Executive Summary

Intel® Identity Protection Technology (Intel® IPT) is a suite of hardware based two factor authentication technologies built into some Intel® processor-based systems, enabling strong online authentication, lower cost deployment and a simplified user experience. In this whitepaper we explore the use of Microsoft System Center® 2012 Configuration Manager to discover managed systems supporting Intel IPT with One Time Password (OTP) and Intel IPT with Public Key Infrastructure (PKI) and make them ready for activation.

Introduction

Systems with Intel IPT include an embedded hardware based isolated execution environment where security materials such as OTP’s and public private key pairs (used with digital certificates) can be generated and used for authentication, digital signing and encryption operations without interference of oversight by Operating System based malware. Security material generated by Intel IPT is bound to individual system hardware preventing it from being maliciously copied and used on other systems.

Security material can be associated with a personal identification number (PIN) that users must enter before material is used for authentication, digital signing and encryption operations. Intel IPT with Protected Transaction Display (PTD) combines the hardware based isolated execution environment with Intel® HD Graphics to protect the PIN entry process from spoofing by local or remote malware thus verifying the physical presence of authorized users.

Embedding these capabilities into systems maintains the benefits of hardware based security whilst reducing costs associated with procuring, deploying and supporting discrete devices, and from a user perspective, the usage experience is simplified.

To evaluate and deploy Intel IPT, enterprises must be able to discover systems in their estate with Intel IPT support, assess system activation-readiness and where necessary, deploy the required Intel IPT middleware to allow application software to access Intel IPT capabilities. This
Discovering Enterprise Systems with Intel® Identity Protection Technology

This paper describes characteristics of Intel IPT systems that can be used with Microsoft System Center 2012 Configuration Manager to discover systems with Intel IPT support and deploy Intel IPT middleware.

Using Microsoft System Center 2012 Configuration Manager to Detect Systems with Intel Identity Protection Technology with One Time Password Support

Intel IPT with OTP was introduced in 2011 and is supported on systems based on 2nd generation or later Intel® Core™ processors, Intel® Xeon® processors, Intel® Pentium® processors, Intel Celeron® processors, Bay Trail and Clover Trail+ tablets and smartphones based on Intel® Atom™ processors and running Microsoft Windows® 7, Windows® 8.X and Google Android®.

Managed systems supporting Intel IPT with OTP can be detected using the standard hardware inventory information collected by Microsoft System Center 2012 Configuration Manager (SCCM) and selecting systems using criteria shown Figure 1.

![Figure 1 - Criteria for Selecting Systems with Intel IPT with OTP Support](image)

An example SCCM query statement for selecting systems with Intel IPT with OTP support is shown in Figure 2. If security policy demands that users must enter a PIN before Intel IPT performs operations using an OTP, the query statement can be modified slightly to that shown in Figure 3 which selects Intel IPT with OTP systems with Intel HD Graphics support so that Intel IPT with PTD can be used for secure PIN entry. These query statements can be used to define collection membership for an SCCM collection created to contain all systems supporting Intel IPT with OTP.

---

1 When Intel IPT with OTP was first introduced, support was available on Ultrabook™ systems and systems based on 2nd generation Intel Core processors. Updated middleware released since launch supports additional processors.
Discovering Enterprise Systems with Intel® Identity Protection Technology

**Figure 2 - SCCM Query Statement to Select Systems with Intel IPT with OTP Support**

```
select * from SMS_R_System
inner join SMS_G_System_PROCESSOR on SMS_G_System_PROCESSOR.ResourceID = SMS_R_System.ResourceId
where SMS_G_System_PROCESSOR.Manufacturer = "GenuineIntel"
and SMS_G_System_PROCESSOR.CPUPortable like "Intel64 Family 6 Model 698"
```

**Figure 3 - SCCM Query Statement to Select Systems with Intel IPT with OTP and Intel IPT with PTD Support**

```
select * from SMS_R_System
inner join SMS_G_System_PROCESSOR on SMS_G_System_PROCESSOR.ResourceID = SMS_R_System.ResourceId
inner join SMS_G_System_SYSTEM_DEVICES on SMS_G_System_SYSTEM_DEVICES.ResourceId = SMS_R_System.ResourceId
where SMS_G_System_PROCESSOR.Manufacturer = "GenuineIntel"
and SMS_G_System_PROCESSOR.CPUPortable like "Intel64 Family 6 Model 698"
and SMS_G_System_SYSTEM_DEVICES.Name like "Intel(R) HD Graphics"
```

Activation readiness of systems with Intel IPT with OTP support can also be determined using Microsoft SCCM 2012 standard hardware inventory information and selecting systems based on the presence or absence of Intel IPT with OTP middleware using criteria shown in Figure 4.

**Figure 4 - Criteria for Selecting Intel IPT with OTP Systems with Middleware Installed**

Example SCCM query statements implementing this criteria are shown in Figure 5 and Figure 6.

**Figure 5 - SCCM Query Statement to Select Intel IPT with OTP Systems with Middleware Installed**

```
select * from SMS_R_System
inner join SMS_G_System_ADD_REMOVE_PROGRAMS on SMS_G_System_ADD_REMOVE_PROGRAMS.ResourceID = SMS_R_System.ResourceId
where (SMS_G_System_ADD_REMOVE_PROGRAMS.DisplayName like "Intel(R) Management Engine Components")
or (SMS_G_System_ADD_REMOVE_PROGRAMS.DisplayName like "Intel(R) Identity Protection Technology")
or SMS_G_System_ADD_REMOVE_PROGRAMS.DisplayName like "Intel(R) Trusted Execution Engine"
```
Discovering Enterprise Systems with Intel® Identity Protection Technology

The SCCM query statements for detecting activation readiness can be used to define collection membership rules for SCCM collections used to drive the deployment process for Intel IPT with OTP.

An SCCM collection containing Intel IPT with OTP systems that are not activation-ready can be used to target and distribute packages containing missing Intel IPT with OTP middleware. Care should be taken to install the correct middleware on Intel Core processor-based systems. Intel Management Engine Components software needs to be installed on all Intel IPT with OTP systems based on 2nd, 3rd and 4th generation Intel Core processors but Intel IPT software V1.X should only be installed on Intel IPT with OTP systems based on 2nd generation Intel Core processors because the Intel Management Engine Components software for 3rd and 4th generation Intel Core processors already includes Intel IPT with OTP middleware. Intel Trusted Execution Engine software needs to be installed on Intel IPT with OTP systems based on Intel Atom processors.

An SCCM collection containing activation-ready Intel IPT with OTP systems can be used to target and distribute packages containing ISV application software to enroll users for their OTP’s. The enrollment process for OTP’s is dependent on the ISV supplying the OTP based authentication solution.

Using Microsoft System Center 2012 Configuration Manager to Detect Systems with Intel Identity Protection Technology with Public Key Infrastructure Support

Intel IPT with PKI was introduced in 2012 and is supported on systems based on 3rd generation or later Intel® Core™ vPro™ processors, Bay Trail tablets based on Intel Atom processors with Intel® Trusted Execution Engine V1.0² and running Microsoft Windows 7 or Windows 8.X.

Managed systems supporting Intel IPT with PKI can be detected using the standard hardware inventory information collected by Microsoft System Center 2012 Configuration Manager (SCCM) and selecting systems using criteria shown in Figure 7.

² Intel IPT with PKI support on Intel Atom processor-based tablets requires a 64-bit Operating System
Discovering Enterprise Systems with Intel® Identity Protection Technology

Figure 7 - Criteria for Selecting Systems with Intel IPT with PKI Support

An example SCCM query statement for selecting systems with Intel IPT with PKI support is shown in Figure 8. If security policy demands that users must enter a PIN before Intel IPT performs operations using a public-private key pair, the query statement can be modified slightly to that shown in Figure 9 which selects Intel IPT with PKI systems with Intel HD Graphics support so that Intel IPT with PTD can be used for secure PIN entry. These query statements can be used to define collection membership for an SCCM collection created to contain all systems supporting Intel IPT with PKI.

---

Figure 8 - SCCM Query Statement to Select Systems with Intel IPT with PKI Support

```sql
select * from SMS_R_System
inner join SMS_G_System_PROCESSOR on SMS_G_System_PROCESSOR.ResourceID = SMS_R_System.ResourceID
inner join SMS_G_System_HARDWARE on SMS_G_System_HARDWARE.ResourceID = SMS_G_System_PROCESSOR.ResourceID
inner join SMS_G_System_HARDWARE_TYPE on SMS_G_System_HARDWARE_TYPE.ResourceID = SMS_G_System_HARDWARE.ResourceID
where SMS_G_System_HARDWARE.Type = 'Processor' and SMS_G_System_HARDWARE.Value like 'Intel%vPro Technology%'
and SMS_G_System_HARDWARE.PROVIDER = 'Manufacturer'
and SMS_G_System_HARDWARE.PROVIDER = 'Intel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_System_HARDWARE.PROVIDER = 'Genuinetel'
and SMS_G_S...
```

Figure 9 - SCCM Query Statement to Select Systems with Intel IPT with PKI and Intel IPT with PTD Support

---

3 To detect systems with Intel vPro technology using Microsoft SCCM 2012 standard hardware inventory, the Intel Management Engine Components software must be installed to enable the Microsoft SCCM client to interrogate the state of the hardware.
Discovering Enterprise Systems with Intel® Identity Protection Technology

Activation readiness of systems with Intel IPT with PKI support can also be determined using Microsoft SCCM 2012 standard hardware inventory information and selecting systems based on the presence or absence of Intel IPT with PKI middleware using criteria shown in Figure 10.

![Figure 10 - Criteria for Selecting Intel IPT with PKI Systems with Middleware Installed](image)

Example SCCM query statements implementing this criteria are shown in Figure 11 and Figure 12.

**Figure 11 - SCCM Query Statement to Select Intel IPT with PKI Systems with Middleware Installed**

```sql
SELECT * FROM SMS_R_System
INNER JOIN SMS_G_System_ADD_REMOVE_PROGRAMS ON SMS_G_System_ADD_REMOVE_PROGRAMS.ResourceID = SMS_R_System.ResourceID
INNER JOIN SMS_G_System_ADD_REMOVE_PROGRAMS_64 ON SMS_G_System_ADD_REMOVE_PROGRAMS_64.ResourceID = SMS_R_System.ResourceID
WHERE SMS_G_System_ADDREMOVE_PROGAMNS.DisplayName like 'Intel(R) Management Engine Components'
AND SMS_G_System_ADD_REMOVE_PROGRAMS.DisplayName like 'Intel® Identity Protection Technology with PKI'
```

**Figure 12 - SCCM Query Statement to Select Intel IPT with PKI Systems without Middleware Installed**

```sql
SELECT * FROM SMS_R_System
WHERE SMS_R_System.ResourceID not in
INNER JOIN SMS_G_System_ADD_REMOVE_PROGRAMS ON SMS_G_System_ADD_REMOVE_PROGRAMS.ResourceID = SMS_R_System.ResourceID
INNER JOIN SMS_G_System_ADD_REMOVE_PROGRAMS_64 ON SMS_G_System_ADD_REMOVE_PROGRAMS_64.ResourceID = SMS_R_System.ResourceID
WHERE SMS_G_System_ADDREMOVE_PROGAMNS.DisplayName like 'Intel(R) Management Engine Components'
AND SMS_G_System_ADD_REMOVE_PROGRAMS.DisplayName like 'Intel® Identity Protection Technology with PKI'
```

The SCCM query statements for detecting activation readiness can be used to define collection membership rules for SCCM collections used to drive the deployment process for Intel IPT with PKI.

An SCCM collection containing Intel IPT with PKI systems that are not activation-ready can be used to target and distribute packages containing missing Intel IPT with PKI middleware. Intel Management Engine Components software needs to be installed on Intel IPT with PKI systems based on 3rd and 4th generation Intel Core processors, Intel Trusted Execution Engine software needs to be installed on Intel IPT with PKI systems based on Intel Atom processors and Intel IPT with PKI software needs to be installed on all Intel IPT with PKI systems.

An SCCM collection containing activation-ready Intel IPT with PKI systems can be used to target and distribute packages containing ISV application software to enroll users for digital certificates using public-private keys generated by Intel IPT with PKI. An example script is shown in Figure 13 enrolling a user for a digital certificate based on Intel IPT with PKI. This script assumes a Microsoft based enterprise integrated certificate authority (CA) is used and a
Discovering Enterprise Systems with Intel® Identity Protection Technology

certificate template has already been created and published to the CA specifying the Intel IPT with PKI crypto service provider (CSP) be used to generate the public private key pair that will be used with the certificate.

![Code Snippet]

Figure 13 - Sample Script for Enrolling for a Digital Certificate based on Intel IPT with PKI

Summary

Intel IPT enables hardware-based two factor authentication which can be deployed at a lower cost compared to discrete tokens and offers a simplified end-user experience. Systems supporting Intel IPT can be discovered and made ready for activation using the standard hardware inventory, query statement and software distribution capabilities of Microsoft System Center 2012 Configuration Manager.

References

Intel Identity Protection Technology, Intel Corporation
http://ipt.intel.com/Home

Intel Architecture and Processor Identification with CPUID Model and Family Numbers, Intel Corporation

Intel Identity Protection Technology Detection Assistant Tool, Intel Corporation
http://iptprd.odce.intel.net/iptdoor3.html

Documentation Library for System Center 2012 Configuration Manager, Microsoft Corporation