RSA SecurID® and Intel® IPT

Protecting users of the Microsoft Windows® platform with a Hardware Root of Trust

The RSA SecurID Software Token for Windows can have its secret symmetric key that is stored on a user's PC securely encrypted and signed by the Intel Identity Protection Technology platform.

With Intel® IPT, the traditional PC malware attack to steal this information is stopped dead in its tracks.

OVERVIEW: TWO SOLUTIONS, ONE GREAT ANSWER

Users are the new perimeter for your organization. Now, you must not only provide and equip them with the latest technology that will keep them productive, but also secure that technology to a very high degree in order to prevent the bad guys from stealing your sensitive information and compromising your organization.

This is a big responsibility, but RSA and Intel have teamed up to help bring together two of the industry's leading technologies to help turn the tables on the cyber attacks. The RSA SecurID® solution is the world's leading two-factor authentication platform deployed by over 30,000 organizations worldwide to protect access to sensitive applications. Likewise, Intel® vPro™ technology addresses many IT security and platform management needs through its broad set of security, manageability, and productivity-enhancing capabilities.

ESTABLISHING A HARDWARE ROOT OF TRUST

The RSA SecurID Software Token for Microsoft Windows® uses the same algorithm as RSA SecurID hardware tokens while eliminating the need for users to carry dedicated hardware key fob devices. This reduces the number of items a user has to manage for safe and secure access to corporate assets, and 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, RSA software tokens can be revoked and recovered when someone leaves the company or loses a device, eliminating the need to replace physical tokens.

The RSA SecurID software token generates a unique and changing One-Time Password (OTP) every 60 seconds. When used in combination with a user's memorized PIN, this provides a very strong – inded two factor strong - set of login credentials that are almost impossible to guess or socially engineer.

In order to generate this unique OTP, a symmetric key is utilized. This key is stored on the user's Windows-based device and is safeguarded securely on the user's PC using a variety of operationg system security features. For some organizations, this is an acceptable level of security. However, for highly sensitive environments where compromise of user credentials to access senstive information could have extremely adverse effects – and let's face it, that would probably describe most organization's – there is a need to go beyond just the operating system software to protect the RSA symmetric key.

HOW IT WORKS

This is where the RSA-Intel solution comes into play. Since the symmetric key needs to be stored on the user's device for easy retrieval and use by the RSA software token application, wrapping it with the Intel® IPT to both encrypt it while it's at rest and sign it to verify its integrity is essential.

Here's how it works. 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® Management Engine (ME). When the RSA key is needed, it must to be brought back into the ME to be unwrapped.

RSA SecurID Software OTP Token Generation involves the following functions:

- Read the signed and encrypted token secret from the Intel® persistent storage device.
- Use the Intel® IPT with PKI Crypto Service Provider (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.

AUTHENTICATION IN ACTION

The RSA-Intel solution can be used for protecting over 400+ integrations already available in market, which includes any RSA or third-party agent that has been built to support the RSA SecurID functionality. Applications include:

- VPNs (SSL and IPSec)
- Proxy servers, firewalls, domain servers
- Web servers
- Wireless networks
- Virtual Desktop Interfaces (VDI)
- More

Intel® IPT with PKI provides an embedded 2nd factor of authentication in the PC to validate legitimate users in an enterprise. Compared to a hardware security module, external reader, or a Trusted Platform Module, 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.

For more information, contact your RSA or Intel Authorized Account Manager or Partner