Intel® Identity Protection Technology with Public Key Infrastructure (Intel® IPT with PKI)

User Guide

Version 4.3

Document Release Date: July 14, 2017

Legal Notices and Disclaimers

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

No computer system can be absolutely secure.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.

Intel, Intel Core, Intel vPro, and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Java is a registered trademark of Oracle and/or its affiliates.

Bluetooth is a trademark owned by its proprietor and used by Intel Corporation under license.

© 2016-2017 Intel Corporation

Table of Contents

1 Introduction **1**
1.1 Overview 1
1.2 Service and Storage Providers 2
1.3 Protected Transaction Display 3
1.3.1 Switchable Graphics 4
1.3.2 PIN Throttling Mechanism 4
1.3.3 PIN Policy Settings 5

2 Prerequisites **6**
2.1 Using the Pre-Check Tool 8

3 Installation **10**
3.1 Preparing the Certification Authority 12
3.1.1 Supported Server Operating Systems 12
3.1.2 Unsupported Certificate Template Settings 12
3.1.3 Installing the CA Components 13

4 Functionality Testing **14**
4.1 Architecture and Tests Overview 15
4.2 Using the Validation Tool 16
4.3 Test Result Examples 18

5 Setting Up Attestation **19**
5.1 Overview of Attestation 19
5.2 Installing the Revocation Lists 21
5.2.1 Downloading the Revocation Lists 21
5.2.2 Distributing the Revocation Lists 22

6 Logging **23**

1 Introduction

This guide describes how to install and use Intel® Identity Protection Technology with Public Key Infrastructure (Intel® IPT with PKI).

1.1 Overview

Intel IPT with PKI uses the Intel® Management Engine (Intel® ME) in supported platforms to provide a hardware based security capability. Intel IPT with PKI provides hardware enhanced protection of RSA cryptographic keys. The Intel IPT with PKI capabilities are exposed as a Cryptographic Service Provider (CSP) or a Key Storage Provider (KSP) via the Microsoft* CSP / KSP software layer. Software that supports the use of cryptographic features through the Microsoft CSP / KSP software layer can use Intel IPT with PKI to:

- Securely generate tamper resistant, persistent RSA key pairs in hardware
- Generate PKI certificates from hardware protected RSA key pairs
- Perform RSA private key operations within a protected hardware environment
- Protect key usage via PINs using Intel IPT with Protected Transaction Display (Intel IPT with PTD)

Both the RSA keys and the PKI certificates generated by Intel IPT with PKI are stored on the hard drive. The RSA keys are first wrapped within the hardware with something called the Platform Binding Key (PBK) before being stored on the hard drive. The PBK is unique for each platform. When the RSA key is needed, it must be brought back into the Intel ME to be unwrapped.

The RSA keys and certificates created by Intel IPT with PKI support existing PKI usage models. Some typical usage scenarios include:

- VPN authentication
- Email and document signing
- SSL web site authentication
- Encryption and decryption of data

Third-party applications based on the Microsoft CSP / KSP software can use Intel IPT with PKI and derive the benefits of enhanced private key protection.

1.2 Service and Storage Providers

Intel IPT with PKI includes these service and storage providers.

Name	Description
Intel IPT CSP – Non-Exportable Keys	The RSA private keys created using this CSP can only be used on the computer on which they were generated and cannot be exported. This CSP is sufficient for use cases where if the computer fails a backup of the private key is not required. **Note:** Do not use this CSP to encrypt files.
Intel IPT CSP – Exportable Keys	This CSP includes the same functionality as the "Non-Exportable" CSP. But, in addition, the RSA private keys created using this CSP can be exported and imported using a migration authority. Use this CSP if you want to encrypt and decrypt files using Intel IPT with PKI. **Note:** • This CSP can only be installed and used on Intel® vPro™ systems. • This CSP is supported only on systems with Intel ME Firmware 10.0.45.1020 and higher, and cannot be installed on systems with a lower version of the Intel ME Firmware. • When using the installer wizard, this CSP is NOT selected by default (if you want to install it, you must specifically select it).
Intel IPT Non-Exportable Key Storage Provider	This KSP implements the RSA algorithm functionality of the Microsoft KSP software layer. The RSA private keys created using this KSP can only be used on the computer on which they were generated and cannot be exported. **Note:** • This KSP only supports the RSA algorithm. All other algorithms available when using the Microsoft KSP software layer are NOT supported by this KSP. • This KSP only supports key lengths of 1024 bit and 2048 bits. All other key lengths available when using the Microsoft KSP software layer are NOT supported.

1.3 Protected Transaction Display

Intel IPT with PKI includes an option to create the RSA keys with PIN protection. When this option is implemented, the user must supply the PIN whenever they want to use the key. The PIN entry itself is protected using Intel IPT with PTD. Intel IPT with PTD protects the PIN by allowing the Intel ME to directly draw the keypad and accept mouse clicks as input. In this way, software running on the main CPU does not have access to what is actually displayed on the screen even though the user can see it.

These are the main features of Intel IPT with PTD:

- Software based screen scraping or malware attacks that attempt to perform a screen capture of the keypad cannot view the actual PIN number layout. Instead, the entire keypad is blacked out, as shown in the screenshots in this document.
- Each time the keypad window is presented, the numeric keypad is randomized. This means that the mouse click locations used to enter the PIN change every time. Capturing the mouse click pattern for successful PIN entry cannot be used for subsequent PIN entries.
- Mouse clicks for the PIN entry are translated and used within the protective hardware. The actual PIN value is not exposed outside of the hardware.
- A "PIN throttling mechanism" tracks the number of incorrect PIN entry attempts, and at specific intervals will refuse additional PIN attempts for a specific period of time. This feature minimizes brute force attacks on the PIN (see PIN Throttling Mechanism on the next page).
- Keyboard entry of the PIN is not allowed. This feature minimizes keyboard logger attacks.

1.3.1 Switchable Graphics

The Switchable Graphics feature allows you to switch between using the Intel graphics and a discrete graphics controller in a laptop or notebook computer. You can switch between the enhanced battery life of the Intel graphics while running on laptop battery power and the performance capabilities of the discrete graphics controller while the notebook is plugged into AC power. The Intel IPT with PKI providers (CSP and KSP) use features that are only available with Intel graphics. If you are experiencing issues with Intel IPT with PKI and are using Switchable Graphics try changing the preferences for the particular application calling the CSP/KSP. The specific preferences will depend on the discrete graphics controller on the system.

1.3.2 PIN Throttling Mechanism

When a user enters an invalid PIN for a PIN protected key, Intel IPT begins an invalid PIN counter. After a number of invalid PIN entries, the Intel IPT with PKI system will enter a mode where PIN entry is locked out for a specific period of time. This feature limits the effectiveness of brute force attacks against a key's PIN. As more invalid PIN attempts are made, the PIN entry lockout time period increases.

This table shows the lockout time periods for the number of invalid PIN entries.

Number of Incorrect PIN Attempts	Time (in minutes) before Next PIN Attempt
1 – 4	0
5 – 7	1
8 – 11	10
12 +	30

The invalid PIN counter will reset to zero 60 minutes after the last invalid PIN attempt. When the hardware is in PIN throttling mode, other operations, such as the usage of a key that is not PIN protected, are not affected.

Note:

- The PIN throttling mechanism does not support separate invalid PIN counters for each user. The throttling mechanism, when activated, is activated for all users. (This means that all users of the computer will need to wait the required time for the counter to be reset before they can use PTD.)
- Entering a valid PIN does not reset the invalid PIN counter back to zero. If the counter was already a high value (because of several invalid PIN entries), future invalid PIN entries will activate the mechanism sooner than necessary.

1.3.3 PIN Policy Settings

The PIN policy settings provide a mechanism to define the complexity requirements for a valid pin for the secure PIN. The PIN policy settings are located in the registry at:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Intel\Intel IPT with PKI`

This table describes the settings that you can change.

Value	Description	Default Value
`PinMinLength`	The minimum acceptable length for the PIN. This value must be greater than or equal to 4. The maximum supported value is 10.	4
`PinMinUnique`	The minimum number of unique digits required in the PIN. This value must be greater than or equal to 3. If this value is greater than the `PinMinLength` the `PinMinLength` value will be used.	3
`PinCacheTimeout`	The time in minutes that a PIN will be cached on the system. The maximum supported time is 10,080 minutes (one week). PIN caching provides a better user experience, with a tradeoff in security. Keep in mind that if PIN caching is turned off, or set for less than 60 minutes, it is possible a user will be asked to enter their PIN, but the invalid PIN tries counter has not reset to zero. This would give a user fewer attempts to correctly enter the PIN before the lockout times take effect. **Note:** The cache is deleted each time the user logs off or the platform is restarted.	10
Note: If invalid values for these parameters are set in the registry then the nearest valid value for that parameter will automatically be used.		

2 Prerequisites

Prerequisite	Details
Processor	The platform must have a 4th generation or higher processor belonging to one of these families of processors: • Intel® Core™ • Intel® Core™ M • Intel® Core™ vPro™ • Intel® Core™ M vPro™ • Intel® Xeon® E3 (v5 or higher) **Note:** Some features are only available on Intel vPro systems (see Service and Storage Providers on page 2).
Intel ME Firmware	Intel Management Engine Firmware Corporate SKU: • Intel ME 9.1 (from version 9.1.35 only) • Intel ME 9.5 (from version 9.5.55 only) • Intel ME 10.0 • Intel ME 11.0 (from 11.0.0.1157 only) • Intel ME 11.6 (from 11.6.0.1117 only) **Note:** • For Intel ME 11.0, version 11.0.0.1202 is the minimum version for platforms that have the Intel Sensor Service enabled. • Some versions of the firmware do not support all features (see Service and Storage Providers on page 2).
Intel ME Software	Intel Management Engine Software version 11.6.0.1019 or higher. **Note:** The Intel ME software installer automatically installs several components. These are the main components required and used by Intel IPT with PKI: • Intel Management Engine Interface (Intel MEI) driver • Intel Dynamic Application Loader (Intel DAL) • The Java Host Interface (JHI) service • Intel Identity Protection Technology (Intel IPT)
Operating System	• Windows* 10 (64-bit) build 10.0.14393.222 or higher • Windows 8.1 (32-bit and 64-bit) • Windows 7 (32-bit and 64-bit) **Note:** Windows 10 RS2 is not currently supported

Prerequisite	Details
Integrated Graphics	Version 21.20.16.4481 or higher of the Intel HD Graphics driver must be installed. **Note**: See also Switchable Graphics on page 4.
Intel IPT	Intel IPT with PKI depends on Intel IPT DLLs that are installed as part of the Intel ME software installer, which is supplied with the firmware kit. This software must be installed before installing Intel IPT with PKI.
* Other names and brands may be claimed as the property of others.	

2.1 Using the Pre-Check Tool

The `Tools\Pre-Check_Tool` folder located in the root of this package contains a pre-check tool that you can use to check if a platform supports Intel IPT with PKI. To use the tool, open a command prompt with administrator privileges and run `IPTPKI_PreCheck.exe`. When all tests pass, the result summary is highlighted in green.

```
D:\Tools\Pre-Check_Tool>IPTPKI_PreCheck.exe

#### Intel(R) IPT with PKI Prerequisites Test ####################

    1. PASS - CPU: Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz
    2. PASS - Intel ME Software version: 11.7.0.1010
    3. PASS - Intel ME Firmware version: 11.0.0.1202
    4. PASS - Intel ME Firmware type: Corporate
    5. PASS - OS version: Windows 10 (10.0.14393)
    6. PASS - Intel DAL service: Installed and running
    7. PASS - Intel DAL version: 11.7.0.1010
    8. PASS - Intel DAL virtual machine type: Intel
    9. PASS - Protected Transaction Display: Enabled
   10. PASS - Intel Graphics Driver version: 21.20.16.4550

Status: This platform includes all prerequisites for Intel IPT with PKI

#### Prerequisites Test Passed ###################
```

If one of the tests fail, the result summary is highlighted in red. For each failed test, details are shown.

```
G:\Tools\Pre-Check_Tool>IPTPKI_PreCheck.exe

#### Intel(R) IPT with PKI Prerequisites Test ####################

    1. PASS - CPU: Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz
    2. PASS - Intel ME Software version: 11.7.0.1010
    3. PASS - Intel ME Firmware version: 11.0.0.1202
    4. PASS - Intel ME Firmware type: Corporate
    5. PASS - OS version: Windows 10 (10.0.14393)
    6. FAIL - Intel DAL service: Installed but stopped
    7. FAIL - Intel DAL version: Unknown
    8. PASS - Intel DAL virtual machine type: Intel
    9. PASS - Protected Transaction Display: Enabled
   10. PASS - Intel Graphics Driver version: 21.20.16.4550

Status: This platform supports Intel IPT with PKI, but does not include all prerequisites

Details:
   Test  #6: Intel DAL service is installed but not running
   Test  #7: Failed to initialize the JHI DLL. Check that Intel ME Software is installed correctly

#### Prerequisites Test Failed ##################
```

Note:

The pre-check tool:

- Must be run from a command prompt that was opened with administrator privileges.
- Relies on the Intel MEI driver to run some of the tests. If the Intel MEI driver is not installed, these tests might fail.

If a tests fails for one of these reasons it will be reported in the details for that test (in the "Details" section). Failures for these reasons do not necessarily mean that the platform cannot support Intel IPT with PKI. Correct the problem and then run the pre-check tool again.

This table describes the tests run by the pre-check tool.

Test	Details
1	Checks that the processor belongs to one of the supported families of processors. **Note:** Test #1 is expected to fail on engineering sample, pre-quality sample, and quality sample platforms. This is because on these types of platforms the CPU returns an unrecognized value. Ignore this failure.
2	Checks the registry to verify that the installed version of Intel ME Software is supported. In addition, this test also checks that the Intel MEI driver is installed. The driver is usually located in the "System devices" section of the Device Manager window. If the driver is not installed, some of the remaining tests will fail (because they depend on communications via the driver).
3	Checks that the Intel ME Firmware version is supported
4	Checks that the Intel ME Firmware is the Corporate SKU (the Consumer SKU is not supported)
5	Checks that the operating system is supported
6	Checks that the Intel DAL service is installed and running (the name shown in the Services window is "Intel Dynamic Host Application Loader Host Interface Service")
7	Checks communications with Intel DAL by trying to get the version number of Intel DAL via an API of Intel DAL
8	Checks that the Intel DAL virtual machine type is "Intel". Older versions of Intel DAL included a non-Intel virtual machine that is not supported by Intel IPT with PKI. This test might return "Unknown" on some older versions of DAL. Both "Unknown" and "Non-Intel" mean that the platform does not support Intel IPT with PKI.
9	Checks that Protected Transaction Display is enabled in the registry. This check does not perform a full test of PTD. To fully test PTD functionality, run the Intel IPT Compliance tests that are a prerequisite for Intel IPT with PKI.
10	Checks that the Intel Graphics Driver is installed and that the version is supported

3 Installation

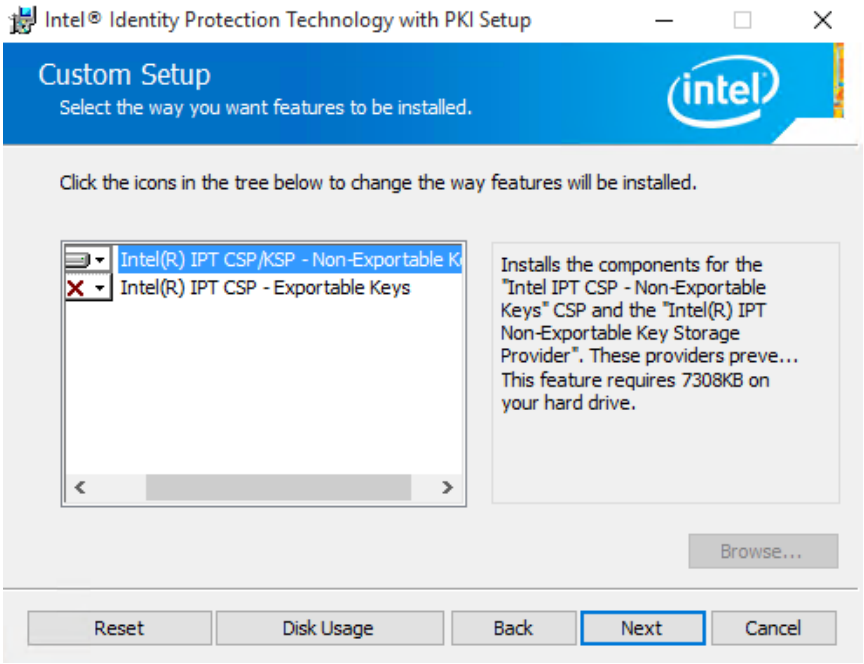
This section describes how to install Intel IPT with PKI.

The installers are located in the `Client_Installers` folder in the root of this package. There are different installers for 32-bit and 64-bit systems, but the installation procedure is the same for both installers. You can install Intel IPT with PKI using the installer wizard or a CLI command. (The installer wizards require version 3.5 of Microsoft .NET Framework to be installed on the computer.)

To install Intel IPT with PKI (using the wizard):

1. Make sure that the system meets the prerequisites described in Prerequisites on page 6.
2. Double-click the correct installer for your system:
   - 64-bit systems: `Intel_IPT_PKI_x64_[version].msi`
   - 32-bit systems: `Intel_IPT_PKI_x86_[version].msi`

   The Welcome window opens.
3. Click **Next**. The End User License Agreement window opens.
4. Select **I accept the terms in the License Agreement** and click **Next**. The Custom Setup window opens.



5. Select the providers that you want to install:
   - **Intel(R) IPT CSP/KSP - Non-Exportable Keys** – This option installs the "Non-Exportable Keys" providers (both CSP and KSP).
   - **Intel(R) IPT CSP - Exportable Keys** – This option installs the "Exportable Keys" provider (CSP only). This option is only shown if the system is an Intel® vPro™ system. If you also want to install this CSP, click the drop-down list button and select **Entire feature will be installed on local hard drive**.
6. Click **Next** and then click **Install** to start the installation.

To silently install Intel IPT with PKI:

1. Make sure that the system meets the prerequisites described in Prerequisites on page 6.
2. Open an administrative command prompt.
3. Use the required command:
   - To install only the "Non-Exportable Keys" providers (CSP and KSP):

     ```
     msiexec /i [installer_filename].msi /qn ADDLOCAL=NonExportable
     ```

   - To install only the "Exportable Keys" provider (CSP only):

     ```
     msiexec /i [installer_filename].msi /qn ADDLOCAL=Exportable
     ```

   - To install all available providers (CSPs and KSPs):

     ```
     msiexec /i [installer_filename].msi /qn ADDLOCAL=All
     ```

     Note:

     The "Intel IPT CSP – Exportable Keys" provider will only be installed if the system is an Intel® vPro™ system and has the supported version of Intel ME (see Service and Storage Providers on page 2).

3.1 Preparing the Certification Authority

A Microsoft Certification Authority (CA) is necessary if you want to do any of these:

- Use Enterprise CA templates when generating certificates
- Use the attestation capabilities of Intel IPT with PKI (see Setting Up Attestation on page 19)
- Use the secure export / import capabilities of Intel IPT with PKI

To enable these capabilities you need to install a set of "CA Components" for Intel IPT with PKI on the server where your organization's CA is located. The installer for these CA Components is included in this package.

Note:

The purpose of the CA Components is to enable the CA to identify the Intel IPT with PKI cryptographic service providers. Installing these CA Components is NOT a full installation of Intel IPT with PKI. Functionality using the public/private key operations in the Intel hardware of the CA is not supported.

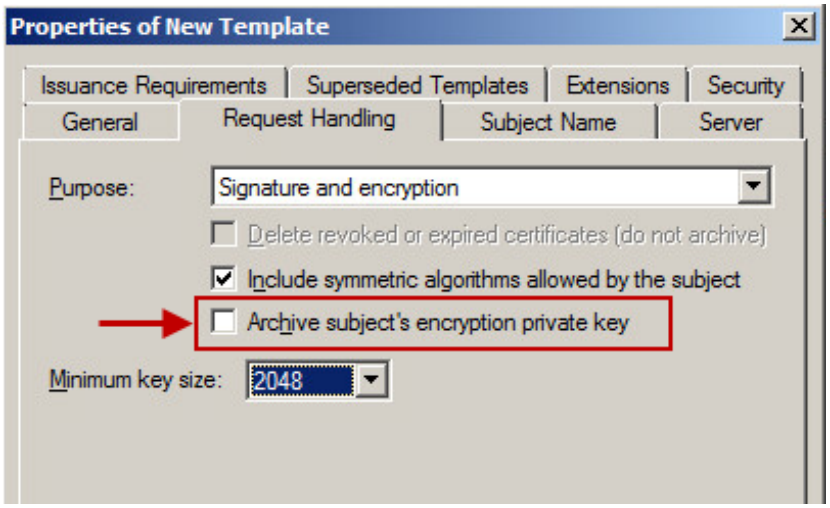
3.1.1 Supported Server Operating Systems

The CA Components of Intel IPT with PKI are supported on these server operating systems:

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

3.1.2 Unsupported Certificate Template Settings

The certificate template option to archive the subject's encryption private key is NOT supported. Make sure that the **Archive subject's encryption private key** check box (in the Request Handling tab) is NOT selected. Selecting this option will cause the enrollment to fail with an "invalid parameter" error message.

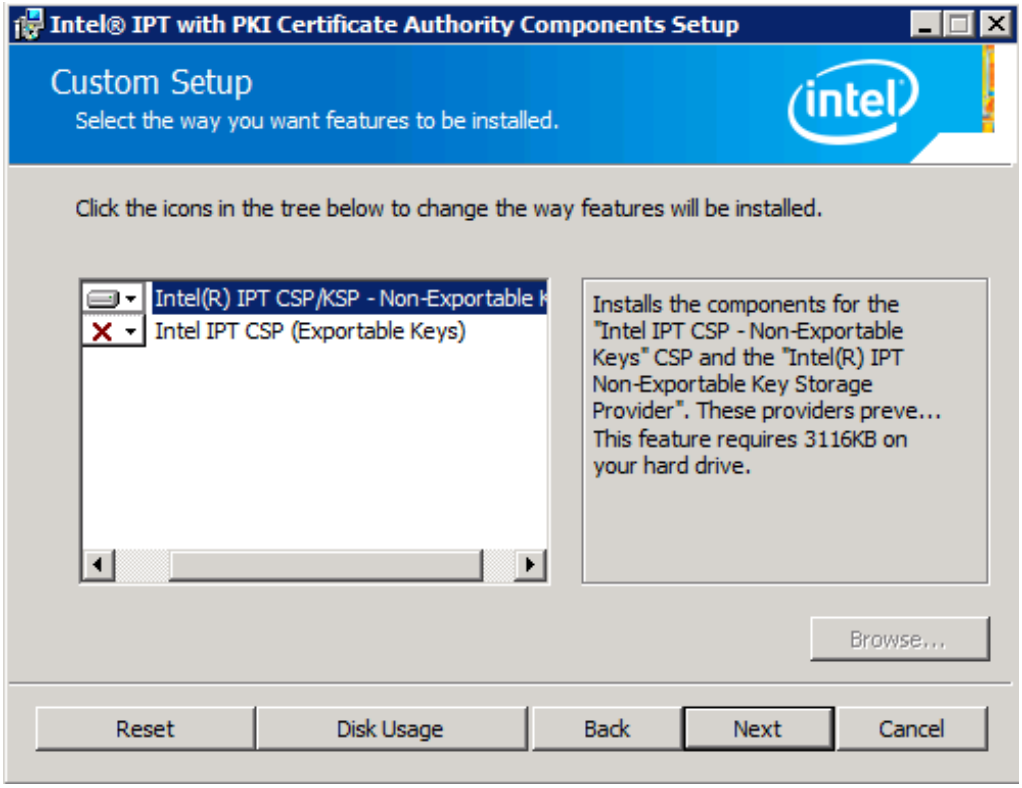


3.1.3 Installing the CA Components

The installer for the CA Components of Intel IPT with PKI is located in the `MS_CA_Installer` folder in the root of this package. You can install Intel IPT with PKI using the installer wizard or a CLI command.

To install the CA Components of Intel IPT with PKI (using the wizard):

1. On the computer where the CA is located, double-click: **Intel_IPT_PKI_CA_Components_x64**. The Welcome window opens.
2. Click **Next**. The End User License Agreement window opens.
3. Select **I accept the terms in the License Agreement** and click **Next**. The Custom Setup window opens.



4. Select the CSPs that you require, according to the features you want to implement:
   - **Intel IPT CSP Non-Exportable Keys** – This CSP only supports attestation.
   - **Intel IPT CSP Exportable Keys** – This CSP supports attestation and secure export/import. By default this CSP is not selected for installation. To install this CSP, click the drop-down list button and select **Entire feature will be installed on local hard drive**.
5. Click **Next** and then click **Install** to start the installation.

To silently install the CA Components of Intel IPT with PKI:

1. On the computer where the CA is located, open an administrative command prompt.
2. Use the required command:
   - To install only the "Intel IPT CSP – Non-Exportable Keys" CSP:

     ```
     msiexec /i [installer_filename].msi /qn ADDLOCAL=CSPNonExportable
     ```

   - To install only the "Intel IPT CSP – Exportable Keys" CSP:

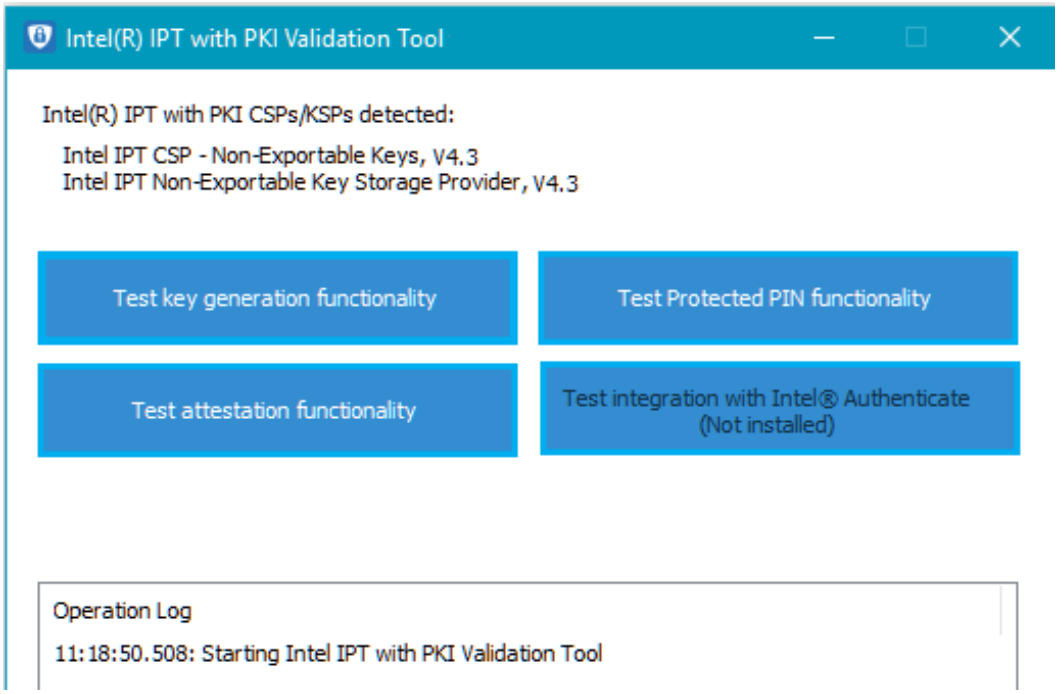
     ```
     msiexec /i [installer_filename].msi /qn ADDLOCAL=CSPExportable
     ```

   - To install all available CSPs:

     ```
     msiexec /i [installer_filename].msi /qn ADDLOCAL=All
     ```

4 Functionality Testing

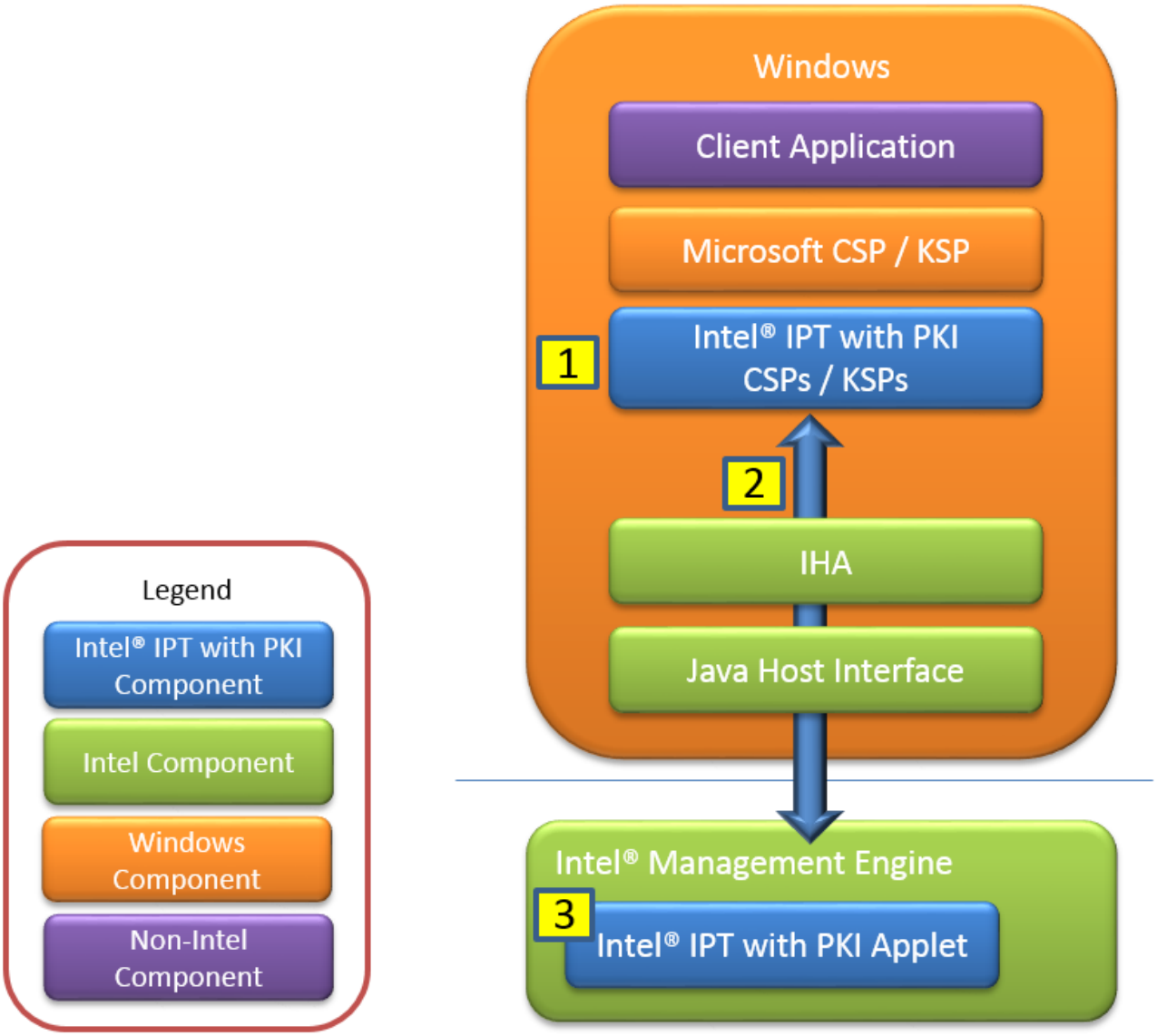
The `Tools\Validation_Tool` folder located in the root of this package contains a validation tool. The validation tool is a simple GUI that you can use to validate that Intel IPT with PKI is installed and working correctly on the platform.



4.1 Architecture and Tests Overview

When you run the tests, the validation tool:

- Confirms that Intel IPT with PKI is installed and recognizable using the Microsoft CSP / KSP interface to make calls to the Intel IPT with PKI providers (1).
- Exercises a communication channel between the Intel IPT with PKI providers and the Intel IPT with PKI applet (2 <---> 3).
- Verifies that end to end software stack communication is successful.



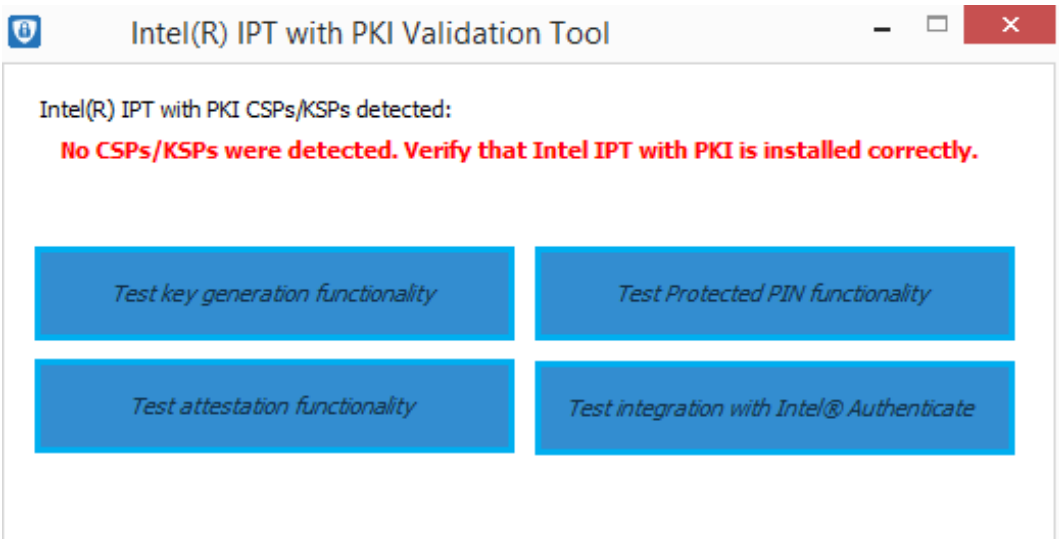
4.2 Using the Validation Tool

This procedure describes how to use the validation tool.

To run the tests:

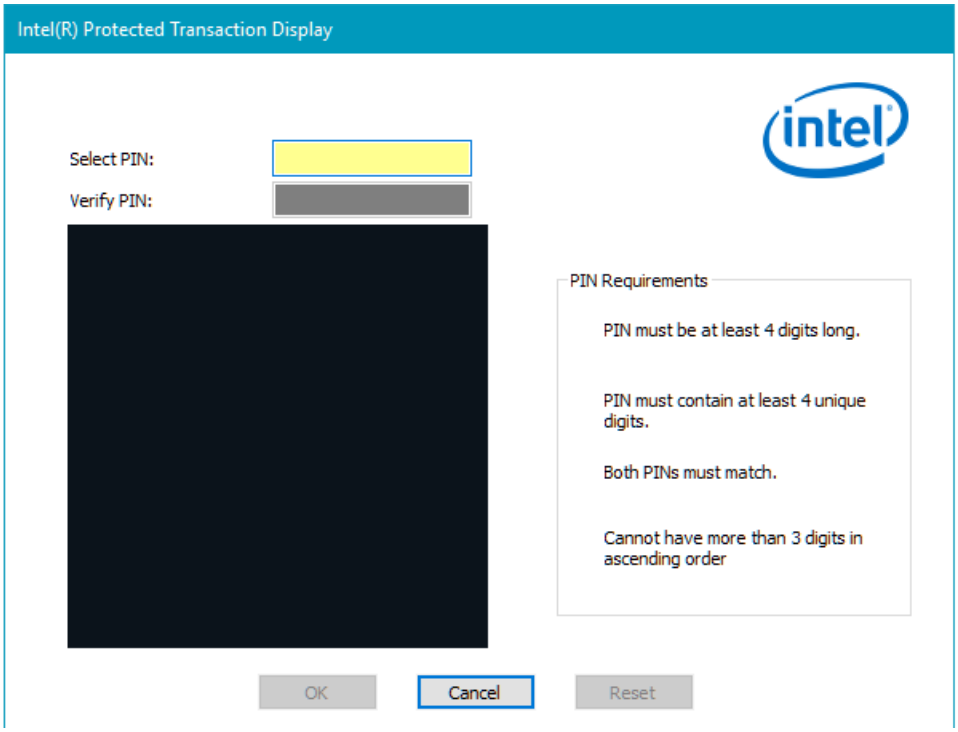
1. Double-click the correct version of the validation tool for your system:
   - 64-bit systems: `IptPkiValidationTool_x64.exe`
   - 32-bit systems: `IptPkiValidationTool_x86.exe`

   The validation tool performs pre-checks on the system. One of these will occur:
   - If the pre-checks failed, the GUI opens but the test buttons are disabled and a red error message is shown:



   This error message indicates that there is a problem with the installation of Intel IPT with PKI. Close the GUI and check that you have installed Intel IPT with PKI.
   - If the pre-checks succeed, the GUI opens with the test buttons enabled. In addition, the Intel IPT with PKI providers that are detected as installed on the system are listed above the test buttons. When you click the test buttons, each test is run on all the installed providers. Continue to step 2.
2. Click **Test key generation functionality**. This test generates a new RSA key, creates a SHA1 hash, and then uses the RSA key to sign the hash. After the test is complete, the test results are displayed (see Test Result Examples on page 18).
3. Click **Test attestation functionality**. This test generates EPID Key Attestation Extension formatted data. Subsequently, the data gets parsed to verify that it is in the valid format. After the test is complete, the test results are displayed (see Test Result Examples on page 18).

4. Click **Test Protected PIN functionality**. This test generates a new RSA key and prompts you to enter a PIN for the key. Next, a SHA1 hash is created. Finally you will be prompted for the PIN of the key so the key can be used to sign the hash. A window with a keypad is shown each time that you need to supply the PIN:



Note:

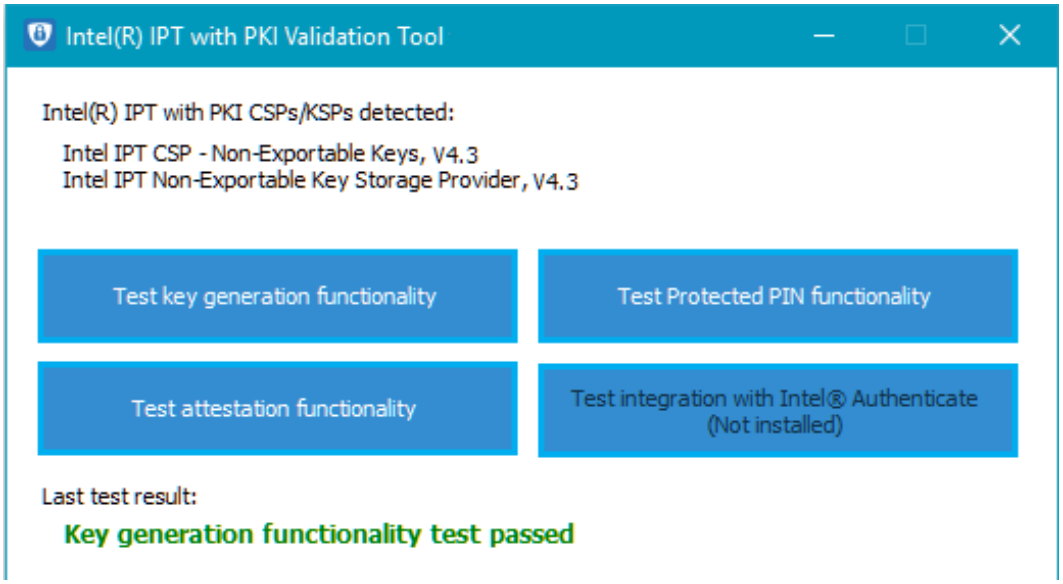
- This test is run for each provider that you installed when installing Intel IPT with PKI. This means that the keypad window will be shown twice for each installed provider. The first time you must enter a PIN, according to the PIN requirements shown on the screen. And the second time you must enter the identical PIN that you entered the first time for that test.
- In this screenshot, the keypad is blacked-out because the keypad is protected from screen capture applications.

After the test is complete, the test results are displayed (see Test Result Examples on the next page).

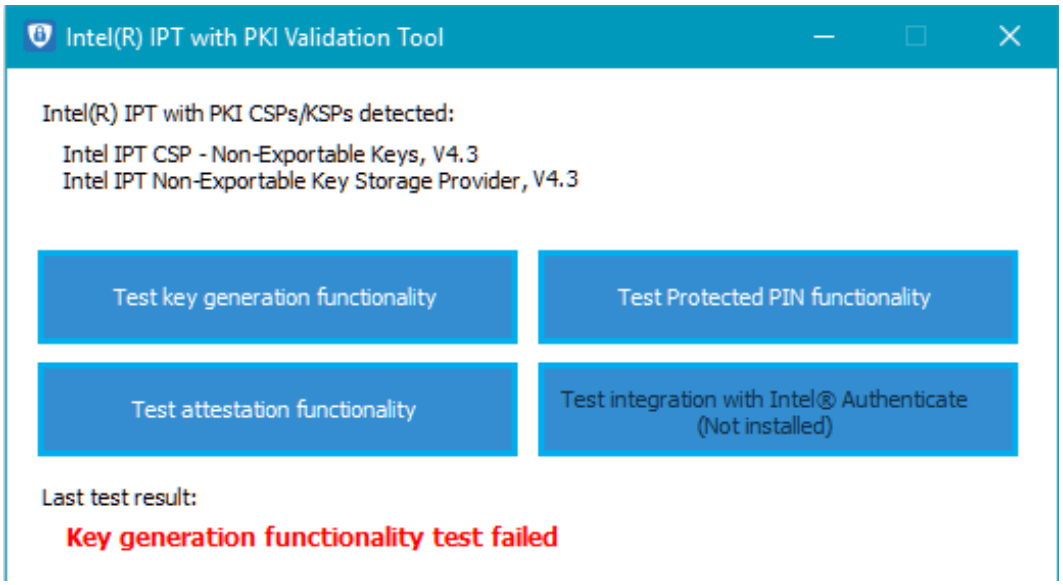
5. Close the validation tool.

4.3 Test Result Examples

This is an example of the message that is shown when a test completes successfully:



This is an example of the message that is shown when a test fails:



This error message indicates that there is a problem with the installation of Intel IPT, or the prerequisites of the system (see Prerequisites on page 6).

5 Setting Up Attestation

This section describes the attestation capabilities of Intel IPT with PKI.

Note:
The attestation capability is only supported on Intel vPro systems.

5.1 Overview of Attestation

Intel IPT with PKI generates and protects the RSA keys that it creates in the trusted execution environment of the Intel ME. Attestation is an additional security layer that enables service providers to verify that they really are "talking" to the trusted execution environment of the Intel ME. By implementing attestation, you can ensure that only requests that really were sent by Intel IPT with PKI are processed by the service provider.

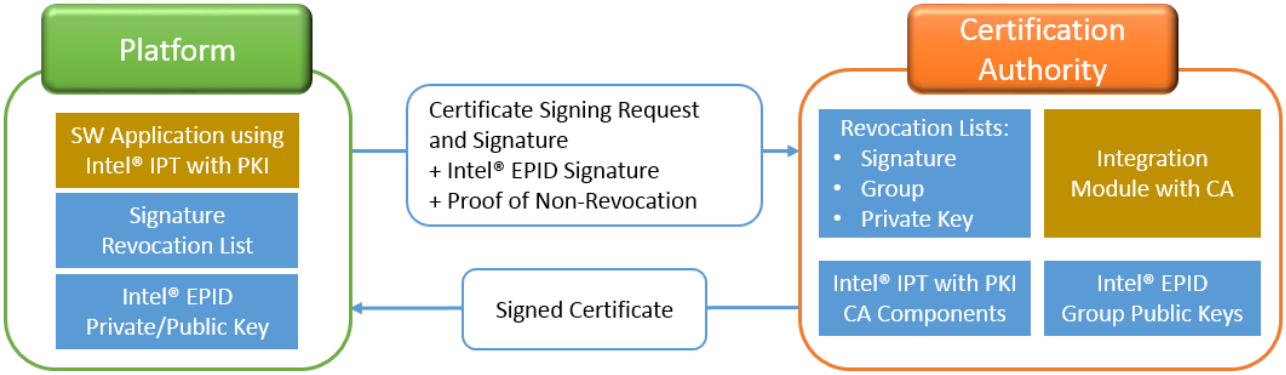
Intel IPT with PKI implements attestation using Intel® Enhanced Privacy ID (Intel® EPID). Intel EPID enables Intel platforms to anonymously prove that they are valid members in a group, without revealing any information about their identity. This table describes the main entities of Intel EPID.

Entity	Description
Authority	In Intel EPID, Intel is the "authority". The authority is responsible for generating the group keys, member keys, parameters, and maintaining revocation lists. These are the two types of keys that are used by Intel EPID: • **Intel EPID Private Key** – Each Intel platform that supports Intel EPID has a unique private key. The private key is burned into the Intel ME by Intel during the manufacturing process. The key is protected by the hardware and cannot be accessed or altered by malware. Each key has one corresponding Intel EPID Group Public Key. • **Intel EPID Group Public Key** – These keys are also created by Intel, with each public key corresponding to multiple Intel EPID private keys. The public keys do not contain any secrets and are digitally signed by Intel. **Note:** An attestation mechanism must support the capability to revoke members or groups when necessary. Intel maintains and publishes three types of revocation lists for Intel EPID. To implement Intel EPID, you must install revocation lists on the verifier and each of the platforms. For more information, see Installing the Revocation Lists on page 21.
Platform	An Intel platform with Intel IPT with PKI installed. If the platform has a valid Intel EPID private key, and is not listed in a revocation list, then it can prove it is a valid member of an Intel EPID group.
Verifier	The verifier is the entity that tries to establish that the platform is a valid member of the group to which it claims it belongs. Because Intel IPT with PKI is dealing with keys and certificates, the verifier role is performed by software on the organization's Certification Authority (CA). The verifier receives the attestation data from the platform and verifies that the platform is a valid group member. If successful, this means that the verifier has actually "talked" to the Intel ME and therefore the request really did originate from Intel IPT with PKI.

The attestation capabilities of Intel IPT with PKI can be used to:

- Enable the CA to verify, before signing the certificate, that a Certificate Signing Request (CSR) really did originate from Intel IPT with PKI.
- Enable IT to backup private keys located in the hardware of the Intel platforms by securely exporting them to a migration authority.

This diagram and the following table describe the flow when using attestation to verify a CSR.



Step	Description
1	The software application using Intel IPT with PKI sends a Certificate Signing Request (CSR) and signature to the organization's CA. For Intel EPID these additional items are also sent: • **Intel EPID Signature** – A data blob containing the Intel EPID attestation properties and settings for this platform. This data blob is signed by Intel IPT with PKI using the unique Intel EPID private key of the platform. • **Proof of Non-Revocation** – Intel IPT with PKI performs an operation (using the signature revocation list) to create proof that the platform is not listed in the signature revocation list.
2	The CA receives the CSR and checks that the signature is valid by performing an RSA operation on the signature using the public key generated by Intel IPT with PKI. (When not using attestation, if the signature is found to be valid, the CA would then process the CSR.)
3	The additional attestation checks are now performed. These checks include validating the Intel EPID signature and verifying that the platform is not included in any of the revocation lists. To implement Intel EPID, you must prepare your CA. For more information, see: • Preparing the Certification Authority on page 12 • Installing the Revocation Lists on the next page **Note:** Some of the attestation checks are processed by DLLs provided by Intel in the "Intel IPT with PKI CA Components" installer. But an additional "integration" module is required to enable these DLLs to be integrated with your CA. This module is currently not provided by Intel.
4	If all verification checks have passed, the CA processes the CSR and sends the signed certificate back to the platform.

5.2 Installing the Revocation Lists

In the Intel EPID ecosystem, the authority (Intel) is the only entity that has the privilege to revoke a member or a group. Once a verifier identifies a platform or group that should be revoked, it notifies the authority with reasons. The authority then examines the request and executes corresponding revocation method if the request is deemed legitimate. In certain cases, the authority may decide to revoke platforms or groups without requests from verifiers.

This table describes the revocation lists and methods supported by Intel EPID.

Revocation Lists	Description
Signature	The authority revokes a platform based on the signature generated by the platform. This revocation method is used when a member has reportedly been misbehaving, but its private key is not yet exposed or known by the authority. The authority can revoke the member by identifying it using a signature the member has previously generated. Misbehavior is defined by the verifiers and the authority. For example, a platform continuously making excessive requests might be considered to be misbehaving.
Private Key	The authority revokes a platform based on the platform's private key. This revocation method is used when a member's private key is proved to be possessed by any party other than the platform itself. For example, if a platform's private key is published on the Internet, then the platform is considered to be compromised (from the Intel EPID perspective).
Group	The authority revokes the entire Intel EPID group by revoking the group public key. Group based revocation is expected to be a rare event and would only happen under limited criteria.

5.2.1 Downloading the Revocation Lists

Intel does not provide an automated download or update mechanism for the Intel EPID revocation lists. Organizations that want to use Intel EPID are responsible to download the revocation lists themselves and then distribute them.

To download the revocation lists:

1. Open a web browser and browse to this URL:http://upgrades.intel.com/content/crl/.
2. Download these three files:
   - `signature_RL.zip` – This zip contains the signature revocation lists for all the groups
   - `private_key_RL.zip` – This zip contains the private key revocation lists for all the groups
   - `EPID.crl` – This is the group revocation list

5.2.2 Distributing the Revocation Lists

After downloading the revocation lists, you must place them in the correct location on the CA server. In addition, you will also need to distribute the signature revocation lists to the platforms where you want to use Intel EPID. (The zip files contain multiple revocation list files. You must open the zip files and place the individual files in the correct locations.)

This table shows where the revocation list files must be installed.

Revocation Lists	Source File	Install On
Signature	`signature_RL.zip`	All platforms and the CA server **Note:** The platforms and the CA server must have the same versions of signature revocation lists installed. If the versions are not identical, then verification will fail. When updating the signature revocation lists, make sure that you update the CA server and the platforms with the same versions.
Private Key	`private_key_RL.zip`	CA server only
Group	`EPID.crl`	CA server only

Note: The default location for the revocation lists is the installation folder:

- CA server:
  `C:\Program Files\Intel\Intel(R)Identity Protection Technology with PKI\Certificate Authority Components`
- Platforms:
  `C:\Program Files(x86)\Intel\Intel(R)Identity Protection Technology with PKI`

You can change the default location for the revocation lists by editing the paths in the registry:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Intel\Intel IPT with PKI`

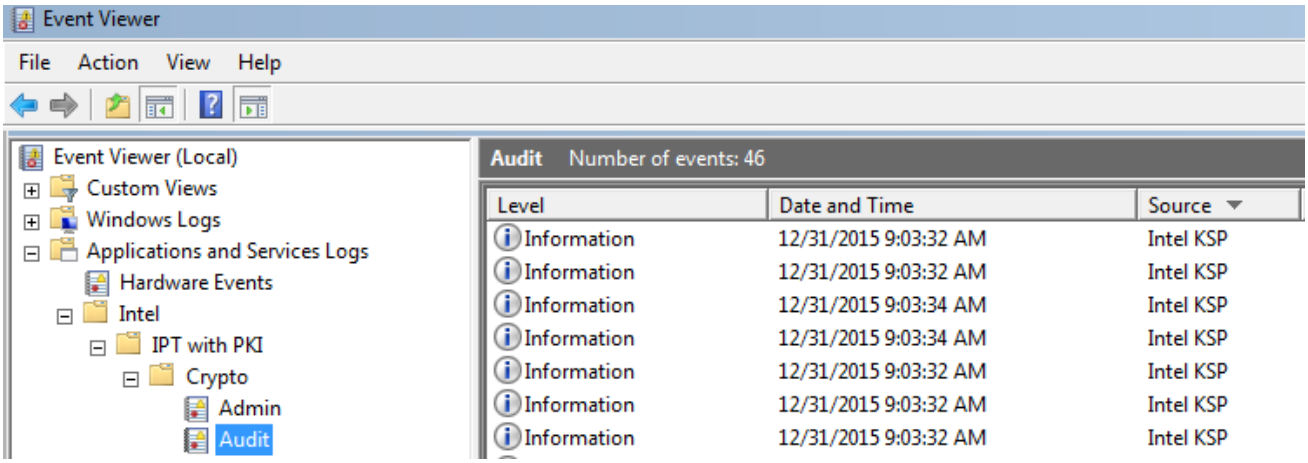
Value	Description
`SigRLPath`	The path to the signature revocation lists
`PrivRLPath`	The path to the private key revocation lists
`EpidCrlPath`	The path to the group revocation lists

Note: If you edit the paths, make sure that you include the full path with a back slash "\" at the end. For example: `C:\Newpath\`.

6 Logging

You can view the logs generated by Intel IPT with PKI in the Event Viewer at this location:

`Applications and Services Logs > Intel > Intel IPT with PKI > Crypto`



The logs are located in these Event Channels:

- **Admin** – This is a legacy log. This log does not include logs from the KSP. By default, only critical errors are logged. To enable logging of all CSP calls, you need to add a registry key DWORD named `iptpkilog` (with a value of 1) to: `HKLM > > SOFTWARE > Policies > Intel > Intel IPT with PKI`.
- **Audit** – This is a new log that has been added from version 4.1. This log is enabled by default and contains logs from both the CSP and the KSP providers. This is the recommended log to use when troubleshooting.