog

- tpm00008089 Name of User Init Wizard Page Element for Key Length in Help is inconsistent with actual dialog

- tpm00008088 Help for Password and Authentication dialog of User Init Wizard is inconsistent with actual dialog

- tpm00008086 EFS error seen in the event viewer after multiple rebooting the system
  Event ID : 7022 – The Encrypting File System (EFS) service hung on starting.

- tpm00008080 Improvements of Japanese translation in Help

- tpm00008067 User Init Wizard Windows flow gets stuck at one point

- tpm00008066 Inconsistent Help for VPN EAP setting on Windows Vista and 7

- tpm00008054 Inconsistent Japanese translation for Logon in Help

- tpm00008053 Duplication of double quote in Japanese Uninstallation notice dialog

- tpm00008052 Improvement of Japanese translation in Advance tab

- tpm00008051 Japanese typo in Password Reset Wizard

- tpm00008044 Windows Vista/7 Editions not suported should be described in Readme

- tpm00008022 Help for Restoration is inconsistent with actual dialog

- tpm00008021 Help for Password Reset is inconsistent and incorrect with actual dialog

- tpm00008020 Inconsistent Help for TNA menu item Enable TPM

- tpm00008019 Change of System Backup schedule without reentering PW is not reflected to Task Scheduler on Vista and 7

- tpm00008015 Request for details regarding why EFS configuration options are not available in EFS setting window of user initialization wizard.

- tpm00007998 Help for License Agreement dialog is inconsistent

- tpm00007996 PSD cannot be unloaded as long as an explorer instance is running in Windows 7

- tpm00007978/ tpm00007977 Inappropriate Japanese translations in Help file

- tpm00007943 Name of Backup Image File is inconsistent in Help and dialogs
  Fixed only for Japanese

- tpm00007915 Cut text on Button Labels in Korean

- tpm00007912 Inconsistent notation of radio button in Help file

- tpm00007911 "Restore All" fails if more than 150 different user are enrolled and saved in system backup archive

- tpm00007910 System backup created in wrong location if re-initialization is done by another administrative user after clearing TPM in BIOS

- tpm00007907 Inappropriate Japanese translations in Help file

- tpm00007901 Successive Log-on / user initialization / log-off of more than 150 different users sporadically reflects in an error: Cannot connect to TPM in TNA

- tpm00007900 Inappropriate Japanese translation in Summary page of Backup Wizard

- tpm00007899 Inconsistent Japanese translation of 'user' in InstallShield

- tpm00007894 Same Message display twice if re-initialization of user with advanced user wizard is done after TPM clear in BIOS

- tpm00007893 Localization of Japanese Readme

- tpm00007892 Irregular EFS behavior at a particular Power Transition Profile

- tpm00007891 Strange message when deleting PSD and giving a non-existent path for saving PSD content

- tpm00007889 System Backup Archive is not protected against encryption

- tpm00007869 User initialization fails for PSD if HD space is exactly on reserved limit for system drive

- tpm00007501 Remove unnecessary character in JP Help file

2.1.9 Obsolete Observations

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

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

2.1.12 Co-requisite hardware or software

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

2.1.12.2 Security Platform Chip
- Security Platform Chip: TPM SLD 9630TT1.1
  Firmware: Version 1.05

- Security Platform Chip: SLB 9635TT1.2
  Firmware: Version 1.02
  Firmware: Version 2.18
  Firmware: Version 3.16
  Firmware: Version 3.17

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 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".