# Strengthening Security with Intel® Platform Trust Technology

## Use Cases for Intel® Platform Trust Technology with Windows* 8-Based Tablets using Intel® Processors


## Executive Summary

Many Windows* 8-based tablets using Intel® processors include Intel® Platform Trust Technology (Intel® PTT). But what are the use cases for this technology? This paper explores some of the available use cases including strengthening the authentication process for disk encryption, embedded smart cards for reducing IT costs and improving the user experience, measured boot for making platforms more trustworthy, and hardware key attestation for making digital certificates more trustworthy.


## Disk Encryption

Disk encryption mitigates risks associated with data loss when devices such as tablets are lost or stolen. Data on local storage devices is encrypted and an authentication process must be completed before data is decrypted and accessible.

Many organizations chose an authentication method requiring a valid PIN or passphrase to be entered during a pre-boot authentication (PBA) process before data can be decrypted allowing the tablet to boot to the operating system. One of the threats to this authentication method involves substituting one or more of the boot components with malware that captures the PIN or passphrase for later use by unauthorized users to decrypt the disk.

Intel PTT with Windows 8 based BitLocker Disk Encryption technology and Secure Boot technology delivers a solution that strengthens the authentication process.

Intel PTT improves the authentication process by enabling disk encryption keys to be locked (or sealed) to the platform configuration so that keys are only released if the platform configuration has not changed from a known good configuration. Attempts to substitute boot components or interfere with the boot device order cause the platform configuration to change and Intel PTT to refuse to release disk encryption keys.

Secure Boot technology records the platform configuration into Intel PTT during the boot process and BitLocker* disk encryption technology seals the disk encryption keys against the platform configuration.

## Virtual Smart Cards

Smart card technology can be used for authentication, digital signing, and data encryption.

Discrete smart cards have certain characteristics that make them attractive from a security perspective:-

- **Crypto operations** are performed by an isolated processor on the smart card to reduce the risk of malware interference.
- **Standard digital certificates** used for authentication, digital signing, and data encryption usage scenarios can be stored on the smart card.
- **A PIN** must be supplied to authorize access and use of the digital certificates stored on the smart card.

## Contents



- **Anti-hammering logic** is built into the smart card to prevent brute force attempts by unauthorized users to guess the PIN.
- **Smart cards are portable** so they can be used with different endpoint devices and stored separately from the device.

However, discrete smart cards have some potential drawbacks:

- **Costs** associated with supplying and maintaining discrete smart cards and readers
- **User requirement** to carry their smart card to perform authentication, digital signing, or data encryption operations with their endpoint device
- **Loss of productivity** if users forget or lose their smart card
- **The experience of using a discrete smart card reader** with newer mobile form factor devices such as tablets, which rarely contain a built-in reader

Intel PTT with Windows 8-based Virtual Smart Card* (VSC*) technology delivers a solution that eliminates the drawbacks associated with discrete smart cards while retaining most of the benefits.

Intel PTT and VSC are both built into the platform, eliminating costs associated with supplying and maintaining discrete smart cards and readers. Because the smart card and reader are built into the platform, the platform effectively becomes the smart card, simplifying the user experience. Users no longer need to remember to carry their smart card. The VSC reader, being integral to the platform, is simple to use and not vulnerable to physical failures or connectivity issues.

Intel PTT includes a separate crypto processor for performing security key operations in an isolated hardware environment.

VSC technology is compatible with standard digital certificates used for authentication, digital signing, and data encryption scenarios. Digital certificates enrolled using VSC devices are stored in the operating system and accessed by application software using existing smart card APIs. All security key operations associated with those digital certificates are performed within the Intel PTT isolated hardware environment, reducing the risk of malware interference.

Intel PTT and VSC technology require PINs or passphrases to be used to authenticate users before digital certificates enrolled using VSC devices can be used. Intel PTT incorporates anti-hammering logic to prevent brute force attacks against those PINs and passphrases.

### Measured Boot

Measured boot is used to measure the firmware and operating system components present in the platform boot path. These measurements can be later retrieved and compared with a set of known good measurements to evaluate the trustworthiness of the components used during the boot process. Called remote attestation, this use case can be used as part of a decision-making process to determine whether a platform can be used to access sensitive services or data.

Intel PTT provides several capabilities to support measured boot:

- **Tamper-resistant storage**, available soon after initial platform power on, where measurements for each firmware and Operating System boot component can be stored
- **Hardware-based signing** of measurements when they are retrieved for later inspection to ensure measurements are genuine

Using measured boot as part of a complete solution requires additional software components to request and retrieve measure-

measurements, store and manage known good measurements, and deliver the attestation process results to other infrastructure components that use these results as part of a decision to grant or deny the platform access to services or data.

### Hardware Key Attestation

Hardware key attestation enables services to determine whether security keys are stored and processed (i.e., protected) by hardware rather than software. Hardware key storage and processing is considered less vulnerable to malware attack; therefore, the ability to distinguish security keys protected by hardware enables IT to make decisions based on this characteristic. For example, digital certificates used to authenticate access to sensitive resources or sign sensitive documents may only be issued by certification authorities if the associated security keys are protected by hardware.

Intel PTT, with Windows 8-based platforms and Windows Server 2012 R2, can be used to deliver a solution for hardware key protection and hardware-based key attestation.

Intel PTT provides hardware key protection by using a separate crypto processor to perform security key operations in an isolated hardware environment.

Windows 8 and Windows Server 2012 R2 based Active Directory Certification Services implement a certificate enrollment protocol that includes optional hardware key attestation.

Intel PTT includes a hardware-resident Endorsement Key (EK) unique to each platform. This can be used by active directory certification services to determine if certificate enrollment requests are associated with security keys protected by hardware. Based on this information, certificates can be issued or denied.

### Conclusions

Intel PTT is included in many Windows 8-based tablets using Intel processors. It can contribute to reducing IT costs, improving the user experience, and improving security.

Learn more about security solutions from Intel **here**.


050114/SD/SD Please Recycle Printed in USA