Intel® IPT (Identity Protection Technology) based Token Provider for RSA SecurID® Software Token for Microsoft* Windows
Legal Notices

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL’S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL® ASSUMES NO LIABILITY WHATSOEVER AND INTEL® DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL® PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel® Product could result, directly or indirectly, in personal injury or death. YOU SHALL INDEMNIFY AND HOLD INTEL® AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS’ FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL® OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL® PRODUCT OR ANY OF ITS PARTS.

Intel® may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked “reserved” or “undefined”. Intel® reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document 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.

Cost reduction scenarios described are intended as examples of how a given Intel®-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

Contact your local Intel® sales office or your distributor to obtain the latest specifications and before placing your product order.

All products, computer systems, dates and figures specified are preliminary based on current expectations, and are subject to change without notice.

No computer system can provide absolute security. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses. Requires an enabled Intel® processor, enabled chipset, firmware and/or software optimized to use the technologies. Consult your system manufacturer and/or software vendor for more information.

Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. To learn more visit: http://www.intel.com/technology/vpro.

Intel, the Intel® logo, Intel® Core and Intel® vPro 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.
Introduction
This paper presents an overview of the Intel® IPT based Token Provider for RSA SecurID® Software Token for Microsoft® Windows® as implemented using Intel® Identity Protection Technology (IPT) with Public Key Infrastructure (PKI). Intel® IPT with PKI provides hardware enhanced protection of RSA cryptographic keys in specific Intel® vPro™ processor-powered systems. The Intel® IPT based Token Provider for RSA SecurID Software Token provides hardware enhanced protection of the RSA Token Seed by using IPT with PKI cryptographic functions to encrypt and sign the token seed. This signed and encrypted token seed is used by the RSA SecurID Software Token to generate the OTP token. The Intel® IPT based Token Provider provides an additional layer of protection to the RSA OTP solution. This whitepaper explains how the Intel® IPT with PKI hardware enhanced cryptographic functions are used to provide a more secure environment for RSA SecurID Software Token.

Table of Contents
Introduction ........................................................................................................................................... 3
Intel® vPro™ Platforms and Features ............................................................................................. 3
Intel® Identity Protection Technology with Public Key Infrastructure .............................................. 4
Overview of RSA SecurID Software Token ..................................................................................... 5
RSA SecurID Software Token for Microsoft Windows ................................................................. 5
  Features ............................................................................................................................................ 5
Overview of the Intel® IPT based Token Provider for RSA SecurID Software Token ...................... 6
  Provisioning the RSA SecurID Software Token Seed ................................................................. 6
  Using the Hardware-Protected RSA SecurID Software Token Seed to Generate the OTP Token ....... 7
Summary ............................................................................................................................................. 8
  Related Links for Intel® IPT with PKI ........................................................................................... 8

Intel® vPro™ Platforms and Features
Intel® vPro™ technology addresses many IT security and platform management needs through its broad set of security, manageability, and productivity-enhancing capabilities. This technology is built into the new Intel® Core™ vPro™ processor family, some smaller form-factor devices based on the Intel® Atom™ processor, and some Intel® Xeon® processors.

Among the notable security features included in Intel® vPro platforms are the Intel® Identity Protection Technologies described in the next chapter. Additional features found on Intel® Core vPro platforms and platforms based on the 4th Generation Intel® Atom Processor for Business include:

- Improved device manageability with Intel® Active Management Technology
  - Out of band system access
  - Hardware-based host agent status checking
Remote diagnostics and repair tools such as hardware-based KVM, IDE redirection, power control and more

- Hardware Assisted Secure Boot coupled with Platform Trust Technology
  - Hardware-assisted secure boot, along with Early Launch Anti-Malware drivers, enable a boot in a known trusted environment.
  - Credential storage and key management capability to meet Windows® 8 CSB requirements, optimized for low power consumption in S0ix environment.

- Improved Data Encryption Performance with New AES Instructions
  - A faster, more secure AES engine for a variety of encryption apps, including whole disk encryption, file storage encryption, conditional access of HD content, internet security, and VoIP. Consumers benefit from increased protection for internet and email content, plus faster, more responsive disk encryption.

- Improved Operating System Security with Intel® Secure Key
  - Security hardware-based random number generator that can be used for generating high-quality keys for cryptographic (encryption and decryption) protocols. Provides quality entropy that is important in the cryptography world for added security.

- Improved Operating System Security with Intel® OS Guard
  - An enhanced hardware-based security feature that better protects the OS kernel. OS Guard protects areas of memory marked as user mode pages and helps prevent attack code, which is in a user mode page or a code page, from taking over the OS kernel. OS Guard is not application-specific and can protect the kernel from any application.

To find out more about the features included in Intel® vPro platforms, visit [http://intel.com/vpro](http://intel.com/vpro).

Intel® Identity Protection Technology with Public Key Infrastructure

Intel® Identity Protection Technology (IPT) with Public Key Infrastructure (PKI) uses the Intel® Management Engine (Intel® ME) in specific Intel® vPro™ processor-powered systems to provide a hardware based security capability. Intel® IPT with PKI provides hardware-enhanced protection of RSA 1024 and 2048 asymmetric cryptographic keys. The Intel® IPT with PKI capability is exposed as a Crypto Service Provider (CSP) via the Microsoft CryptoAPI software layer. Software that supports the use of cryptographic features through CryptoAPI 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 that use the Intel® IPT with PKI Protected Transaction Display (PTD)

Both the RSA key-pair 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 using Intel® IPT with PKI, and cannot be exported from the Intel® ME. When the RSA key is needed, it must to be brought back into the ME to be unwrapped.

The hardware enhancements of Intel® IPT with PKI focus on enhanced RSA private key protection; but it should be noted that the installed CSP can be used for any algorithms typically supported by software.
based CSPs. Non-RSA operations are performed in software, and provide the same level of protection as existing software-based CSPs shipped with Microsoft Windows 7* and above. Applications based on CryptoAPI should be able to transparently use Intel® IPT with PKI and derive the benefits of enhanced private key protection with little, if any, modification.

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

Intel® IPT with PKI provides an embedded 2\(^{nd}\) factor of authentication in the PC to validate legitimate users in an enterprise. Compared to a hardware security module, external reader, or a TPM, Intel® IPT with PKI is can be less expensive and easier to deploy. Compared to a software-based cryptographic product, Intel® IPT with PKI is generally more secure. Intel® IPT with PKI provides a good balance between security, ease of deployment, and cost.

Overview of RSA SecurID Software Token

RSA SecurID software tokens use the same algorithm (AES-128) as RSA SecurID hardware tokens while eliminating the need for users to carry dedicated hardware key fob devices. Instead of being stored in hardware, the symmetric key is safeguarded securely on utilizing the Intel® IPT with PKI. RSA SecurID software authenticators reduce the number of items a user has to manage for safer and more secure access to corporate assets. Software tokens can help the enterprise cost-effectively manage secure access to information and streamline the workflow for distributing and managing two-factor authentication for a global work force. Additionally, software tokens can be revoked and recovered when someone leaves the company or loses a device, eliminating the need to replace tokens.

RSA SecurID Software Token for Microsoft Windows

Features

- Strong two-factor authentication to protected network resources
- Software token automation for integration with available RSA SecurID Partner applications
- Silent, secure installation
- Multiple token provisioning options including Dynamic Seed Provisioning (CT-KIP)
- Web plug-in for faster access to protected web sites with Microsoft Internet Explorer
- Interoperability with Windows screen readers for visually impaired users
Overview of the Intel® IPT based Token Provider for RSA SecurID Software Token

The Intel® IPT based Token Provider provides two functions, 1) the initial encryption, signing, and storage of the token seed using a platform binding key when it is provisioned to the system, and 2) the signature validation, decryption, and calculation of the OTP token.

Provisioning the RSA SecurID Software Token Seed

Provisioning the RSA SecurID Software Token involves the following functions:

- Import the token seed from a file or from the web.
- Use the Intel® IPT with PKI Cryptographic Service Provider (CSP) to generate a platform binding key, which is unique per platform.
- Encrypt the token seed using the platform binding key.
- Use the Intel® IPT with PKI CSP to sign the encrypted token seed using the platform binding key.
- Store the signed and encrypted token seed in the Intel® persistent storage device.

Figure 1 – Token Seed Provisioning Architecture
Using the Hardware-Protected RSA SecurID Software Token Seed to Generate the OTP Token

RSA SecurID Software OTP Token Generation involves the following functions:

- Read the signed and encrypted token seed from the Intel® persistent storage device.
- Use the Intel® IPT with PKI CSP based Platform binding key to validate the signature on the signed and encrypted token seed.
- Use the Intel® IPT with PKI CSP to decrypt the token seed.
- Call the RSA Token Library to generate the next OTP token.
Summary
The Intel® IPT based Token Provider for RSA SecurID Software Token provides hardware-enhanced protection of the RSA Token Seed by using IPT with PKI cryptographic functions to encrypt and sign the RSA SecurID Software token seed and bind it to the specific Intel platform.

Related Links for Intel® IPT with PKI
For more information on Intel® IPT with PKI and Protected Transaction Display visit:

- Intel® Identity Protection Technology:
- Microsoft CryptoAPI interface:
- RSA SecurID Software Token for Microsoft Windows Page:
- RSA SecurID/RSA Authentication Manager Page:
  - [http://www.emc.com/security/rsa-securid.htm](http://www.emc.com/security/rsa-securid.htm)
- RSA Ready (Integration Partner) page:
  - [https://community.emc.com/community/connect/rsaxchange/rsa-ready](https://community.emc.com/community/connect/rsaxchange/rsa-ready)