Trusted Platform Module (TPM) based Security on Notebook PCs - White Paper

Sundeep Bajikar
(sundeep.bajikar@intel.com)

Mobile Platforms Group
Intel Corporation

June 20, 2002

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. Intel products are not intended for use in medical, life saving, life sustaining applications.

Except that a license is hereby granted to copy and reproduce this Document for internal use only.

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.

This product 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.

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

Copies of documents which have an ordering number and are referenced in this document, or other Intel literature, may be obtained from:

Intel Corporation
www.intel.com
or call 1-800-548-4725

CONTENTS

Introduction

Business and commerce depend on trust. With the growth of the Internet, wireless communication technologies and connected mobile computing, trust has become a pivotal issue for e-Commerce. Since notebook PCs are increasingly used for e-Commerce, there is a growing need to make the notebook platform more trustworthy.

As the mobility of the platform increases, it becomes more and more susceptible to theft. Stolen data is often regarded as being more valuable than the notebook hardware itself. Thus, the need to protect user data and secrets is underscored in a mobile computing environment.

In the Spring of 1999, the Trusted Computing Platform Alliance (TCPA) was chartered to encourage industry participation in the development and adoption of an open specification for an improved computing platform. The TCPA participants agreed that the specification for the trusted computing PC platform should focus on two areas – ensuring privacy and enhancing security. TCPA members include Intel*, Microsoft*, Infineon*, National*, Atmel*, and a large number of other organizations.

The objective of the TCPA is to complement existing capabilities, including the X.509 standard for digital certificates, IPSEC (Internet Protocol Security Protocol), IKE (Internet Key Exchange), VPN (Virtual Private Network), PKI (Public Key Infrastructure), PC/SC Specification for smart cards, biometrics, S/MIME (Secure Multi-purpose Internet Mail Extensions), SSL, SET (Secure Electronic Transaction), IEEE 802.11 WEP, IEEE 802.1x, etc. The TCPA provides for a platform root of trust, which uniquely identifies a particular platform, and provides various crypto capabilities including hardware-protected storage.

The Trusted Platform Module (TPM) is defined as a hardware instantiation of the TCPA specification. The current revision of the TCPA main specification is version 1.1a.

This document provides a discussion about the various requirements for a TCPA-enabled mobile PC platform, as described in the TCPA specifications listed in the "References" section towards the end of the document.

Notebook Security Threats

Notebook computers are exposed to several security threats. Notebook security threats can be broadly classified into:

Physical data theft

This threat arises from the fact that notebook computers are more susceptible to be stolen than their desktop counterparts. Once stolen, notebooks can be subject to a variety of hardware as well as software attacks. It is often found that the stolen data is more valuable than just the cost of the notebook hardware.

Data communication attack

Notebooks often operate outside of corporate firewalls. Also, they use various means of communication to access the corporate network or the Internet. There are a number of ways in which a determined hacker can attack the communication channel used by the notebook to steal the data being transceived. This poses a threat to sensitive data resident on the notebook as also sensitive data resident on the network. Furthermore, this poses a threat to the entire network, as a compromised communication channel can be vulnerable to various types of attacks on different critical pieces of the network infrastructure.

Threat Matrix

The table below performs a gap analysis on current solutions to notebook threat models to point out the areas in which a TPM on the platform can help.

Threats	**Current Solutions**	**Weaknesses**	**TPM Solutions**
Data theft	Data encryption (EFS, VPN, encrypted email, etc.)	Encryption keys are stored on the hard disk and are susceptible to tampering	Protected storage of keys through hardware
Unauthorized access to platform	1. Username / Password 2. Biometrics and external tokens for user authentication	1. Subject to dictionary attacks 2. Biometrics can be spoofed 3. Authentication credentials not bound to platform	Protection of authentication credentials by binding them to platform
Unauthorized access to network	Windows network logon, IEEE 802.1x	1. Can be bypassed 2. Certificate can be spoofed 3. Authentication data is stored on the hard disk and is susceptible to tampering	1. PKI based method for platform authentication 2. Hardware protection of authentication data

TPM Architecture

The TPM hardware along with its supporting software and firmware provides the platform root of trust. It is able to extend its trust to other parts of the platform by building a chain of trust, where each link extends its trust to the next one. The following sections describe the capabilities and contents of the TPM and explain how the trust comes about in various usage scenarios.

The TPM is basically a secure micro-controller with added cryptographic functionalities. To simplify system integration into the PC platform, the TPM uses the Low Pin Count (LPC) bus interface to attach to the PC chipset.

Crypto Capabilities

The TPM provides a set of crypto capabilities that allow certain crypto functions to be executed within the TPM hardware. Hardware and software agents outside of the TPM do not have access to the execution of these crypto functions within the TPM hardware, and as such, can only provide I/O to the TPM.
A TPM has the following hardware crypto capabilities.

RSA Accelerator

The TPM contains a hardware engine to perform up to 2048 bit RSA encryption/decryption. The TPM uses its built-in RSA engine during digital signing and key wrapping operations.

Engine for SHA-1 hash algorithm

The TPM uses its built-in hash engine to compute hash values of small pieces of data. Large pieces of data (such as an email message) are hashed outside of the TPM, as the TPM hardware may be too slow in performance for such purposes.

Random Number Generator

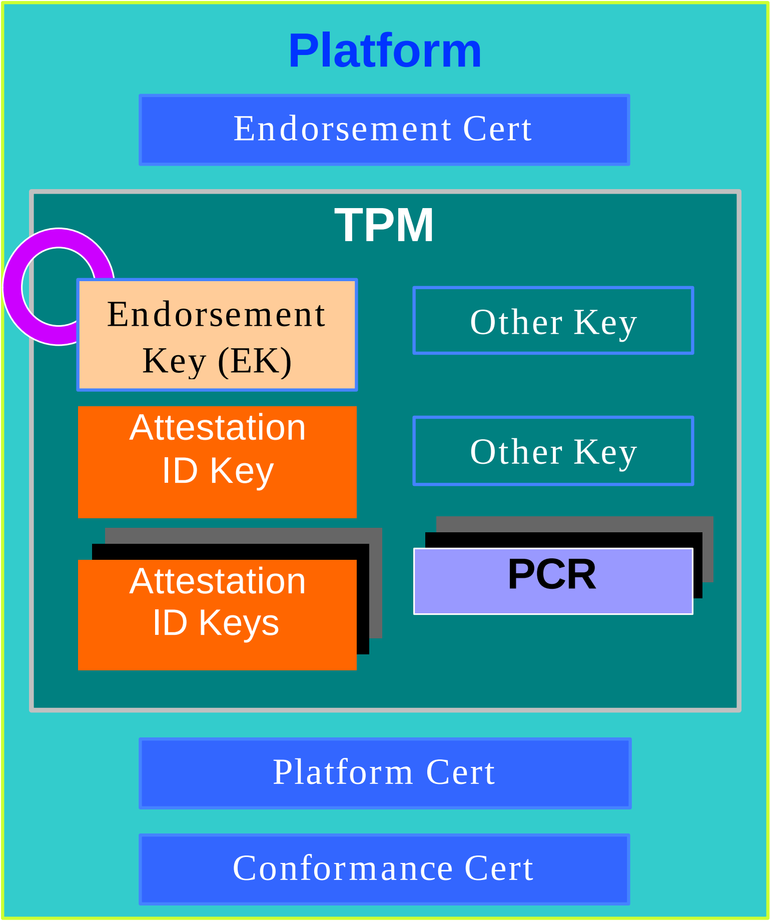
The RNG is used to generate keys for various purposes.

Limited NVRAM for TPM Contents

Refer to the next sub-section for the TPM Contents.

Contents

The figure on the next page illustrates the various contents within the TPM's internal hardware protected storage.



Endorsement Key (EK)

The Endorsement Key (EK) is a public/private key-pair. The size of the key-pair is mandated to have a modulus (a.k.a. key size) of 2048 bits. The private component of the key-pair is generated within the TPM and is never exposed outside the TPM.

The EK is unique to the particular TPM and therefore the particular platform. There are two ways to generate the EK. The first method is to use the TPM command specified for this purpose (TPM_CreateEndorsementKeyPair). The second method is called “squirting”, in which the TPM manufacturer can “squirt” an externally generated EK into the TPM during the manufacturing process.

Note that much of the value (or trust) associated with the TPM comes from the fact that the EK is unique and that it is protected within the TPM at all times. This property is certified by the Endorsement Certificate (Cert). The same party that provides the EK may not provide the Endorsement Cert.

Attestation Identity Key (AIK)

AIKs are used to provide platform authentication to a service provider. This is also called pseudo-anonymous authentication and is different from user authentication. Refer to the section on attestation under usage models for an illustration of how AIKs are obtained.

Certificates

Three types of certificates that may be stored in the TPM are: Endorsement Certificate (Endorsement Cert), Platform Cert, and Conformance Cert.

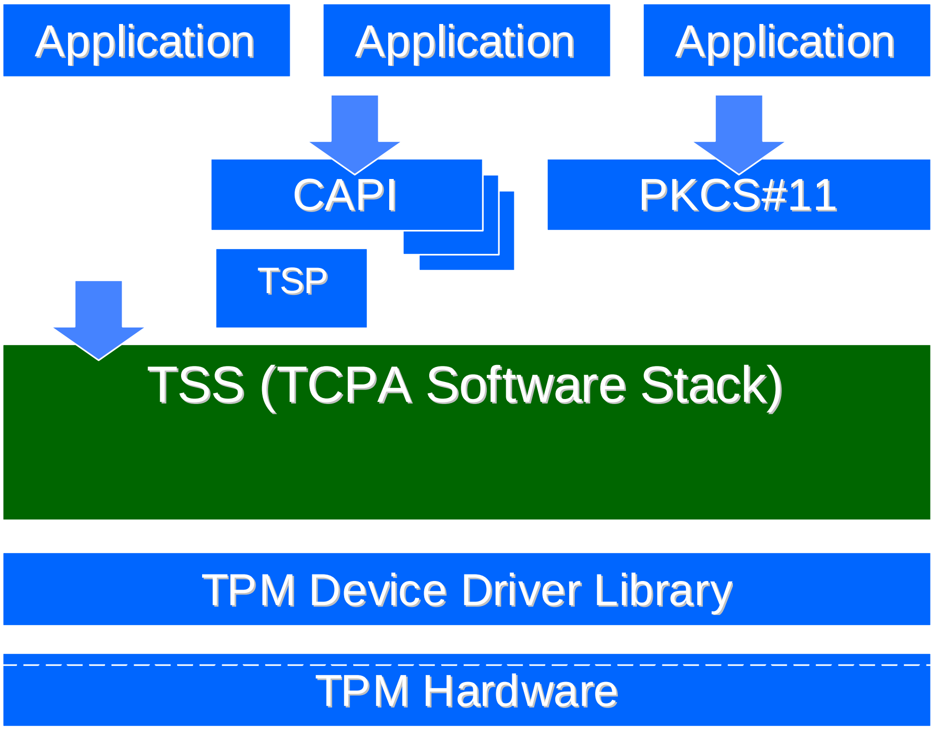
The Endorsement Cert contains the public key of the EK. The purpose of the Endorsement Cert is to provide attestation that the particular TPM is genuine, i.e. that the EK is protected.

The Platform Cert is provided by the platform vendor and provides attestation that the security components of the platform are genuine.

The Conformance Cert is provided by the platform vendor or an evaluation lab. It provides attestation by an accredited party as to the security properties of the platform.

Software Stack

The figure below illustrates the TPM software stack. At the lowest level is the TPM hardware device, which is accessed via the TPM device driver library.



Applications can utilize the TPM either through the MS-CAPI standard interface, or by directly implementing a communication interface with theTSS, especially for certain TCPA functions that may not be supported by MS-CAPI.

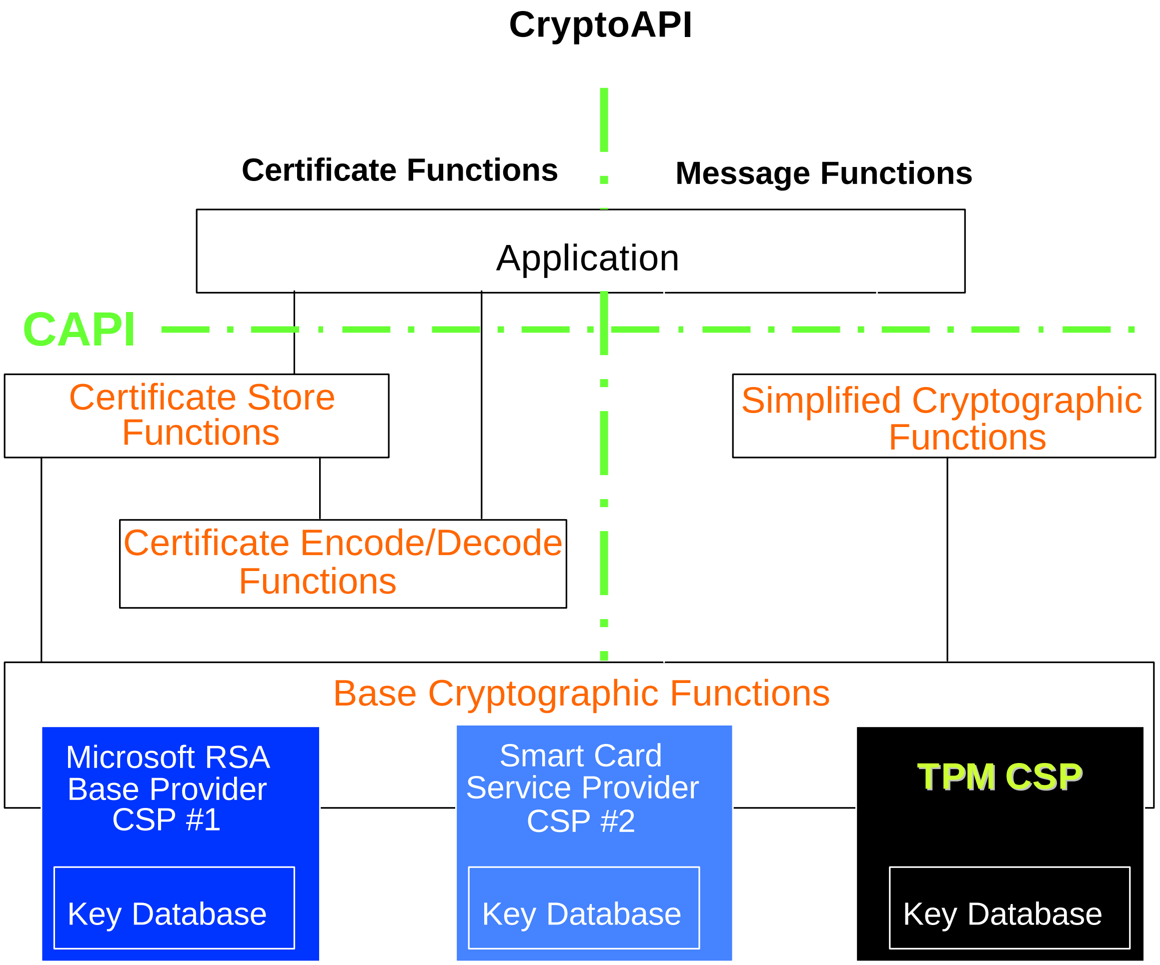
TCPA Software Stack (TSS)

The TCPA Software Stack (TSS) is comprised of modules and components that provide the supporting functionality to the TPM. Based on the TCPA specification, certain functions and services are outside of the scope of the TPM hardware. These functions and services are delivered using the host CPU and system memory. The TSS provides the necessary software architecture to support the offloading of security functions from the TPM to the main CPU and memory resources of the system.

Microsoft* CAPI TPM Crypto Service Provider (CSP)

The Microsoft* Cryptographic API (CAPI) provides services that enable application developers to add cryptography to their Win32 applications. Applications can use the functions in CAPI without knowing anything about the underlying implementation of security hardware. All cryptographic operations are performed by independent modules known as Cryptographic Service Providers (CSPs). One CSP, the Microsoft* RSA Base Provider, is bundled with the operating system. Each CSP provides a different implementation of the CAPI. Some provide stronger cryptographic algorithms while others contain hardware components such as smartcards.

The Microsoft* CAPI system is composed of a number of different components, as illustrated in the figure below.


CryptoAPI
Certificate Functions
Message Functions
Application
CAPI
Certificate Store Functions
Simplified Cryptographic Functions
Certificate Encode/Decode Functions
Base Cryptographic Functions
Microsoft RSA Base Provider CSP #1
Key Database
Smart Card Service Provider CSP #2
Key Database
TPM CSP
Key Database

The TPM CSP provides an interface between the CAPI and theTSS. Since the scope of the TSS is much broader than that of the CAPI, several TSS capabilities are not accessible through the CAPI. Such advanced capabilities are directly accessed through the TSS – applications needing such capabilities have to directly talk to the TSS.

BIOS Code

The TCPA specifies the measurement of integrity of BIOS code at system startup. In order to accomplish such integrity measurement and reporting, the system BIOS has to be enhanced with integrity measurement functions. Depending on the existing BIOS architecture, such enhancements can be a complex task.

Platform vendors may wish to provide various pre-boot security functions using the TPM. The necessary code to provide such functions is either implemented directly within the system BIOS or provided as an option ROM.

Whether or not any pre-boot functionality is provided on the platform, minimum changes have to be made to the BIOS code to ensure that the TPM is defined as a motherboard device within the ACPI descriptor tables. This enables the Operating System to identify the device, allocate resources to it, and load necessary device drivers.

Usage Models

Hardware Protected Storage

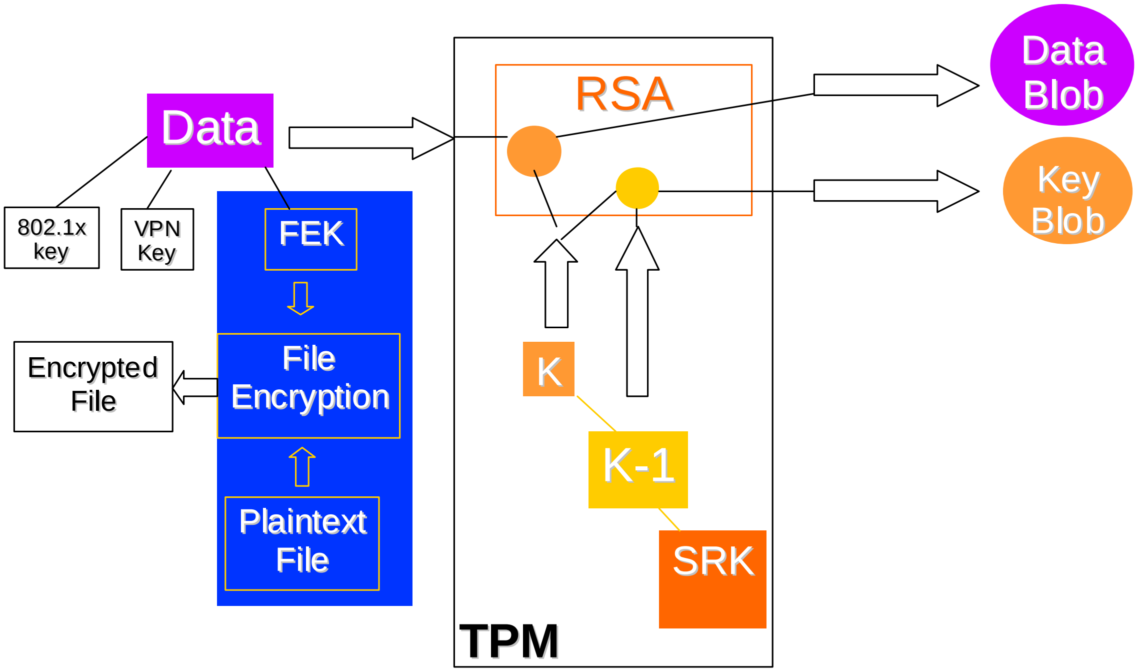
Hardware protected storage provides the ability to protect the user's secret data through a dedicated piece of hardware. Examples of secret data that the user might want to protect include File Encryption keys, VPN keys, Authentication keys, etc. Hardware protection is accomplished by encrypting the secret data in such a manner that it can only be decrypted by the dedicated piece of hardware, which contains the necessary private key.

For small pieces of secret data such as keys less than 2048 bits long, the encryption of the secret data can be performed within the TPM hardware using its built in RSA engine. For large pieces of secret data, there are two options in general:

1. The platform can encrypt the large piece of secret data using a one-time symmetric key (less than 2048 bits). The platform can then use the TPM to protect the one-time symmetric key.
2. The platform can render the large piece of secret data as smaller blocks of secret data and then use the TPM to encrypt each of the smaller blocks. The platform has the responsibility to manage the block creation and re-assembly to recover the original piece of secret data upon decryption.

In general, the first option is easier and faster. The figure below illustrates the process of using the TPM to encrypt a small piece of secret data.

The TPM implements a key hierarchy of all keys used for protected storage functions. The root of this hierarchy is the Storage Root Key (SRK). Each key in the hierarchy is encrypted using the key that is at the next level up in the hierarchy. Thus, the encryption of secret data using the TPM results in a "Data Blob" and a "Key Blob", both of which are opaque and can be stored away on arbitrary media.

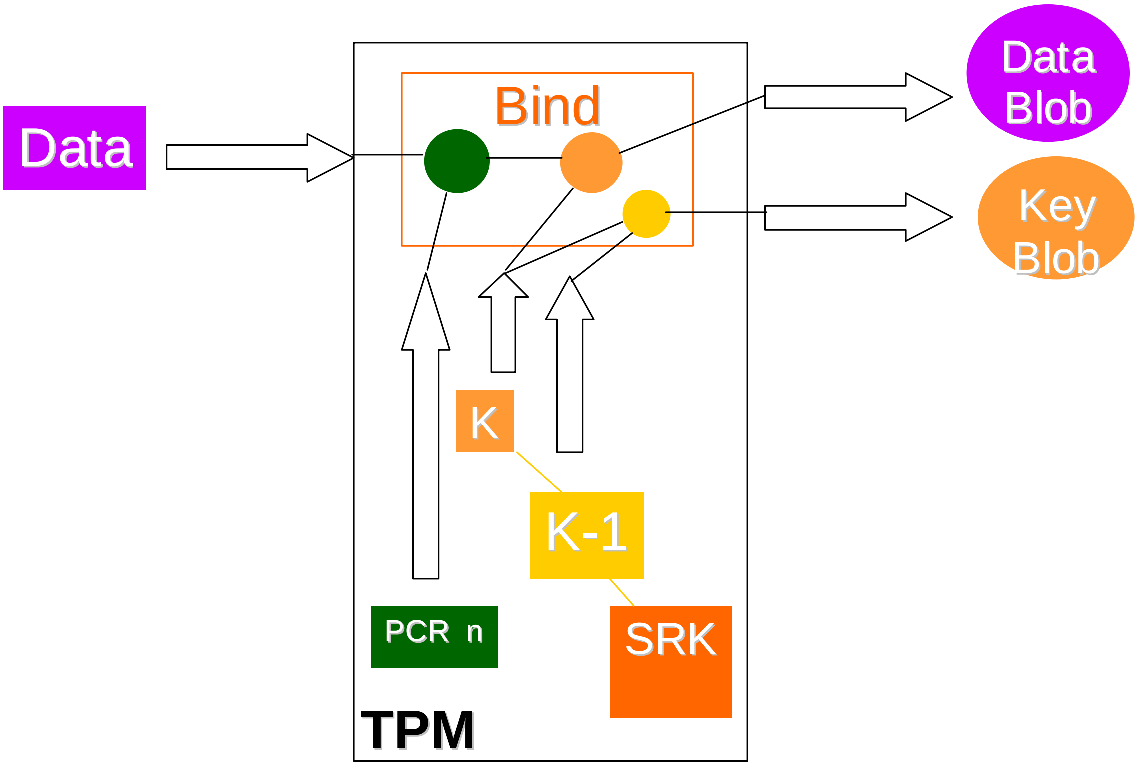


Binding Information to the Platform

Certain types of critical data can be logically bound to the platform on which they can be used. Data that is bound to a particular platform is only accessible by that platform if the conditions specified in the binding are met. If this data migrates to a different platform, or if the specific binding conditions on the same platform are not met, the data cannot be accessed.

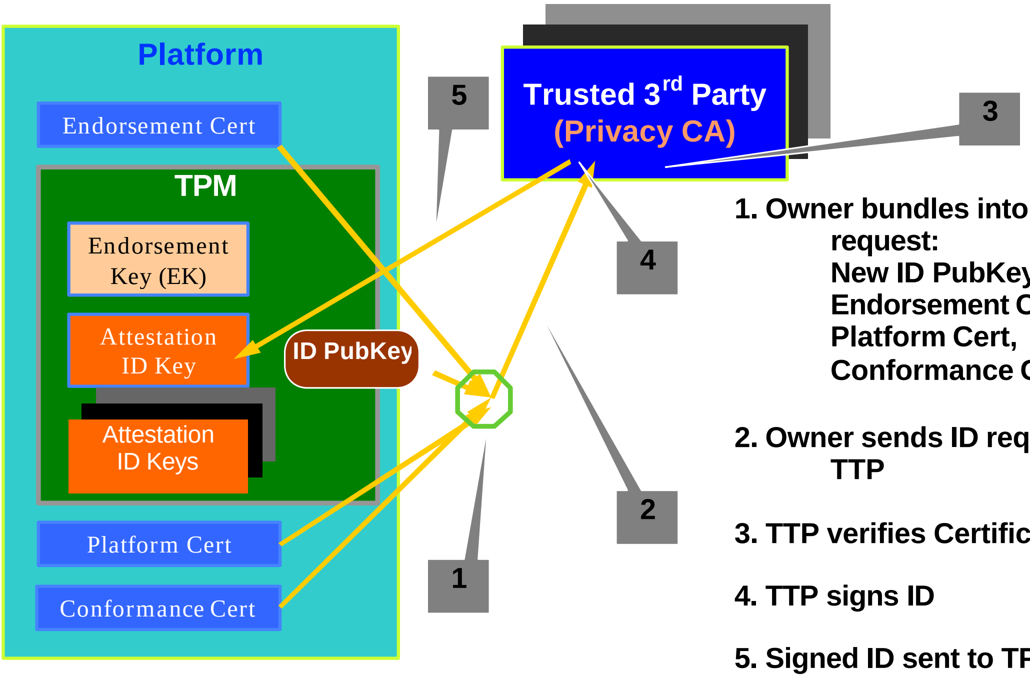
Specific hardware and/or software configuration information about the platform can be used to implement the logical binding of critical information to it. Such information about the platform is calculated by the TPM software stack and stored into the Platform Configuration Registers (PCR) available within the TPM.

While binding secret data to the platform, the TPM merges the data together with the values contained in one or more PCR registers and then encrypts the combination as a whole. At a later time, when the secret data needs to be accessed, the values of the necessary platform configurations are calculated and the data is released for use only if the calculated and stored values match.



Attestation (Platform Authentication)

The figure below illustrates the process of acquiring AIKs.



1. Owner bundles into an ID request:
New ID PubKey
Endorsement Cert,
Platform Cert,
Conformance Cert

2. Owner sends ID request to TTP

3. TTP verifies Certificates

4. TTP signs ID

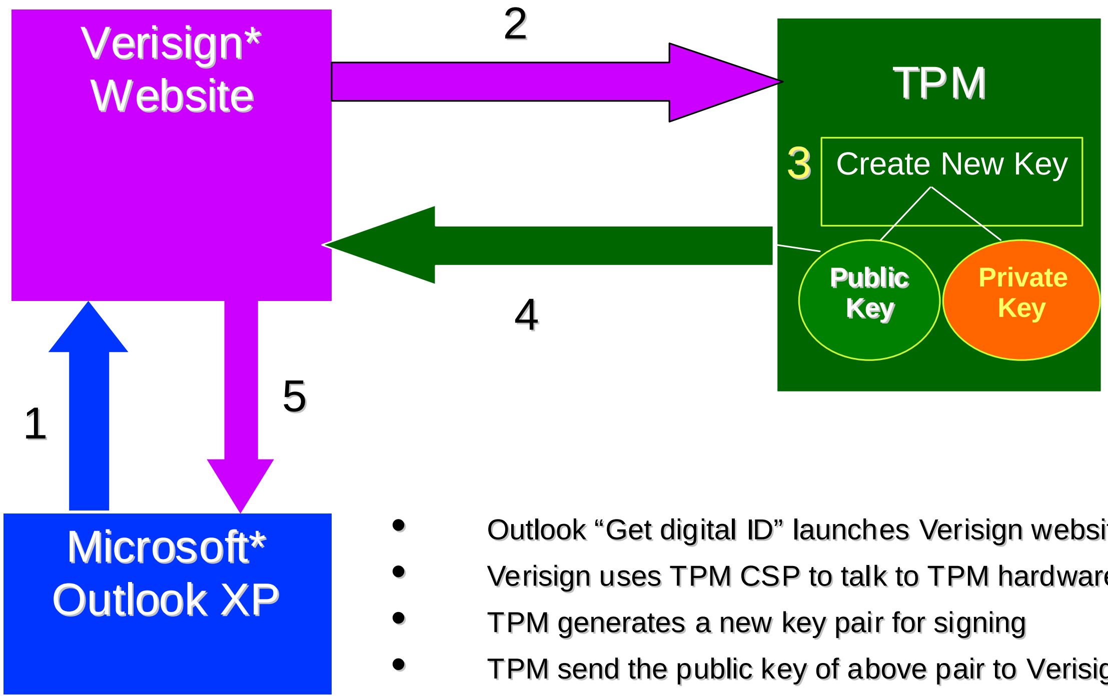
5. Signed ID sent to TPM

AIKs are created using Certificates (also called Credentials) available within the TPM. AIKs do not have any direct association with the EK or the credentials.

AIKs are always bound to the platform and can be used to provide attestation to the platform's identification and configuration. It is important to note that the service provider (or challenger) trusts the Trusted Third Party (TTP) to do its due diligence before issuing AIKs to a platform.

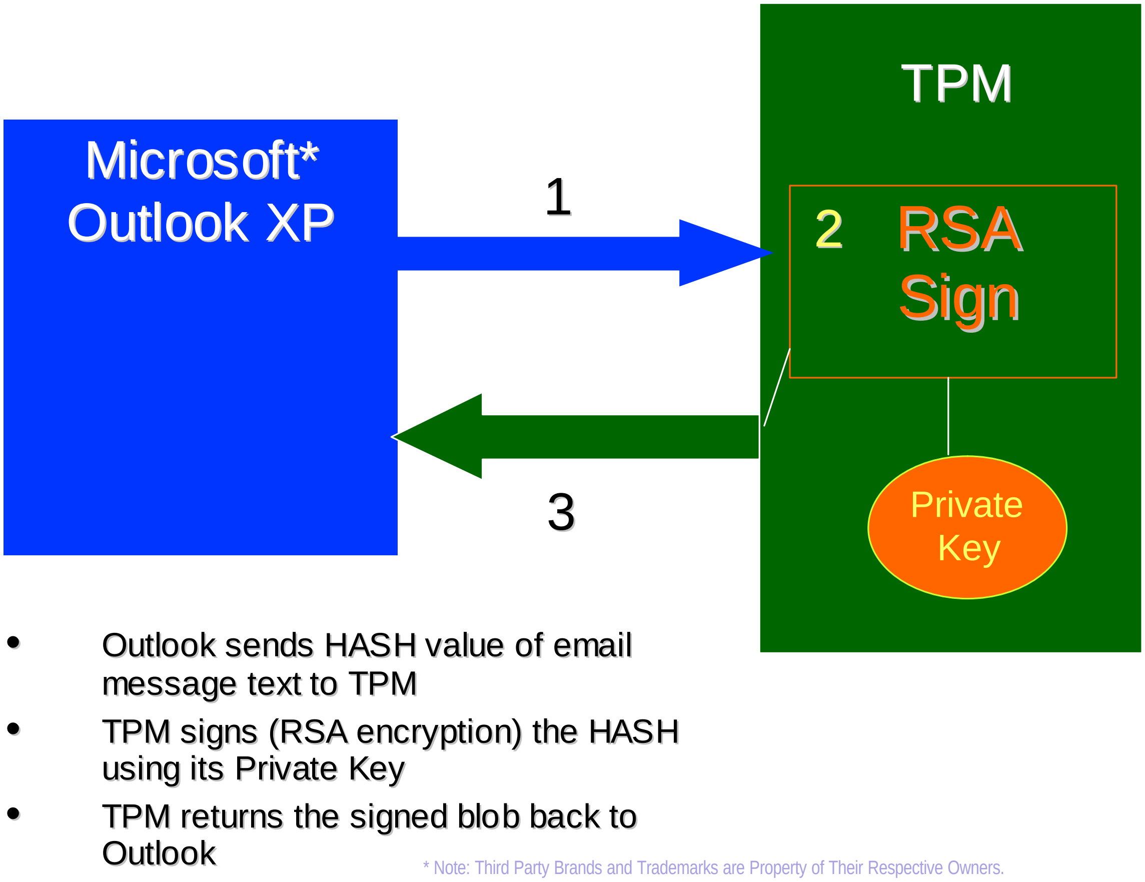
Example Application (Microsoft Outlook)*

The illustration below shows how the TPM can be used through Microsoft* Outlook to acquire an email signing/encryption certificate from a TTP such as Verisign*, and carry out email signing and encryption.



- Outlook "Get digital ID" launches Verisign website
- Verisign uses TPM CSP to talk to TPM hardware
- TPM generates a new key pair for signing
- TPM send the public key of above pair to Verisign
- Verisign "signs" the public key and returns to Outlook

* Note: Third Party Brands and Trademarks are Property of Their Respective Owners.



- Outlook sends HASH value of email message text to TPM
- TPM signs (RSA encryption) the HASH using its Private Key
- TPM returns the signed blob back to Outlook

* Note: Third Party Brands and Trademarks are Property of Their Respective Owners.

TPM implementation on Notebook PCs

Mechanical Requirements

The TPM has to be permanently attached to the motherboard by soldering it down. This reinforces the fact that the TPM provides a 1:1 binding between itself and the platform that it is attached to. Due to this requirement it is a good idea to factor in the real estate required for the TPM at an early stage in the motherboard design and layout process. The TCPA also recommends the provision of a tamper detection mechanism that can provide tamper evidence. An example of a tamper detection mechanism is the use of tamper tape.

Electrical Requirements

The TPM attaches to the platform via the LPC bus. Mobile platforms implement aggressive techniques for power management to conserve battery life. The LPC bus is powered down during platform sleep states and so is the TPM. It is important that the TPM comply with platform power management schemes, as specified in the ACPI specification.

Software Requirements

All the components identified in the software stack subsection of the TPM architecture section are required. At this time there is no single provider of all the different software components, and as such, each TPM vendor has to supply all the necessary components to implement their TPM part on the platform.

Privacy Related Requirements

Please refer to the next section on managing privacy.

Managing Privacy

Introduction

Privacy is extremely important to every business and individual concerned about protecting confidential & personal information. In the computing context, privacy provides a way to prevent others from gaining access to information without the informed consent of its owners. Cell phones, caller ID, credit cards, and Internet provide people with dramatic new levels of freedom that can enhance business processes and personal lives, but these innovations come with a privacy price tag. All of these systems are capable of providing information, including financial and personal data that most users assume to be confidential. The TCPA believes that the ability to ensure such confidentiality through privacy controls is an essential prerequisite of a trusted system. The following sections take a look at the different types of platform users and the privacy control mechanisms available on a TPM device.

Customer Types

As described in the previous sections, the TPM helps provide means to protect data and to provide platform identification in a trusted manner. Different types of users have different security and privacy needs. Below are two broad categories of platform users.

Privacy conscious consumer

This type of user is extremely protective of his platform and doesn’t necessarily understand the exact benefits and limitations of a TPM based platform. This type of user would rather just not use the TPM.

A variation of this category is a user that wants to control when & how the TPM in the platform is used. For example, this user may want to use the protected storage capability of the TPM at all times, but not the capability to provide platform authentication. This type of user would need a way to disable the platform attestation capability when he has to.

Enterprise User

This type of user has limited control of the security and privacy functions of the platform, as these are controlled by the corporate IT department.

Privacy Requirements

Fair information practices require the use of the following principles (where applicable) while designing a product with privacy related implications:

Notice

Before collection of information, or its use or disclosure, the owner of the information must be notified about the "who, how, what & why" aspects of the information transfer. The notice must be provided in a clear, easy to read and follow type of manner.

In the case of platforms with TPMs, the owner of the platform must be made aware of the nature and extent of the security features provided by the TPM, and a set of guidelines for proper use.

Access

Individuals must be given reasonable access to personal information for the purpose of reviewing for accuracy and making updates. This principle is not directly applicable to TPM based platforms.

Choice

An individual is able to decide if and how their private information may be used. Choice is typically provided through "Opt-in" or "Opt-out" mechanisms.

Opt-in

This mechanism requires the user to say "Yes" before a particular function, feature, or service is provided, i.e. it is disabled by default.

Opt-out

This mechanism requires the user to explicitly say "No" to a particular feature or function to disable it, i.e. it is enabled by default.

In the case of platforms with TPMs, the platform manufacturer must provide a mechanism for user "opt-in" or "opt-out" according to the manufacturer's product privacy guidelines.

Security

This refers to the protection of private information that is stored or transmitted.

In the case of platforms with TPMs, the TPM, if enabled, enables protected storage of private information.

TPM Configuration & Shipping Options

The TPM allows for numerous states to be set before the shipping of the platform. The three main controls on the TPM are: Physical Presence, Enable Ownership, and Enabling the TPM. The stated default in the specification is to ship without a TPM Owner, with TakeOwnership disabled and the TPM itself disabled. This combination is the most restrictive and the highest privacy sensitive setting.

The platform manufacturer will set the TPM according to the requirements specified by the platform user. Thus, although the physical hardware may be exactly the same, the settings may be different.

Physical Presence requires that the platform designer include some mechanism to indicate that a human is next to the platform. This could be the inclusion of a jumper that can be set, a button to push (including the keyboard), or biometric device. It is important that this mechanism creates an unambiguous indication that the human is present – something that cannot be spoofed by local or remotely running software.

The TPM must have an "owner" to perform most operations. Taking ownership, as a TCPA function, has to be accomplished by the platform (and TPM) owner before the TPM can perform any useful operations. One way to clear any previous ownership and create a new TPM owner is through the physical presence mechanism. The TakeOwnership flag provides the capability to disallow the creation of a TPM owner.

The TCPA provides mechanisms to temporarily activate/deactivate and enable/disable the TPM. Please refer to the TCPA specification for the details. However, in addition to the privacy protections provided by the TCPA, it is generally a good idea to provide a separate hardware disable mechanism for the TPM device in the system so that it is possible to guarantee that the TPM device is completely shut off in the system when required.

Banias TPM Enabling Initiatives

The TPM is a key element of Intel's Safer Computing initiative. On September 10, 2002, at the Intel Developers Forum in San Jose, CA, Intel and VeriSign* announced their collaboration on enhancing the value and garnering industry support of safer computing for PC clients, with an initial focus on next generation wireless notebook PCs. VeriSign* will optimize its digital certificates and "Personal Trust Agent (PTA)" on the future mobile computing platforms with TPM support, based on Intel's next generation mobile processor, code named Banias. The collaboration will enable PC OEMs to integrate VeriSign's* PTA and digital certificates into Banias processor-based notebooks, enabling a platform ready for corporate IT to deploy with VeriSign's Public Key Infrastructure services to enable strong authentication, authorization, digital signatures, encryption and more secure messaging.

Intel and VeriSign* will jointly promote security (especially security on wireless notebooks), TPM version 1.1 adoption, and VeriSign's* Managed PKI services. By incorporating digital certificate functionality into TPM chips that support Banias processor-based notebook PCs, a user's digital certificates and attributes can be stored in hardware, making it much more difficult to compromise the certificates and attributes via traditional network or Internet connections. This also transforms any TPM-enabled Banias processor-based notebook PC into a "digital credential" that can then be used to perform many e-business functions in the corporate IT environment, such as single sign-on, more secure remote access, and trusted peer-to-peer computing.

References

TCPA Main Specification v1.1b
TSS Specification v1.0
TCPA PC Specific Implementation Specification