TRUSTED PLATFORM MODULE

The TPM is a microcontroller that stores keys, passwords and digital certificates. It typically is affixed to the motherboard of a PC. This silicon ensures that the information stored there is made more secure from external software attack and physical theft.

TPMs currently are provided by **Atmel**, **Broadcom**, **Infineon**, **Sinosun**, **STMicroelectronics**, and **Winbond** in discrete and integrated forms.

TPM BASIC FUNCTIONS

Measure and record integrity metrics.
Report integrity metrics.
Protect keys and other small data.

TPM ARCHITECTURE

The **Input and Output** component manages information flow over the communications bus. It performs protocol encoding/decoding suitable for communication over external and internal buses. It routes messages to appropriate components.

The **Cryptographic Co-Processor** implements cryptographic operations within the TPM. Those operations include the following: **asymmetric key generation** (RSA), **asymmetric encryption/decryption** (RSA), **hashing** (SHA-1) and **random number generation** (RNG).

The **Opt-In** component provides mechanisms and protections to allow the TPM to be turned on/off, enabled/disabled, activated/deactivated. The Opt-In component maintains the state of persistent and volatile flags and enforces the semantics associated with these flags.

The **Power Detection** component manages the TPM power states in conjunction with platform power states. TCG requires that the TPM be notified of all power state changes.

The **Execution Engine** runs program code to execute the TPM commands received from the I/O port.

The **Non-volatile Memory** component is used to store persistent identity and state associated with the TPM.

A **Platform Configuration Register** (PCR) is a 160-bit storage location for discrete integrity measurements. There are a minimum of 16 PCR registers. All PCR registers are **shielded locations** and

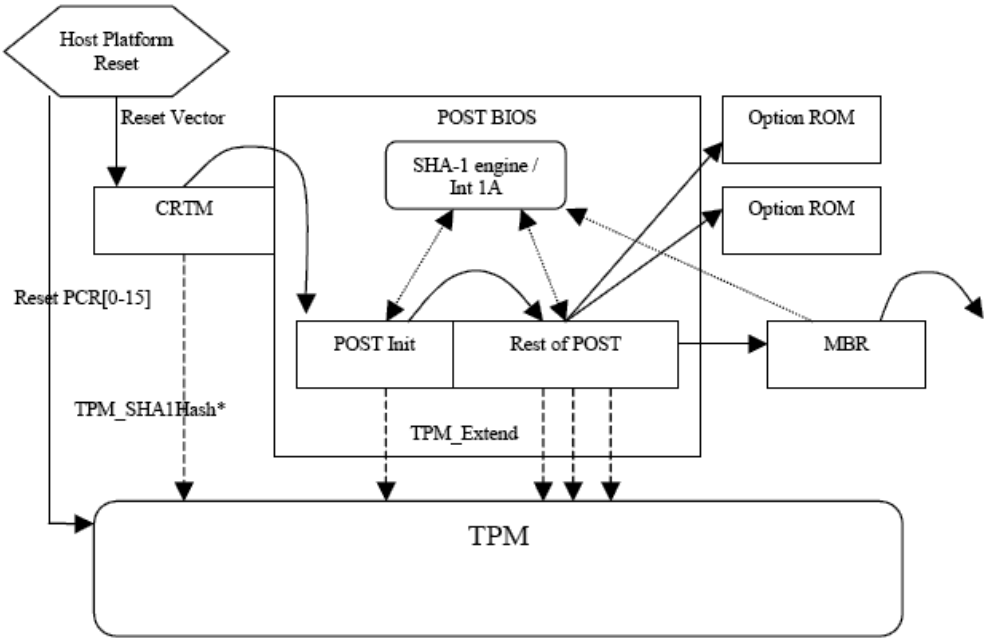
are inside of the TPM.

ROOT OF TRUSTS

Root of Trust is a component that must always behave in the expected manner, because its misbehavior cannot be detected.

Root of Trust for Measurement (RTM) a computing engine capable of making reliable integrity measurements. Typically the normal platform computing engine, controlled by the CRTM. This is the root of the chain of transitive trust. The RTM is axiomatically trusted. Trust in this component is expressed in the Host Platform Certificate. This is the point from which all trust in the measurement process is predicated. The RTM includes a core component (the CRTM).

Core RTM (CRTM) is the component of the RTM from which the platform begins execution of one of its trusted states.



Static Core RTM (S-CRTM) MUST be an immutable portion of the Host Platform's initialization code that executes upon a Host Platform Reset. The Host Platform's execution MUST begin at the CRTM upon any Host Platform Reset. The trust in the Host Platform is based on this component. The trust in all measurements is based on the integrity of this component.

- The BIOS is composed of a BIOS Boot Block and a POST BIOS. CRTM is the BIOS Boot Block.
- CRTM is the entire BIOS.

Dynamic Core RTM (D-CRTM) MUST be an immutable portion of the Host Platform but is not required to begin at the Host Platform Reset. The location and method of executing this is Host Platform implementation dependent but MUST be a Trusted Process. While the D-CRTM executes after, and in some respects within, the S-CRTM, the value of the D-CRTM's transitive trust chain does not depend

on the S-CRTM's transitive trust chain.

INTEL TXT

Root of Trust for Storage (RTS) is a computing engine capable of maintaining an accurate summary of values of integrity digests and the sequence of digests. Also the RTS provides protection on data in use by the TPM but held in external storage devices. The RTS provides confidentiality and integrity for the external blobs. The RTS also provides the mechanism to ensure that the release of information only occurs in a named environment. The naming of an environment uses the PCR selection to enumerate the values. Data protected by the RTS can migrate to other TPM.

Root of Trust for Reporting (RTR) is a computing engine capable of reliably reporting information held by the RTS.

TPM KEY PROPERTIES

Storage Key is used to wrap and unwrap other keys in the Protected Storage hierarchy.

Signing Key is used for signing operations, only. This means that it MUST be a leaf of the Protected Storage key hierarchy.

Binding Key can be used for **TPM_Bind** and **TPM_UnBind** operations only. Binding is equivalent to traditional asymmetric encryption.

Attestation Identity Key (AIK) is a special purpose signature key created by the TPM; an asymmetric key, the private portion of which is non-migratable and protected by the TPM. The public portion of an AIK is part of the AIK Credential, issued using either the Privacy CA or DAA protocol. An AIK can only be created by the TPM Owner or a delegate authorized by the TPM Owner. The AIK can be used for platform authentication, platform attestation and certification of keys.

Migratable key is a key which is not bound to a specific TPM and with suitable authorization can be used outside a TPM or moved to another TPM.

Non-migratable key is a key which is bound to a single TPM; a key that is (statistically) unique to a single TPM but may be moved between TPMs using the maintenance process.

Endorsement Key (EK) is an RSA Key pair composed of a public key and private. The EK is used to recognize a genuine TPM. The EK is used to decrypt information sent to a TPM in the Privacy CA and DAA protocols, and during the installation of an Owner in the TPM.

Storage Root Key (SRK) is the root key of a hierarchy of keys associated with a TPM's Protected Storage function; a non-migratable key generated within a TPM.

The **maintenance** feature is a vendor-specific feature, and its implementation is vendor specific. Maintenance is different from backup/migration, because maintenance provides for the migration of both migratory and non-migratory data.

AUTHENTICATION TO THE TPM

Object Specific Authorization Protocol (OSAP).
Object Independent Authorization Protocol (OIAP).

CREDENTIALS

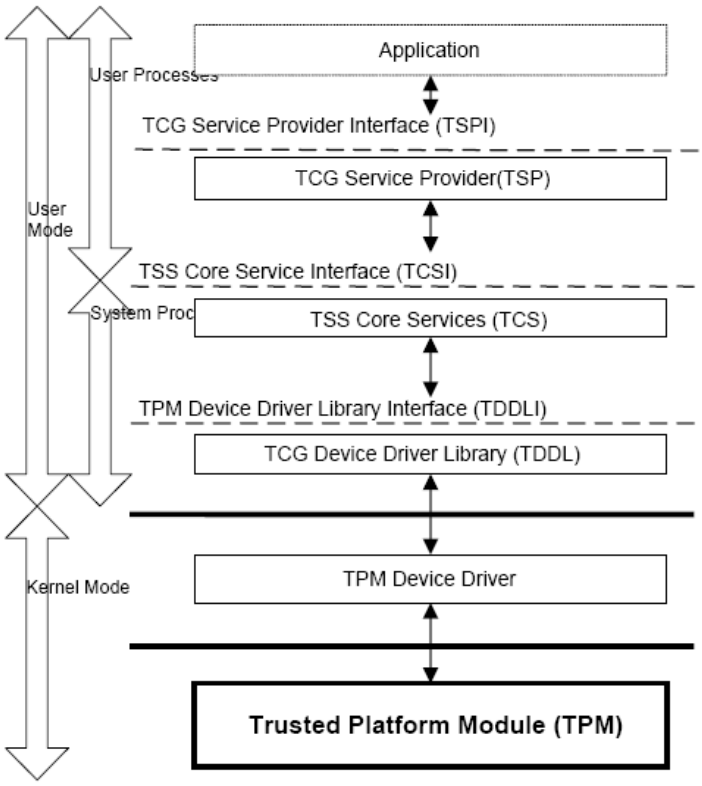
Platform credential is a credential, typically a digital certificate, attesting that a specific platform contains a unique TPM and TBB.

Endorsement Key Credential is a credential containing the public part from the EK that asserts that the holder of the private part from the EK is a TPM conforming to TCG specifications. Also EK Credential contains TPM model and TPM manufacture.

AIK Credential is a credential issued by a Privacy CA that contains the public portion of an AIK key signed by a Privacy CA. The meaning and significance of the fields and the Privacy CA signature is a matter of policy. Typically it states that the public key is associated with a valid TPM.

TCG SOFTWARE STACK (TSS)

The **TSS** is a software specification that provides a standard API for accessing the functions of the TPM. Application developers can use this software specification to develop interoperable client applications for more tamper-resistant computing.



The **TCG Service Provider (TSP)** provides the high-level TCG functions allowing applications to focus on their specialty while relying on the TSP to perform most of the trusted functions provided by the TPM.

The **TCG Core Services (TCS)** provides a common set of services per platform for all service providers. Since the TPM is not required to be multithreaded, it provides threaded access to the TPM.

The **TCG Device Driver Library (TDDL)** is an intermediate module that exists between the TCS and the kernel mode TPM Device Driver (TDD). The TDDL provides a user mode interface. Because the TPM is not required to be multithreaded, the TDDL is to be a single instance, single threaded module.

The **TCG Device Driver (TDD)** is the kernel mode component that receives bytestreams from the TDDL and sends them to the TPM returning the responses back to the TDDL.

TrouSerS is an CPL (Common Public License) licensed Trusted Computing Software Stack. Today, we're working towards compliance with the TSS 1.1 specification, but will begin work on complying with the 1.2 spec as soon as its released.

The **NTRU Core TCG Software Stack** (CTSS) is interoperable with all 1.1b compliant TPMs. It is designed for portability with current support for Windows XP/2000 and Linux 2.4 platforms.

TPM USECASES

Trusted Grub is the enhancement of Linux boot loader GRUB for adding the TCG measurement capability. It supports TCG 1.1b compliant PCs. Main features are:

- Measurement during the process of loading Grub
- Stage 1 measures the first sector of the stage 1.5 (or stage 2).
- Stage 1(=MBR) itself is measured by BIOS just when it is loaded.
- The first sector of stage 1.5 (or stage 2) measures the remaining sectors.
- Stage 1.5 measures the stage 2, too.
- Just after the Grub is booted, it measures the configuration file named grub.conf.
- Then it measures a number of files in the sequence specified in this configuration file.

The **Enforcer** is a Linux Security Module designed to improve integrity of a computer running Linux by ensuring no tampering of the file system. It can interact with TPM to provide higher levels of assurance for software and sensitive data. It can check, as every file is opened, if the file has been changed, and take a specified action when it detects tampering. The actions can be any combination of log the error, deny access to the file, panic the system, or several operations that work with the TPM.

The **OpenCryptoki** is an implementation of the PKCS#11 standard which defines an API to be used to interact with devices that hold cryptographic data and perform cryptographic functions. Providing PKCS#11 support for the TPM will allow applications to easily exploit the capabilities of the TPM.

OpenSSL TPM Engine

TPM Emulator

TPM tools

Wave Systems' EMBASSY Trust Suite introduces support for Windows Vista, providing TPM management and security applications that further enhance Vista's security. For systems containing the **Seagate Momentus® 5400 FDE.2** hard drive, the Embassy Security Center includes the Trusted Drive Manager to activate and manage the drive’s hardware-based full disk encryption.

TPM ATTACKS

Dictionary attack.
TPM Reset attack.

LINKS FOR FURTHER READING

[1] http://trousers.sourceforge.net/grub.html
[2] http://trousers.sourceforge.net/pkcs11.html
[3] http://enforcer.sourceforge.net
[4] http://trousers.sourceforge.net
[5] http://www.ntru.com
[6] http://www.wavesys.com
[7] https://www.trustedcomputinggroup.org