TPM Enhanced Provisioning Tool

Introduction

The purpose of this tool is to provide flexible and easily extensible provisioning features as well as diagnostic features for developers. Using the tool run with command line options enables provisioning and TPM non volatile index verification, using the tool without command line options enables the interactive mode exposing the diagnostic features.

Part 1: Provisioning

This section explains how this tool can be used to create and write to TPM non volatile indexes.

To provision the TPM all the files need to be in the same directory, then commands can be run like the below examples. The a-la-cart style system makes it easy to create indexes, populate their nv data, and script the process. The def and nvi files are plain text editable, and we suggest editing with notepad++ because it preserves the formatting well.

Using the tool with a .def command line argument defines an NV index on the TPM if the TPM is unlocked and compares the existing definition of that index if the TPM is locked.

Using the tool with a .nvi command line argument writes data to the NV index on the TPM if the TPM is unlocked and compares the existing data of that index if the TPM is locked.

Command line examples:

```
ServerTPMTool.efi Aux3.def
ServerTPMTool.efi PS.def
ServerTPMTool.efi PPI.def
ServerTPMTool.efi PS.nvi
ServerTPMTool.efi PPI.nvi
ServerTPMTool.efi TPM_Lock.def
```

A script that performs these actions called DefaultTPMProvision.nsh is provided for convenience.

Def file format: (with sample values)

```
File Signature: TPM1.2
Major Version: 1
Minor Version: 0
TPM Version: 102
reserved0 [0]: 0
```

```
reserved0 [1]: 0
reserved0 [2]: 0
reserved0 [3]: 0
Tag: C1
Parameter Size: 65
Ordinal: CC
Define Space Tag 0: 18
Index Value: 50000003
Read Size of Select: 3
Read PCR Selct [0]: 0
Read PCR Selct [1]: 0
Read PCR Selct [2]: 0
Read Locality at Release: 1F
Read Digest at Release: 0000000000000000000000000000000000000000
Write Size of Select: 3
Write PCR Selct [0]: 0
Write PCR Selct [1]: 0
Write PCR Selct [2]: 0
Write Locality at Release: 18
Write Digest at Release: 0000000000000000000000000000000000000000
Define Space Tag 1: 17
Attributes: 0
Read ST Clear: 0
Write ST Clear: 0
Write S Define: 0
Data Size: 96
encAuthValue Value: 0000000000000000000000000000000000000000
Auth Value: 0000000000000000000000000000000000000000
Reserved1 [0]: 0
```

Nvi file format: (with sample values)

```
Index Value: 50000001
File Offset: 0
Data Size: 54
Index Offset: 0
NV Data:
02020001000000000000000000000000000000000000000000000000000000000000010203040
5060708091011121314151617181920
```

Part 2: Interactive Features

The interactive options use the same def and nvi files as the automated section in part 1. There is a host of debugging features as well help developers with diagnostics.
Note: this part of the software is in development. Most of it works.

Main menu:

1: Display TPM Status (Version, V-flags, P-flags, etc)

2: NV RAM Functions
3: Lock the TPM
4: Take Ownership
5: Clear Ownership
6: PCR Functions
7: TIS Functions
Q: Quit

TPM Status Menu:

1: Display TPM Interface Status
2: Display TPM Volatile flags
3: Display TPM Non-Volatile flags
Q: Previous Menu

TPM NV Ram Menu:

1: Display Existing Index values\n");
2: Create a new index definition file from scratch.\n");
3: Create a definition file from an existing Index and edit it.\n");
4: Edit an existing definition file.\n");
5: Create NV Index\n");
6: Verify NV Index DEF \n");
7: Delete NV Index\n");
8: Read NV Data\n");
9: Write NV Data\n");
10: Verify NV Data \n");
11: Display NV Index DEF\n");
12: Display DEF File\n");
Q: Previous Menu\n");

TPM PCR Functions:

1: Create PCR Dump File (i.e., capture the PCR values for use in creating a PCR Info)
2: Display PCR values
3: Display PCR Log
4: Extend PCR (future)
5: Clear PCR (future)
Q: Previous Menu

TPM TIS Functions: (not implemented)

1: Read <RegAddress>
2: Write <RegAddress> <ByteValue>
3: Locality <level>
4: Get <RegName>
5: Set <BitName>
Q: Previous Menu

Known bugs

INTEL® TRUSTED EXECUTION TECHNOLOGY TOOLKIT
ENABLING TOOLS LICENSE AGREEMENT

1.0 DEFINITIONS

1.1 “**End User**” means a third party licensee to whom you license your Licensee Program (either directly or through your usual distribution channels and methods) for use on Intel-based platforms pursuant to a license agreement that complies with the requirements of Exhibit B.

1.2 “**Intel**” means Intel Corporation and its majority-owned global subsidiaries.

1.3 “**Licensee**”, “you” and “your” refers to you, the licensee under this Agreement.

1.4 “**Licensee Programs**” means software programs developed by Licensee or on Licensee’s behalf using any of the licensed Materials, as further described in Subsection 2.1(a) below.

1.5 "**Materials**" are defined as the Object Code, Source Code, Third Party Software, documentation, license key codes, APIs and any other materials (including any updates, error corrections and upgrades thereto) provided by Intel to Licensee under this Agreement.

1.6 “**Object Code**” means computer programming code provided by Intel to Licensee under this Agreement in binary form suitable for machine execution by a processor without the intervening steps of interpretation or compilation.

1.7 “**Source Code**” means computer programming code provided by Intel to Licensee under this Agreement in human-readable format.

1.8 “**Third Party Software**” is defined as third party software programs and associated information included in the Materials, which may be subject to certain additional or different third party license terms (reference Exhibit A hereto and the ReadMe and text files provided with the Materials).

1.9 “**Intel TXT**” refers to Intel’s proprietary Trusted Execution Technology (which is Intel’s trademark, all rights reserved).

2.0 LICENSE AND LICENSE RESTRICTIONS

2.1 LIMITED COPYRIGHT LICENSE: Subject to Licensee’s compliance with all terms and conditions of this Agreement, Intel grants to Licensee a limited, non-exclusive, non-transferable license during the term of this Agreement under Intel’s copyrights to:

a. use the Materials for the limited purposes (the “**Purposes**”) of developing, using, distributing to End Users, and supporting derivative tools, utilities and related materials (the “**Licensee Programs**”) for use on Intel-based platforms that (i) verify that BIOS and platform conform to the applicable Intel TXT requirements, (ii) provision Trusted Platform Modules (TPMs) for Intel TXT, (iii) create and manage launch control policies for Intel TXT, (iv) evaluate and manage platform configuration regarding any aspect of Intel TXT, and/or (v) otherwise promote appropriate use of TXT;

b. make, and distribute internally to your employees and contractors who have agreed in writing to comply with the terms of this Agreement, copies of the Materials (including the Source Code) solely for use in support of the Purposes;

c. make, and distribute externally to your End Users, copies of the Materials (excluding the Source Code, which you are not permitted to redistribute externally), independently and/or as incorporated into your Licensee Programs, solely for use in support of the Purposes; and

d. modify and create derivative works of the Materials, and distribute such derivative works to End Users subject to Intel's rights in the Materials as specified herein (again, you are not permitted to redistribute externally any of the Source Code), solely for use in support of the Purposes.

2.2 LICENSE RESTRICTIONS: Licensee may not:

a. use, copy or distribute any of the Materials except as expressly permitted by this Agreement;

b. rent, lease or otherwise make available any of the Materials to any third party, except as expressly permitted by this Agreement;

c. assign this Agreement or transfer any of the Materials without the express written consent of Intel;

d. modify, adapt or translate any of the Materials, in whole or in part, except as provided in this Agreement;

e. decompile, disassemble or reverse engineer any of the Materials;

f. remove or in any manner alter any product identification, proprietary, trademark, copyright or other notices contained in the Materials;

g. attempt to modify or tamper with the normal function of a license manager that regulates usage of the Materials; or

h. use Intel's name, logo or any Intel trademark without Intel's written permission.

3.0 OWNERSHIP: The Materials are and shall remain the property of Intel or its third party suppliers. Licensee understands and agree that no license under any Intel patent, copyright (except as expressly described in Section 2.1 above), trade secret or other intellectual property right is granted or conferred upon Licensee either expressly, by implication, inducement, estoppel or otherwise, and that any further license under such intellectual property rights must be express and in writing. Title in and to any permitted derivative works of the Materials shall be held by Licensee subject to Intel's underlying ownership of the Materials.

4.0 FEEDBACK: Licensee is not obligated to provide Intel with comments or suggestions regarding the Materials. However, should Licensee provide Intel with any feedback, input, designs, comments or suggestions for the modification, correction, improvement or enhancement of any of the Materials (collectively, "**Feedback**"), then Licensee hereby grants to Intel a non-exclusive, perpetual, irrevocable, worldwide, royalty-free license under Licensee's intellectual property rights in such Feedback, including the right to sublicense it, and the rights to use and disclose it in any manner Intel chooses, and to display, perform, create derivative works, copy, make, sell and otherwise dispose of Intel's and its sublicensees' products embodying such Feedback in any manner and via any media Intel chooses without reference to the source of such Feedback.

5.0 AUDITS: Intel reserves the right, not more than once per year, to conduct an audit of Licensee's activities relating to this Agreement upon not less than five (5) business days prior written notice and during Licensee's normal business hours solely to verify Licensee's compliance with the terms and conditions of this Agreement. If any such audit discloses substantial material breaches by Licensee, without limiting any other remedies Intel may have, Licensee shall reimburse Intel for the reasonable costs of such audit (including Intel employee time).

6.0 DISCLAIMER OF WARRANTIES

NEITHER INTEL NOR ITS SUPPLIERS MAKE ANY REPRESENTATION OR WARRANTY OR CONDITION OF ANY KIND, WHETHER EXPRESS OR IMPLIED (EITHER IN FACT OR BY OPERATION OF LAW), WITH RESPECT TO ANY OF THE LICENSED MATERIALS. INTEL AND ITS SUPPLIERS EXPRESSLY DISCLAIM ALL EXPRESS AND IMPLIED WARRANTIES OR CONDITIONS, INCLUDING WITHOUT LIMITATION MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. WITHOUT LIMITING THE FOREGOING, INTEL AND ITS SUPPLIERS DO NOT WARRANT THAT THE SOURCE CODE OR OBJECT CODE IS ERROR-FREE OR THAT ITS OPERATION WILL BE SECURE, ERROR-FREE OR UNINTERRUPTED, AND HEREBY DISCLAIM ANY AND ALL LIABILITY ON ACCOUNT THEREOF. ALL MATERIALS ARE LICENSED ON AN "AS-IS" BASIS AND NEITHER INTEL NOR ITS SUPPLIERS WILL PROVIDE ANY SUPPORT, ASSISTANCE, INSTALLATION, TRAINING OR OTHER SERVICES HEREUNDER. INTEL AND ITS SUPPLIERS MAY PROVIDE ANY CORRECTIONS, UPDATES, ENHANCEMENTS OR EXTENSIONS AT THEIR SOLE DISCRETION.

7.0 LIMITATION OF LIABILITY

IN NO EVENT WILL INTEL OR ITS SUPPLIERS BE LIABLE IN ANY WAY FOR: (A) ANY REPRESENTATION OR WARRANTY MADE TO ANY THIRD PARTY BY LICENSEE OR ITS ANY AGENT; (B) ANY FAILURE OF ANY OF THE MATERIALS TO PERFORM AS PLANNED; OR (C) ANY DAMAGE OR LIABILITY RESULTING IN ANY WAY FROM ANY USE OF THE MATERIALS.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, INTEL AND ITS SUPPLIERS SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, IN RELATION TO THIS AGREEMENT.

IN NO EVENT SHALL INTEL'S AGGREGATE LIABILITY FOR ANY CLAIMS UNDER OR RELATED TO THIS AGREEMENT EXCEED ONE THOUSAND DOLLARS ($1,000).

.

8.0 CONFIDENTIALITY: Licensee acknowledges that Intel considers the Source Code Intel's confidential trade secret, and shall treat it as such in accordance with Licensee's confidentiality agreement with Intel or, if no such agreement has been agreed by Intel and Licensee, in accordance with Intel's standard confidentiality agreement generally used for similar development licenses at the time the Materials are provided to Licensee.

9.0 TERM, TERMINATION AND EFFECT OF TERMINATION

9.1 TERM: This Agreement shall commence when Licensee copies, installs or otherwise uses any of the Materials provided by Intel hereunder, and shall remain in effect until terminated by either party.

9.2 TERMINATION: Either Intel or Licensee may terminate this Agreement at any time, with or without cause, on thirty (30) days written notice. This Agreement shall also terminate automatically and immediately upon any breach by Licensee of any of the license restrictions in Subsection 2.2. Any such termination shall be without prejudice to any other remedy available to either party, at law or in equity.

9.3 EFFECT OF TERMINATION: Upon termination of the Agreement for any reason, Licensee shall (a) cease all distribution and other use of the Materials, (b) at Intel's option, either return to Intel or destroy the original and all full or partial copies of the Materials, and (c) certify in writing to Intel that they have been destroyed. In addition, in the event Licensee breaches any of the license restrictions in Subsection 2.2, upon written request by Intel, Licensee shall cease all distribution and other use of any derivative works of the Materials, and provide written certification of same to Intel. Irrespective of the basis of termination, however, Licensee may retain one (1) copy of the Materials solely for Licensee's own internal use in supporting its products.

9.4 SURVIVAL: Those provisions of this Agreement, which by virtue of their nature and surrounding circumstances, reasonably should survive termination of this Agreement shall so survive (including, without limitation, Subsection 2.2, Sections 3.0 through 8.0, Subsections 9.3 and 9.4 and 11.0).

10.0 EXPORT COMPLIANCE: Licensee shall not export, either directly or indirectly, any of the Materials or any product, service or technical data or system incorporating any of the Materials or derivative works thereof in violation of any U.S. export law or without first obtaining all licenses and other approvals required by the U.S. Department of Commerce and any other agency or department of the U.S. government.

11.0 U.S. GOVERNMENT RESTRICTED RIGHTS: The Materials, technical data and computer software covered by this Agreement is a “Commercial Item,” as such term is defined by the FAR 2.101 (48 C.F.R. 2.101) and is “commercial computer software” and “commercial computer software documentation” as specified under FAR 12.212 (48 C.F.R. 12.212) or DFARS 227.7202 (48 C.F.R. 227.7202), as applicable. This commercial computer software and related documentation is provided to end users for use by and on behalf of the U.S. Government, with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Use for or on behalf of the U.S. Government is permitted only if the party acquiring or using this software is properly authorized by an appropriate U.S. Government official. This use by or for the U.S. Government clause is in lieu of, and supersedes, any other FAR, DFARS, or other provision that addresses Government rights in the computer software or documentation covered by this license. All copyright licenses granted to the U.S. Government are coextensive with the technical data and computer software licenses granted herein. The U.S. Government shall only have the right to reproduce, distribute, perform, display, and prepare derivative works as needed to implement those rights.

12.0 GENERAL

12.1 GOVERNING LAW AND VENUE: Any claim arising under or relating to this Agreement shall be governed by the internal substantive laws of the State of Delaware or federal courts located in Delaware, without regard to principles of conflict of laws. Each party hereby agrees to jurisdiction and venue in the courts of the State of Delaware for all disputes and litigation arising under or relating to this Agreement.

12.2 SEVERABILITY: If any paragraph, provision, or clause in this Agreement shall be found or held to be invalid or unenforceable in any jurisdiction in which this Agreement is being performed, the remainder of this Agreement shall be valid and enforceable and the parties shall use good faith to negotiate a substitute, valid and enforceable provision which most nearly effects the parties' intent in entering into this Agreement.

12.3 ENTIRE AGREEMENT: This is the complete and exclusive Agreement between the parties relating to this subject matter. No amendment shall be effective unless in writing signed by authorized representatives of both parties.