Chipcard & Security

Release Notes
(V4.3.200.3390 RTM)

Infineon TPM Professional Package

Version: 1.60

Date: 2013-09-10

Dev. / Step Code:	**Sales Code:**
Status:	**Date:** 2013-09-10
Document: IFX_ReleaseNotes.doc	**Created with**: Microsoft Office Word
Author: CCS TI SW PC	**TEL.**
Document path:	

REVISION HISTORY

VERSION	DATE	CHANGE MADE BY	SECTION NUMBER	DESCRIPTION OF CHANGE
1.20	2012-08-28	CCS TI SWT SW	2.1, 2.1.10, 2.2.9	Infineon Professional Package V4.3 RTM
1.30	2012-12-18	CCS TI SWT SW	2.1.1, 2.1.2, 2.1.3, 2.1.5, 2.1.7, 2.1.10 2.2.4, 2.3, 2.4	Infineon Professional Package V4.3.100 Release Candidate
1.40	2013-01-29		2.1.1, 2.2.3	Infineon Professional Package V4.3.100 RTM
1.50	2013-07-02		2.1.1, 2.1.2, 2.1.3, 2.1.5, 2.1.7; 2.2.9	Infineon Professional Package V4.3.200 Release Candidate
1.60	2013-09-10		2.1.1, 2.1.10, 2.2.3, 2.2.8 2.2.9	Infineon Professional Package V4.3.200 RTM

Contents

1 Introduction

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

2 Release Notes

2.1 General Information

2.1.1 Purpose of the build

Version: V4.3.200.3390 RTM

2.1.2 Descriptive Name of Deliverable

Infineon TPM Professional Package

Marketing Version: 4.3.200.3390

2.1.3 Vendor Version Number

Build: 04.03.3390.00

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 New with this version

- Support of Windows 8.1
- Settings Tool does not display <Chip Version> for SLB 9655 and newer in <More Details> any longer. Field is not shown at all.

2.1.6 Supported Languages

CS	--> Czech
DE	--> German
EN	--> English
ES	--> Spanish
FR	--> French
IT	--> Italian
JA	--> Japanese
KO	--> Korean
PT-BR	--> Brazilian Portuguese
RU	--> Russian
zh-Hans	--> Chinese Simplified
zh-Hant	--> Chinese Traditional

2.1.7 Supported Operating Systems

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

- Microsoft Windows XP Service Pack 3
  (Professional , Home Edition, Media Center Edition 2005, Tablet PC Edition 2005)
- Microsoft Windows Vista Service Pack 2
  (Home Basic, Home Premium, Business, Enterprise, Ultimate)
- Microsoft Windows 7 Service Pack 1
  (Home Premium, Professional, Enterprise, Ultimate)
- Microsoft Windows Server 2008 Service Pack 2
- Microsoft Windows 8
  (Windows 8, Windows 8 Pro, Windows 8 Enterprise)
- Microsoft Windows 8.1
  (Windows 8.1, Windows 8.1 Pro, Windows 8.1 Enterprise)

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

- Microsoft Windows XP Professional x64 Edition Service Pack 2 (AMD64)
- Microsoft Windows Vista Service Pack 2
  (Home Basic, Home Premium, Business, Enterprise, Ultimate)
- Microsoft Windows 7 Service Pack 1
  (Home Premium, Professional, Enterprise, Ultimate)
- Microsoft Windows Server 2008 R2 Service Pack 1
- Microsoft Windows 8
  (Windows 8, Windows 8 Pro, Windows 8 Enterprise)
- Microsoft Windows 8.1
  (Windows 8.1, Windows 8.1 Pro, Windows 8.1 Enterprise)
- Microsoft Windows Server 2012

2.1.8 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
- Infineon Security Platform Chip TPM SLB 9635TT1.2
- Infineon Security Platform Chip TPM SLB 9655

2.1.9 Prerequisites

-

2.1.10 Compatibility requirements

- Tested with Mozilla Thunderbird 17.0.8

- Tested with Mozilla Firefox 23.0.1
- Microsoft Office applications
  Microsoft Office 2003, Microsoft Office 2007, Microsoft Office 2010 and Microsoft Office 2013 (for S/MIME and SSL client side authentication via Infineon TPM User CSP).
- 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.

2.2 Known Observations from Test Report

2.2.1 Not supported functionality

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

2.2.2 Setup

- tpm00008578 Missing characters on Installation Wizard [Preparing to install...] page
  Service request raised at Flexera. Flexera rejected service request since they are not able to reproduce this behavior and engineering rejects any bugs that are not easily reproducible.
- tpm00006105 Warning message for unsupported operating systems
  Warning message for unsupported OS appears after the installation of prerequisites. According information is provided in 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”.
- 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

2.2.3 Encrypting File System

- tpm00008900 Encrypted Power Point file is opened in read-only mode
  After “Logout from Encrypting File System” is done Power Point sporadically opens an EFS encrypted Power Point file in read only mode
- tpm00008648 Unexpected User Authentication dialog will be displayed for EFS encrypted file if EFS encryption key is no longer available

- tpm00007939 EFS configuration shows problem if policy "Require smart card for EFS" is set
  During action "Initialize EFS ..." a balloon with title "Encrypting File System needs your smart card PIN" pops up. Clicking on the balloon another dialog is displayed. Select "Create a new smart card certificate" in the dialog. Dialog quits with error message "The smart card resource manager is not running" and Quick Wizard completes successfully. But when trying to encrypt a file the dialog as mentioned above comes up again and file cannot be encrypted.
- 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.

2.2.4 PSD

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

2.2.5 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.

2.2.6 Settings Tool

- tpm00007752 CPA Update of BitLocker tab information
  To get BitLocker status updates (Encrypting, Decrypting etc.) user has to switch to another tab then change back to "BitLocker" tab.
- tpm00006609The "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 on 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.

2.2.7 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.

2.2.8 Miscellaneous

- tpm00008807 Error event log (ID 16385) written when "Preparation of TPM setting" is enabled
- tpm00007764 Microsoft VPN connection when using EAP-TLS with certificates of keys with strong private key protection
  Issue is mentioned in readme.txt as “Known Bugs and Limitation”.
- 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.
- tpm00006893 IE protected mode prevents usage of TPM CSP
  Connection to a SSL Website that requires a client site certificate and is not in a Trusted Zone (where protected mode is off per default) fails using a TPM certificate with template "Client Authentication - User".
  Workaround: Put Website into Trusted Zone
- 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

- 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 (Windows XP)
  When the Basic User Key password is present, the user cannot perform Shutdown or Restart. However Standby and Hibernate can be performed.

2.2.9 Windows 8 and 8.1 related

- If the system shuts down or goes into sleep or hibernation while performing Security Platform operation requiring access to the TPM (such as initializing the Security Platform, changing Basic User Password and others), the operation might not finish properly. It is recommended to avoid power state transitions while performing such operations. In case such failure is observed, please repeat the operation after system restart.
- Windows SmartScreen
  Windows 8 might prevent running Setup.exe with „Windows protected your PC“ message. This might happen when Setup.exe is run from an untrusted (for example network) location or copied from an untrusted location and then started locally. This is because Infineon TPM Professional Package 4.3 uses new code signing certificate that has not yet established sufficient reputation with Windows SmartScreen Application Reputation service. User should continue the installation by selecting More Options -> Run Anyway.
- Event log entries when disabling TPM chip via Settings Tool
  When disabling TPM via Settings Tool, every action in Settings Tool (e.g. press button "More details ..") results in event log error entries with 'TPM' as source. Disabling via tpm.msc reduces the count of entries, but there is still one.
- Upgrade from Windows 7 x64 to Windows 8 x64
  CSP registration for 32 bit is lost. Workaround: Repair or reinstall Infineon Professional Package.
- Missing user authentication while re-connecting a WLAN connection
  Connection is re-established without asking for the Basic User Password again.
- Basic User Password (BUP) option "Remember for all applications" is not working for VPN connections
  BUP dialog appears on Windows 8 if a user establishes a VPN connection using a TPM certificate even if user has checked BUP option "Remember for all applications" while e.g. encrypting a file before.
- tpm00008905 Installation on Windows 8.1 continues after confirmation to cancel the installation
  This can happen in various situations, for example, when no TPM is found, or when an upgrade has been detected. Installation continues even after user acknowledges or confirms aborting the installation.
  This is a known InstallShield issue for Windows 8.1.

Workaround: User can still abort installation by pressing Cancel in subsequent built-in InstallShield wizard pages.

2.3 Observations Fixed in this Release

2.4 Obsolete Observations

2.5 Installation Instructions

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

Installing Infineon TPM Professional Package Software requires administrative rights.

2.6 Co-requisite hardware or software

2.6.1 BIOS Requirements

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

2.6.2 Security Platform Chip

- Security Platform Chip: TPM SLD 9630TT1.1
  Firmware: Version 1.05
- Security Platform Chip: SLB 9635TT1.2
  Firmware: Version 3.19
- Security Platform Chip: SLB 9655
  Firmware: Version 4.32

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".