Trusted Platform Module (TPM)

Information Technologies for IPR Protection
• The **Trusted Computing Group (TCG)**, successor to the **Trusted Computing Platform Alliance (TCPA)**, is an initiative led by AMD, Hewlett-Packard, IBM, Infineon, Intel, Lenovo, Microsoft, and Sun Microsystems to implement trusted computing.

• TCG's original major goal was the development of a **Trusted Platform Module (TPM)**, a semiconductor intellectual property core or integrated circuit that conforms to the trusted platform module specification put forward by the Trusted Computing Group and is to be included with computers to enable trusted computing features.
What is TPM?

- The TPM is a microcontroller that stores keys, passwords and digital certificates.
- It typically is affixed to the motherboard of a PC, but can be used in any computing device that requires these functions.
- The nature of this silicon ensures that the information stored there is made more secure from external software attack and physical theft.
• **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.
  
  – **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**
TPM as an Endpoint of Communication (1/2)

- Classic message exchange based on asymmetric cryptography suggests that messages intended for one and only one individual can be encrypted using a public key.
- Furthermore, the message can be protected from tampering by signing with the private key.
- Keys are communication endpoints and improperly managed keys can result in loss of security.
- Additionally, improperly configured endpoints may also result in loss of security.
- The TPM aids in improving security by providing both key management and configuration management features.
Four classes of protected message exchange:

- **Binding**
  - The sender uses the public key of the intended recipient to encrypt the message.
  - When the private key is managed by the TPM as a non-migratable key only the TPM that created the key may use it.

- **Signing**
  - Signing associates the integrity of a message with the key used to generate the signature.

- **Sealing**
  - **Sealing** takes binding one step further. Sealed messages are bound to a set of platform metrics specified by the message sender.

- **Sealed-Signing**
  - Signing operations can also be linked to PCR registers as a way of increasing the assurance that the platform that signed the message meets a specific configuration requirement.
Key Attributes

- All keys managed by the TPM have an attribute designation of *migratable* or *non-migratable*.
- The key attribute determines whether a key may be transferred from one TPM to another.
- Attribute value is established at the time the key is created and cannot be changed.
Key Types (1/2)

- **Signing keys**
  - Asymmetric general purpose keys used to sign application data and messages.
  - Signing keys can be migratable or non-migratable. Migratable keys may be exported / imported between TPM devices. The TPM can sign application data and enforce migration restrictions.

- **Storage keys**
  - Asymmetric general purpose keys used to encrypt data or other keys.
  - Storage keys are used for wrapping keys and data managed externally.

- **Identity Keys (a.k.a. AIK keys)**
  - Non-migratable signing keys that are exclusively used to sign data originated by the TPM (such as TPM capabilities and PCR register values).
Key Types (2/2)

- **Endorsement Key (EK)**
  - A non-migratable decryption key for the platform.
  - It is used to decrypt owner authorization data at the time a platform owner is established and to decrypt messages associated with AIK creation.
  - It is never used for encryption or signing.

- **Bind keys**
  - May be used to encrypt small amounts of data (such as a symmetric key) on one platform and decrypt it on another.

- **Legacy Keys**
  - Keys created outside the TPM. They are imported to the TPM after which may be used for signing and encryption operations.
  - They are by definition migratable.

- **Authentication Keys**
  - Symmetric keys used to protect transport sessions involving the TPM.
• **External Storage**
  To allow for virtually unlimited keys and storage areas the RTS packages keys destined for external storage into encrypted key BLOBs.

• **Key Cache Management**
  The TPM exposes interfaces that allow external programs the ability to manage the limited storage resources of the TPM.
The TCG privacy model generally follows the privacy guiding principles established by the W3C P3P working group

- **Notice and Communication**
  - Service providers should provide timely and effective notices of their information practices, and user agents should provide effective tools for users to access these notices and make decisions based on them.

- **Choice & Control**
  - Users should be given the ability to make meaningful choices about the collection, use, and disclosure of personal information.

- **Fairness & Integrity**
  - Users should retain control over their personal information and decide the conditions under which they will share it. Service providers should treat users and their personal information with fairness and integrity. This is essential for protecting privacy and promoting trust.

- **Confidentiality**
  - Users' personal information should always be protected with reasonable security safeguards in keeping with the sensitivity of the information.
Criticisms

• **Remote attestation** creates an unforgeable summary of the software on a computer
  – Still a potential threat to privacy.

• **Binding and sealing**
  – A herald to *Digital Rights Management* systems of unprecedented restrictiveness.
Software Stack

Application → CAPI → CSP → TSS (TCPA Software Stack) → TPM Device Driver Library → TPM Hardware

Application → PKCS#11
CryptoAPI

- CryptoAPI is an API developed by Microsoft to provide any application, not just Web-based programs, with easy-to-implement security features.
Using CryptoAPI

- Retrieve available *cryptographic service providers*:
  - `CryptEnumProviders()`

- Acquire a handle to a particular key container within a particular cryptographic service provider (CSP):
  - `CryptAcquireContext()`

- Get the handle to the key / key pair:
  - `CryptGenKey()`, `CryptGetUserKey()`

- Encrypt and decrypt data:
  - `CryptEncrypt()`, `CryptDecrypt()`

- Store a session key:
  - `CryptExportKey()`, `CryptImportKey()`

- Export the public key information associated with the corresponding private key:
  - `CryptExportPublicKeyInfo()`, `CryptExportPublicKeyInfoEx()`
• Trusted Computing Group
  https://www.trustedcomputinggroup.org/
• Crypto API
  http://www.msdn.com/