Intel® Identity Protection Technology-based Token Provider for RSA SecurID* Software Token for Microsoft Windows*

Intel® Identity Protection Technology provides a more secure environment for RSA SecurID* software token

Introduction

This paper presents an overview of the token provider for EMC's RSA SecurID* software token implemented using Intel® Identity Protection Technology (Intel® IPT) with public key infrastructure (PKI). Intel IPT with PKI provides hardware-enhanced protection of RSA cryptographic keys in specific Intel® Core™ vPro™ processor-powered systems. The token provider for EMC's RSA SecurID* based on Intel IPT provides hardware-enhanced protection of the RSA token seed by using Intel 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 token provider based on Intel IPT 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 2

Intel® Core™ vPro™ Platforms and Features 2

Intel® IPT with Public Key Infrastructure 3

Overview of RSA SecurID* Software Token 4

RSA SecurID Software Token for Microsoft Windows 5

Features 5

Overview of the Intel® IPT based token provider for RSA SecurID software token 5

Provisioning the RSA SecurID software token Seed 5

Using the Hardware-Protected RSA SecurID software Token Seed to Generate the OTP Token 6

Device Type Binding and Device Serial Number Binding 7

Device Type Binding 7

Device Serial Number Binding 8

Summary 8

Related Links for Intel® IPT with PKI 8

Legal Notices 9

Intel® Core™ vPro™ Platforms and Features

Intel® Core™ 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® Core™ vPro™ platforms is the Intel Identity Protection Technology 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 Intel® AES New Instructions (Intel® AES-NI)
    - Intel® AES-NI provides 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
    - A 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. Intel OS Guard protects areas of memory marked as user mode pages and helps prevent attack code in a user mode page or a code page, from taking over the OS kernel. Intel OS Guard is not application-specific and can protect the kernel from any application.

To find out more about the features included in Intel® Core™ vPro™ platforms, visit http://intel.com/vpro.

Intel® IPT with Public Key Infrastructure

Intel IPT with PKI uses the Intel® Management Engine (Intel® ME) in specific Intel® Core™ 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 be brought back into the Intel 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 a PC-embedded 2nd factor of authentication to validate legitimate users in an enterprise. Compared to a hardware security module, external reader, or a TPM, Intel IPT with PKI 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 securely safeguarded utilizing 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 CSP that is included in the Intel IPT with PKI binaries to generate a platform binding key, which is unique per platform.
- Encrypt the token seed using the platform binding key.
- Use the Intel 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.

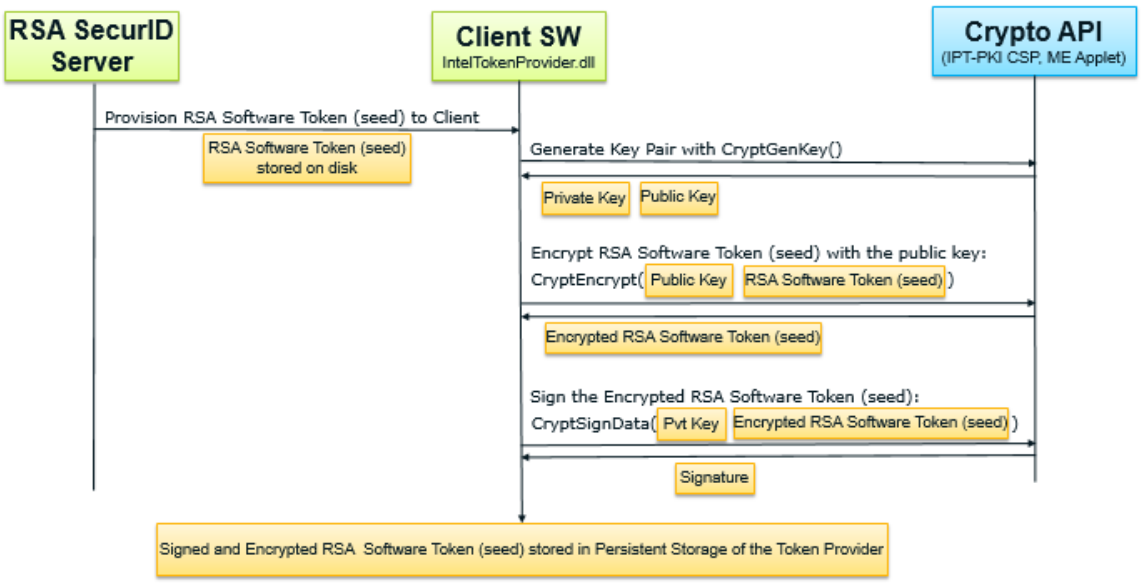


Figure 1 – Token Seed Provisioning Architecture

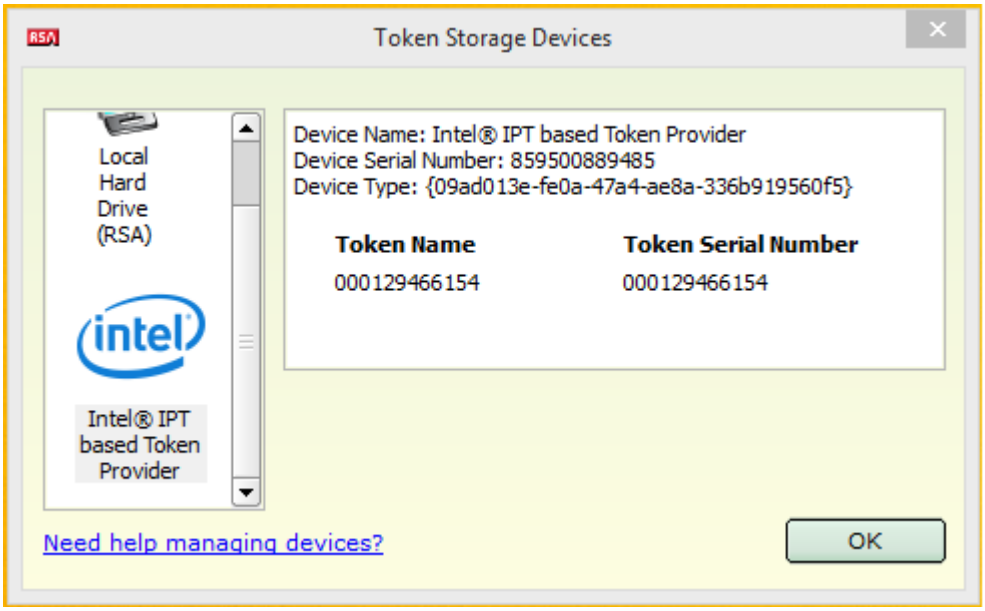


Figure 2 – The Token Storage Devices screen [or UI]

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 CSP-based platform binding key from Intel IPT with PKI to validate the signature on the signed and encrypted token seed.
- Use the CSP from Intel IPT with PKI to decrypt the token seed.
- Call the RSA token library to generate the next OTP token.

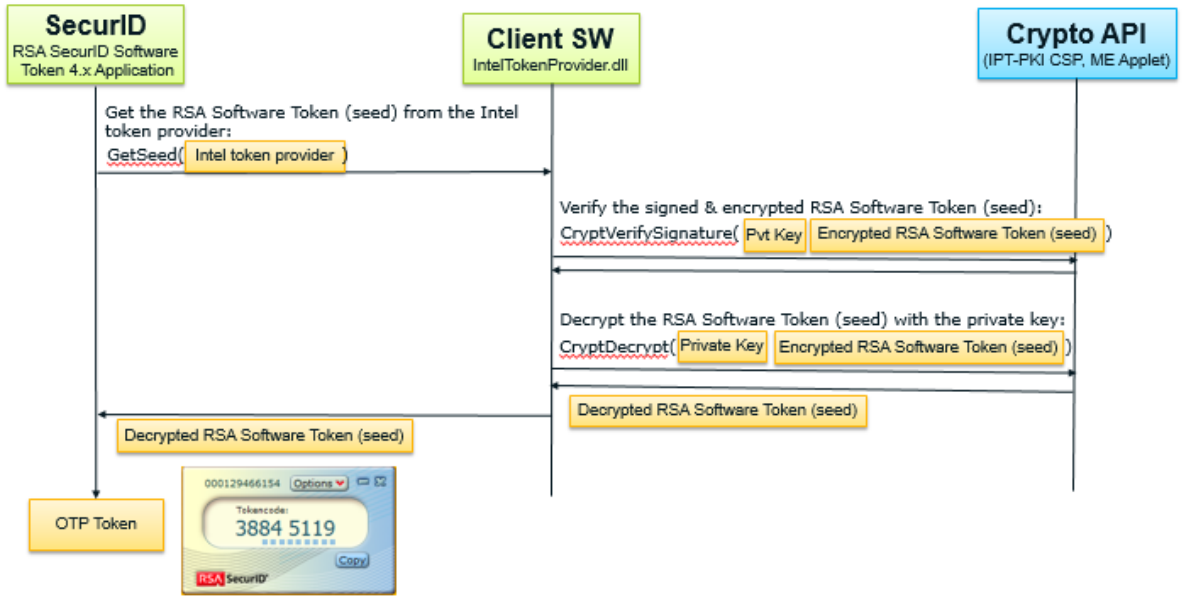


Figure 3 – Using the hardware-protected token seed to generate the OTP token

Device Type Binding and Device Serial Number Binding

RSA SecurID Software Tokens supports security features called Device Type Binding and Device Serial Number Binding. Device Type Binding allows the IT administrator to enforce the class of device that a token should be provisioned to. Device Serial Number Binding allows the IT administrator to issue a token that is bound to a specific system. The Intel IPT-based token provider supports both of these enhanced security features.

Device Type Binding

Device Type binding prevents a user from importing a given software token file into a different container other than the one that is specified by the IT administrator. For more information on how to implement this feature, please consult the RSA Authentication Manager 8.1 Administrators Guide. You can download the Administrators Guide from the RSA site here:

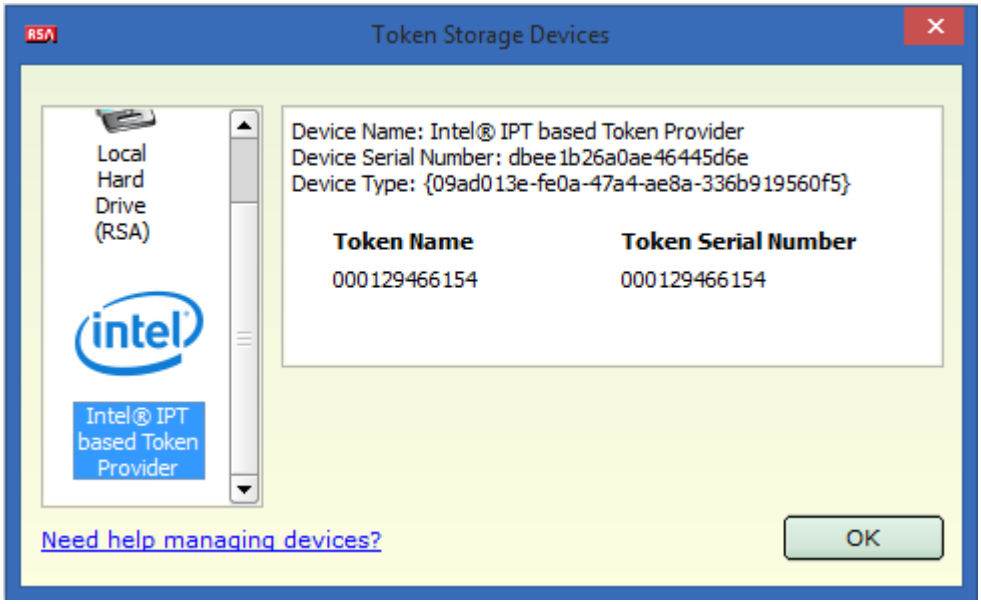
http://www.emc.com/collateral/15-min-guide/h12276-am8-administrators-guide.pdf

In addition, you can download the device definition file for Intel IPT-based token provider by right clicking on the link below and doing a "save as" to get the file:

https://sftp.rsa.com/human.aspx?Username=partner&password=rsasecured&arg01=181340228&arg12=downloaddirect&transaction=signon&quiet=true

Device Serial Number Binding

Device Serial Number Binding allows the IT administrator to bind the token to a specific device. If you are attempting to bind the token to a specific device, the IT administrator should instruct the user to open the RSA Software Token application and select **Options…Token Storage Devices**:



The Device Serial Number is listed as a property of the Intel IPT-based token provider (dbee1b26a0ae46445d6e in the example above).

Instructions for configuring this feature in RSA SecurID RSA Ready Implementation Guide for RSA SecurID can be found in the "RSA Ready Community" link on:

http://www.emc.com/security/rsa-securid/rsa-securid-software-authenticators/ms-windows.htm

Summary

The token provider for EMC's RSA SecurID* software token based on Intel IPT provides hardware-enhanced protection of the RSA token seed by using Intel 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:
  - http://ipt.intel.com/welcome/protect-business-data.aspx
- Microsoft CryptoAPI interface:
  - http://technet.microsoft.com/en-us/library/cc962093.aspx
- RSA SecurID software tokens for Microsoft Windows Page:
  - http://www.emc.com/security/rsa-securid/rsa-securid-software-authenticators/ms-windows.htm
- RSA SecurID/RSA Authentication Manager Page:
  - http://www.emc.com/security/rsa-securid.htm
- RSA Ready (Integration Partner) page:
  - https://community.emc.com/community/connect/rsaxchange/rsa-ready

Legal Notices