Trusted Computing

Seong Soo Kim
Roger Heiniluoma

Trusted Computing

- DOD developed criteria for determining Trust levels for computer systems
- Started work in 1967, and revised regularly until 1985.
- Published under the "Rainbow" Series
  - Trusted Computing is the "Orange Book"
  - "Dark Lavender", "Hot Peach", and "Venice Blue" are some of the 33 other books in the DOD series.

Trusted Computing

- The Orange Book standard held for nearly twenty years as the US DoD's standard for evaluating the security fitness of computing systems.
- Evolution of the systems forced the government to reconsider the system, and base evaluations on the new "Common Criteria"

Trusted Computing

- Trusted Computing Standards are now constantly re-evaluated by the National Security Telecommunications and Information Systems Security Committee
- The committee recommends and specifies security related issues from training to wireless, to web browser security.
- Some of the committee memoranda are still classified.

Common Criteria

- ISO Standard 15408 (1999)
- Like most ISO standards, the documentation places a reader in acronym hell.
- There are 7 basic levels of certification called “EAL’s” (Evaluation Assurance Level)
- Administered through the CCEVS , after looking through the documentation, it is obvious that this is a government project.

EAL 1 – functionally tested

- This is the lowest assurance level for which evaluation is meaningful and economically justified. It is intended to detect obvious errors for a minimum outlay, but is unlikely to result in the detection of subtle security weaknesses. It is applicable where the requirement is for a low level of independently assured security. An EAL1 rating could support the contention that due care has been exercised with respect to systems handling personal or similar information.

- ***An EAL1 evaluation provides analysis of the security functions, using a functional and interface specification of the TOE, to understand the TOE's security behaviour. The analysis is supported by independent testing of the security functions.***

EAL2 - structurally tested

- This is the highest assurance level that can be used without imposing other than minimal additional tasks on the developer. If the developer applies reasonable standards of care, EAL2 may be feasible with no developer involvement other than support for security functional testing. It is applicable where the requirement is for allow to moderate level of independently assured security, but the complete TOE development record is not readily available. This may arise when securing legacy systems, or where access to the developer is limited.

- ***An EAL2 evaluation provides analysis of the TOE security functions, using its functional and interface specification as well as the high-level design of the subsystems of the TOE. Independent testing of the security functions is performed, and the evaluators review the developer's evidence of "black box" testing, and a search for obvious vulnerabilities.***

EAL3 - methodically tested and checked

- This assurance level permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage, without substantial alteration of existing sound development practices. It is applicable where the requirement is for a moderate level of independently assured security, with a thorough investigation of the TOE and its development without incurring substantial re-engineering costs.

- ***An EAL3 evaluation provides an analysis supported by "grey box" testing, selective independent confirmation of the developer test results, and evidence of a developer search for obvious vulnerabilities. Development environment controls and TOE configuration management are also required.***

EAL4 - methodically designed, tested and reviewed

- This is the highest assurance level which it is likely to be economically feasible to retrofit to an existing product line. EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices, which are rigorous but not overly specialised. It is applicable where the requirement is for a moderate to high level of independently assured security in conventional commodity products, and there is willingness to incur some additional security-specific engineering costs.

- ***An EAL4 evaluation provides an analysis supported by the low-level design of the modules of the TOE, and a subset of the implementation. Testing is supported by an independent search for obvious vulnerabilities. Development controls are supported by a life-cycle model, identification of tools, and automated configuration management.***

Beyond EAL 4

- Above EAL4 increasing application of specialised security engineering techniques is required. TOEs meeting the requirements of these levels of assurance will have been designed and developed with the intent of meeting those requirements. At the top, EAL7, level there are significant limitations on the practicability of meeting the requirements, partly due to substantial cost impact on the developer and evaluator activities, and also because anything other than the simplest of products is likely to be too complex to submit to current state-of-the-art techniques for formal analysis.

EAL5 - semiformally designed and tested

- EAL5 permits a developer to gain maximum assurance from security engineering based on rigorous commercial development practices, supported by moderate application of specialised security engineering techniques. Such a TOE will be designed and developed with the intent of meeting EAL5 requirements. EAL5 is applicable where the requirement is for a high level of independently assured security in a planned development, with a rigorous development approach but without incurring unreasonable costs for specialised security engineering techniques.

- ***An EAL5 evaluation provides an analysis of all the implementation. Assurance is supplemented by a formal model and a semiformal presentation of the functional specification and high level design, and a semiformal demonstration of correspondence. The search for vulnerabilities must ensure relative resistance to penetration attack. Modular design is required, and covert channel analysis may also be required.***

EAL6 - semiformally verified design and tested

- EAL6 permits a developer to gain high assurance from application of specialised security engineering techniques in a rigorous development environment, to produce a premium product for protecting high value assets against significant risks. EAL6 is applicable to the development of specialised security products, for application in high risk situations which justify the additional costs.

- ***An EAL6 evaluation provides an analysis which is supported by a modular and layered approach to design, and a structured presentation of the implementation. The independent search for vulnerabilities must ensure high resistance to penetration attack. Any search for covert channels must be systematic. Development environment and configuration management controls are further strengthened.***

EAL7 - formally verified design and tested

- EAL7 represents an achievable upper bound on evaluation assurance for practically useful products. It should only be considered for experimental application to all but conceptually simple and well understood products. EAL7 is applicable to the development of specialised security products, for application in extraordinarily high risk situations which justify the extraordinary additional costs. Practical application of this level is currently limited to products with tightly focused security functionality which is amenable to formal analysis.

- ***For an EAL7 evaluation the formal model is supplemented by a formal presentation of the functional specification and high level design showing correspondence. Evidence of developer "white box" testing and complete independent confirmation of developer test results are required. Complexity of the design must be minimised.***

So what does it mean ?

- In the commercial world, very little, as there is very little attention given to these standards outside the realm of government procurement.
- Even within government contracts, the standards are often only applicable to security sensitive systems.
- Very little of what we have discussed in this course so far directly pertains to these standards.
- The standards are criteria for making and evaluating security claims, not for specifying particular security standards to be met.

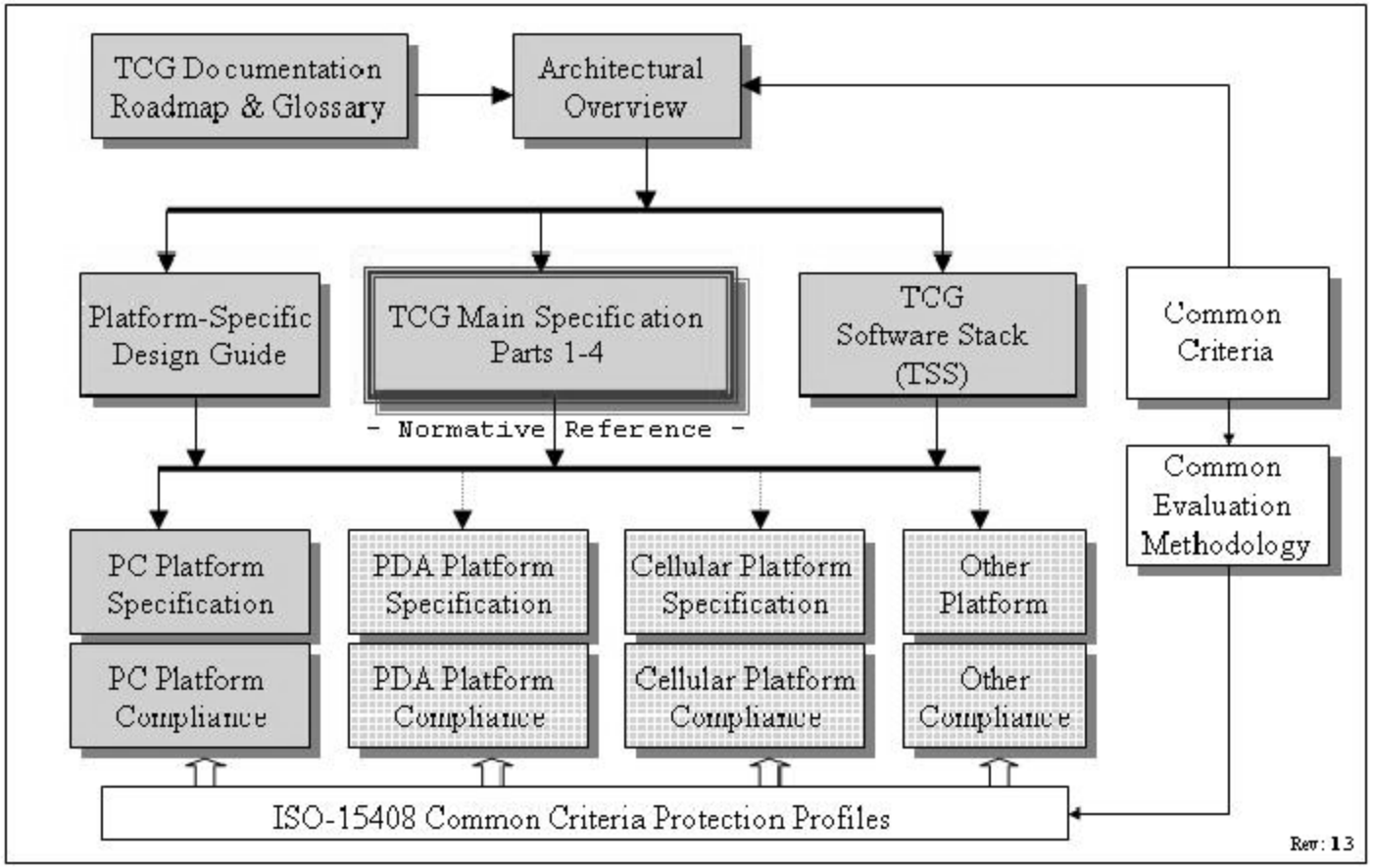
Trusted Computing Group

- Rather than an open standard for evaluation, the TCG established a specific set of security primitives and protocols to be implemented.
  - "**The Trusted Computing Group (TCG) is an industry standards body, comprised of computer and device manufacturers, software vendors, and others with a stake in enhancing the security of the computing environment across multiple platforms and devices.**
  - TCG will develop and promote open industry standard specifications for trusted computing hardware building blocks and software interfaces across multiple platforms, including PC's, servers, PDA's, and digital phones. This will enable more secure data storage, online business practices, and online commerce transactions while protecting privacy and individual rights."

Trusted Computing Group

- **The TCG takes the Common Criteria Standards, published as “Protection Profiles” and develops platform specific recommendations, implemented as “Trusted Platform Modules”**
- **The TCG has very specific guidelines such as:**
  - The TPM MUST support key sizes of 512, 768, 1024, and 2048 bits. The TPM MAY support other key sizes.
  - The RSA public exponent MUST be e, where e = $2^{16}+1$.

TCG Doc Roadmap – Main Spec



The Major Components of a TPM

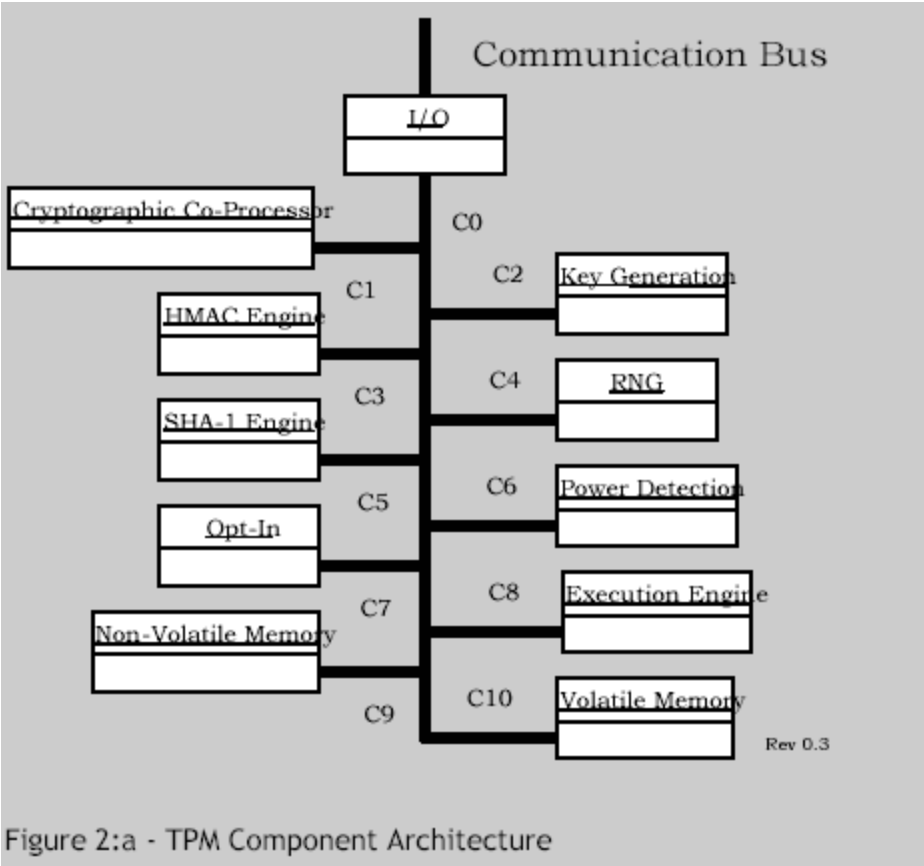


Figure 2:a - TPM Component Architecture

SAMPLE TPM-1

- **[TPM Architecture]**

- minimum algorithms: RSA, SHA-1, HMAC

- **1. Cryptographic Co-Processor :**
- Figure 2:a C1, implements cryptographic operations within the TPM.
- Asymmetric key generation (RSA), Asymmetric encryption/decryption (RSA), Hashing (SHA-1), Random number generation (RNG)
- May be other asymmetric algorithms such as DSA or elliptic curve.
- All Storage keys MUST be of strength equivalent to a 2048 bits RSA key or greater.

- RSA Engine

- no requirement concerning how the RSA algorithm is to be implemented.
- MUST support RSA.
- MUST use the RSA algorithm for encryption and digital signatures.
- MUST support key sizes of 512, 768, 1024, and 2048 bits. - minimum RECOMMENDED key size is 2048 bits.

- Signature Operations

- MUST use the RSA algorithm for signature operations

SAMPLE TPM-2

- Symmetric Encryption Engine:

- uses symmetric encryption to encrypt authentication information, provide confidentiality in transport sessions and provide internal encryption

- Using Keys

- Keys can be symmetric or asymmetric.

SAMPLE TPM-3

- **2. Key Generation**
- The Key Generation component, Figure 2:a C2, creates RSA key pairs and symmetric keys.

- Asymmetric – RSA

- TPM MUST generate asymmetric key pairs.
- private key is held in a shielded location.

SAMPLE TPM-4

- **3. HMAC Engine**
- Figure 2:a C3
- proof of knowledge of the authorization data and proof that the request arriving is authorized and has no modifications made to the command in transit.

- RFC 2104 will use a key length of 20 bytes and a block size of 64 bytes.

SAMPLE TPM-5

- **4. Random Number Generator**

- Figure 2:a C4 is the source of randomness
- salt-data may be provided by hardware or software sources – for example; from thermal noise, or by monitoring random keyboard strokes or mouse movements.
- allows implementation of a Pseudo Random Number Generator (PRNG) algorithm.

- **4.1 Entropy Source and Collector**
- The entropy source is the process or processes that provide entropy. These types of sources could include noise, clock variations, air movement, and other types of events.
- The entropy collector is the process that collects the entropy, removes bias, and smoothes the output.
- entropy collector must remove the bias before updating the state register.

- **4.2 State Register**
- non-volatile register and a volatile register.
- The TPM saves the current value of the volatile state register to the non-volatile register on TPM power-down.

SAMPLE TPM-6

- **4.3 Mixing Function**
- The mixing function takes the state register and produces output.
- The mixing function takes the value from a state register and creates the RNG output.

- **4.4 RNG Reset**
- These tests prove only that the RNG is still operating properly;

SAMPLE TPM-7

- **5. SHA-1 Engine**
- Figure 2:a C5, hash capability is primarily used by the TPM, as it is a trusted implementation of a hash algorithm.
- The TPM MUST implement the SHA-1 hash algorithm as defined by FIPS-180-1.
- The output of SHA-1 is 160 bits

- **6. Power Detection**
- Figure 2:a C6, manages the TPM power states in conjunction with platform power states.
- TCG requires that the TPM be notified of all power state changes.

- **7. Opt-In**
- mechanisms and protections to allow the TPM to be turned on/off, enabled/disabled, activated/deactivated.
- maintains the state of persistent and volatile flags and enforces the semantics
- no remote entity should be able to change TPM status without either knowledge of the TPM Owner or the Operator is physically present at the platform.

SAMPLE TPM-8

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

- **9. Non-Volatile Memory**
- Figure 2:a C9, is used to store persistent identity and state associated with the TPM.

SAMPLE TPM-9

[TPM Operation]

- **1. Initialization**
- TPM_Init transitions the TPM from a power-off state to an initialization process.

- **2. Self-Test Modes**
- TPM_SHA1Start, TPM_SHA1Update, TPM_SHA1Complete, TPM_SHA1CompleteExtend,
- TPM_Extend, TPM_Startup,
- TPM_ContinueSelfTest

- **2.1 Operational Self-Test**
- The response from the self-tests is pass or fail.
- A) RNG functionality
- B) Reading and extending the integrity registers.
- Testing the EK integrity, if it exists
- The integrity of the protected capabilities of the TPM

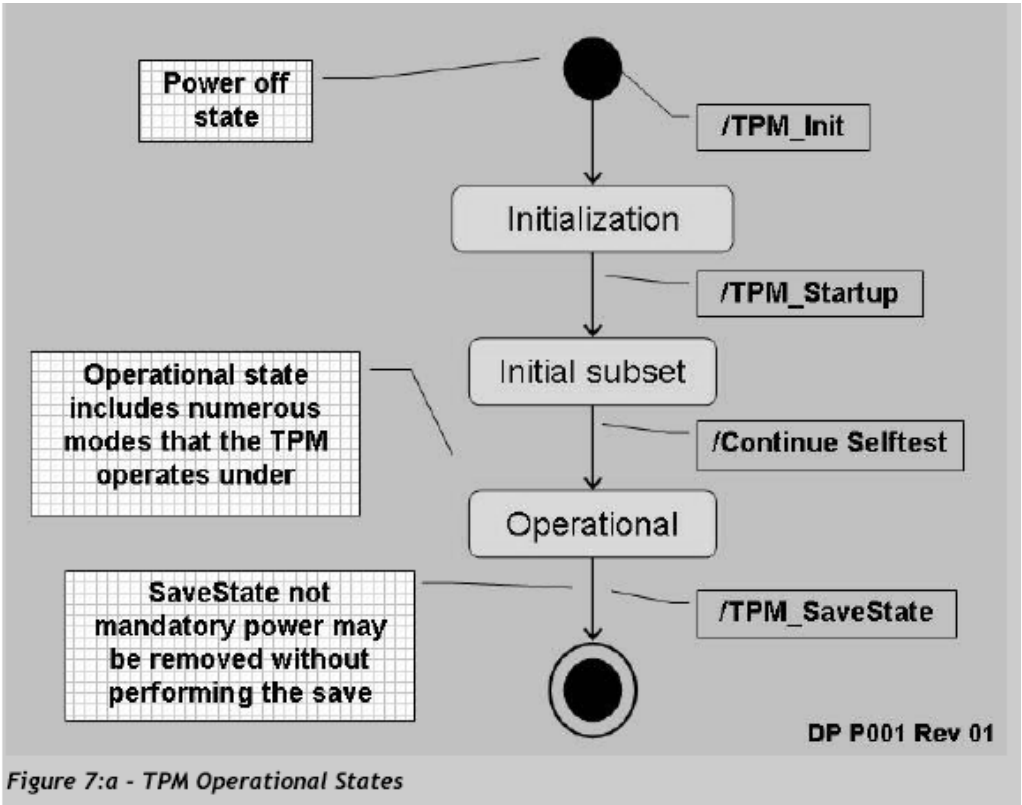


Figure 7:a - TPM Operational States

SAMPLE TPM-10

- **2.1 Operational Self-Test**
- A) The hash functionality
- B) Any symmetric algorithms : This check will use known data with a random key to encrypt and decrypt the data
- C) The key-wrapping mechanism
- Self-Test Failure → shutdown mode

- **3. Startup**
- from the initialization state to an operational state; Clear, State and Deactivated.

- **4. Operational Mode**
- enabled or disabled, active or inactive and owned or unowned.
- **4.1 Enabling a TPM**
- A disabled TPM is not able to execute commands that use the resources of a TPM.
- **4.2 Activating a TPM**
- A deactivated TPM is not able to execute commands that use TPM resources.
- The TPM_TakeOwnership command is available when deactivated.
- **4.3 Taking TPM Ownership**
- The owner of the TPM has ultimate control of the TPM.
- The owner of the TPM can enable or disable the TPM, create AIK and set policies for the TPM.
- TPM Owner authentication value MUST be a 160-bits which is held in persistent storage

SAMPLE TPM-11

- **5. Physical Presence**

- Physical presence implies direct interaction by a person – i.e. Operator with the platform
- Clearing an existing Owner from the TPM,
- Temporarily deactivating a TPM,
- Temporarily disabling a TPM.

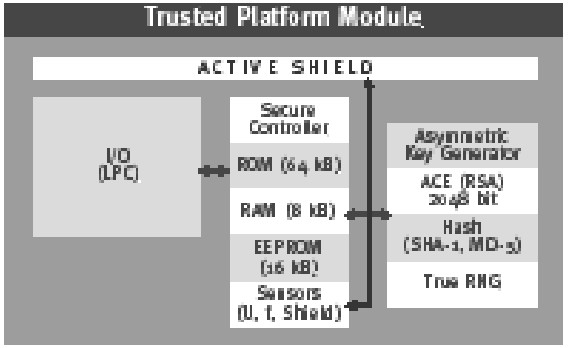
SAMPLE TPM-12

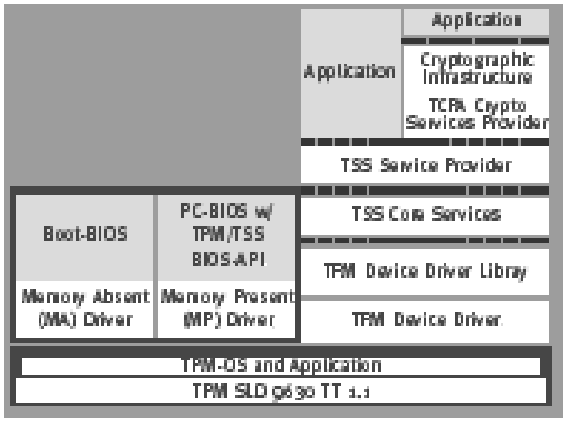
- **Intel: Infineon Trusted Platform Module (TPM)**
- This component on the PC motherboard is specifically designed to enhance platform security
- the TPM provides hardware-based protection for the encryption and digital signature keys that secure your data's confidentiality .

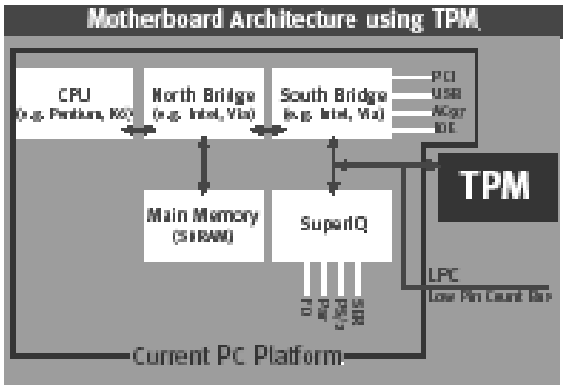
- Intel Desktop Board D865GRH Features

- **Features:**
- Intel® Pentium® 4 processor with a 400/533/800 MHz,
- Intel® Celeron® processor with a 400 MHz

- Secure Controller
- Protected Storage (EEPROM)
- Hardware-RSA-Accelerator (Signature Calculation, Signature Verification and Key Generation at 2048bit Key-using CRT)
- Hardware Hash Accelerator (SHA-1, MD-5)
- Asymmetric Key Generation (RSA, key lengths of up to 2048 bit)
- True Random Number Generator
- Low Power Consumption
- Low Pin Count (LPC) Interface
- Embedded Secure Operating System
- TCG Software Stack (TSS) compliant to specification 1.1b
- TPM Cryptographic Service Provider (CSP)
- This solution is based on the TCG Main Specification version 1.1b







SAMPLE TPM-13

[Attacks and Threats]

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

SAMPLE TPM-14

- The Intel TPM is basically a secure micro-controller with added cryptographic functionalities.

1. Crypto Capabilities

- a set of crypto capabilities that allow certain crypto functions to be executed within the TPM hardware.

(1) 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.

(2) 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.

(3) **Random Number Generator**

- The RNG is used to generate keys for various purposes.

(4) **Limited NVRAM for TPM Contents**

SAMPLE TPM-15

2. Contents

- the various contents within the TPM's internal hardware protected storage.

(1) 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.
- Generating method i) TPM command (TPM_CreateEndorsementKeyPair).
  ii) TPM manufacturer can squirt an externally generated EK into the TPM
- The EK is certified by the Endorsement Certificate (Cert).

(2) 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.

(3) Certificates

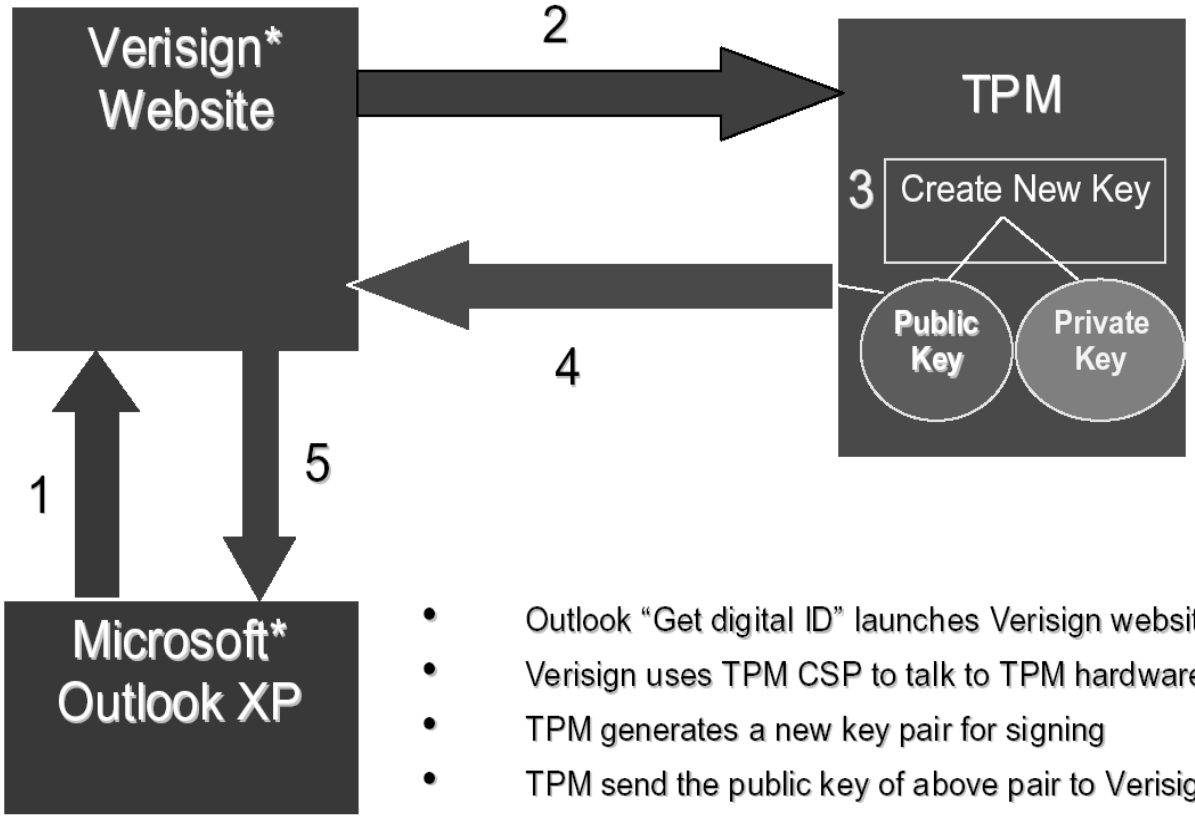
i) The Endorsement Cert contains the public key of the EK. particular TPM is genuine,

ii) The Platform Cert means the security components of the platform are genuine.

iii) The Conformance Cert provides attestation by an accredited party.

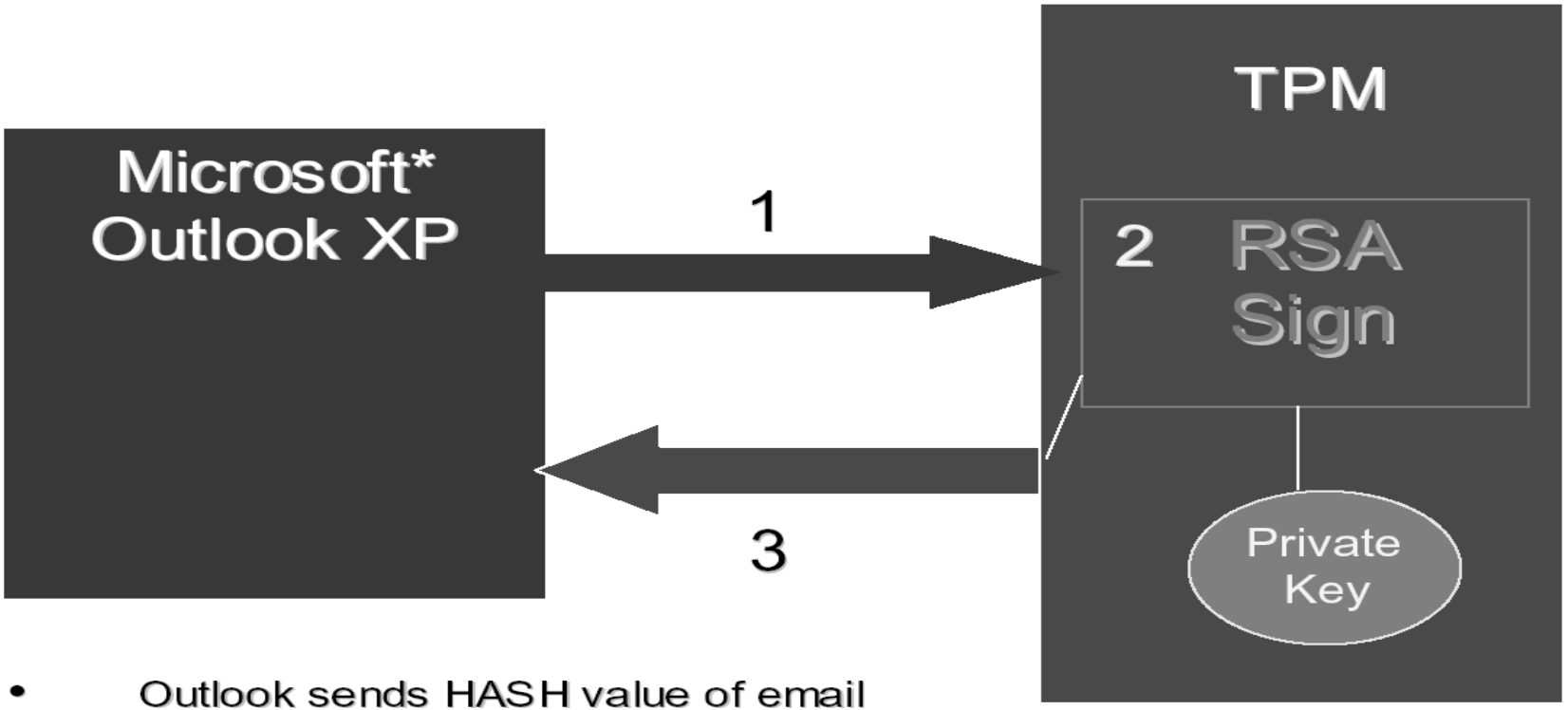
SAMPLE TPM-16

- ***Example Application (Microsoft* Outlook)***
- 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

SAMPLE TPM-17



- 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

SAMPLE TPM-18

- Various products related to Trusted Platform Module (TPM)

- Intel : D865GRH Board
- Infineon : The Infineon TPM product (SLD 9630 TT 1.1)
- HP : Compaq nc8000
- Wave Systems : EMBASSY Trusted Client
- Atmel: Trusted Platform Module (AT97SC3201)
- American Megatrends, Inc. : AMIBIOS8

- Cygnacom : Security Evaluation Laboratory (SEL) : Security Testing and Evaluation

Drawbacks to the TPM

- The TPM, for all its' advances, still would be subject to power and timing analyses.
- The specification does not call for the use of lookup tables or other mechanisms to prevent these attacks

Summary

- Using the Common Criteria ISO 15408, we have a common dialog framework when discussing security evaluations of a variety of systems.
- Using the TCG's Trusted Platform Module specification, we can produce a uniform security framework across multiple operating systems

Summary

- Neither of these elements whether alone nor in combination is sufficient to assure a secure computing environment.
- These are merely tools to evaluate the strengths and weaknesses of various systems against a published standard.
- The new standards have good mechanisms for continued evolution as security needs change, but still only encompass part of an overall security strategy.