An Introduction to Trusted Platform Technology

Siani Pearson

Hewlett Packard Laboratories, UK

Siani_Pearson@hp.com

HP WORLD 2002 Conference & Expo

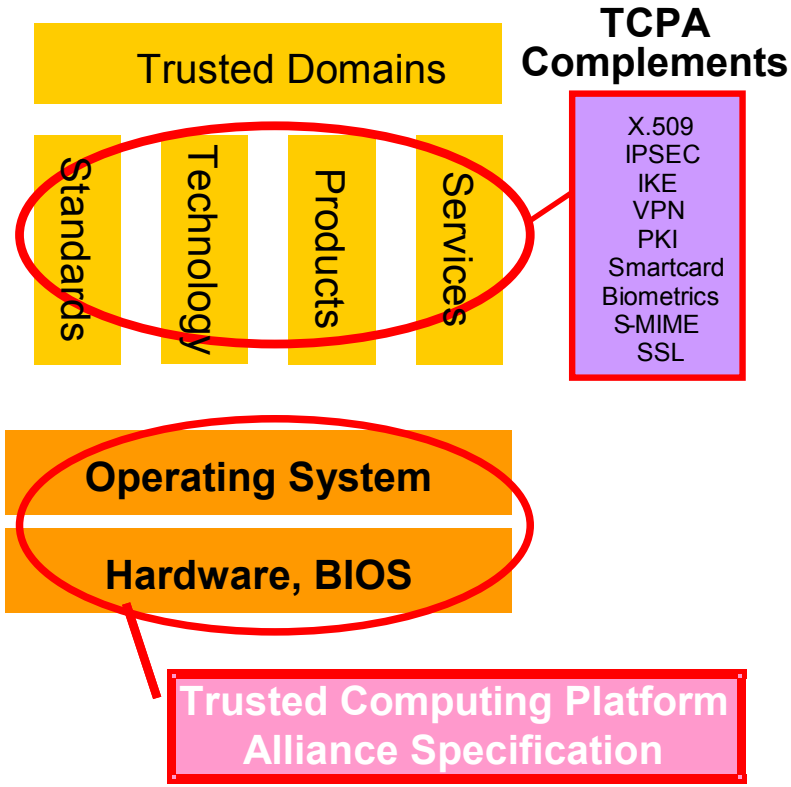
Content

- What is Trusted Platform technology and TCPA?
- Why is Trusted Platform technology being developed?
- What are the main concepts?
- Where can this technology be applied?
- How can I find out more?

TCPA: industry work group

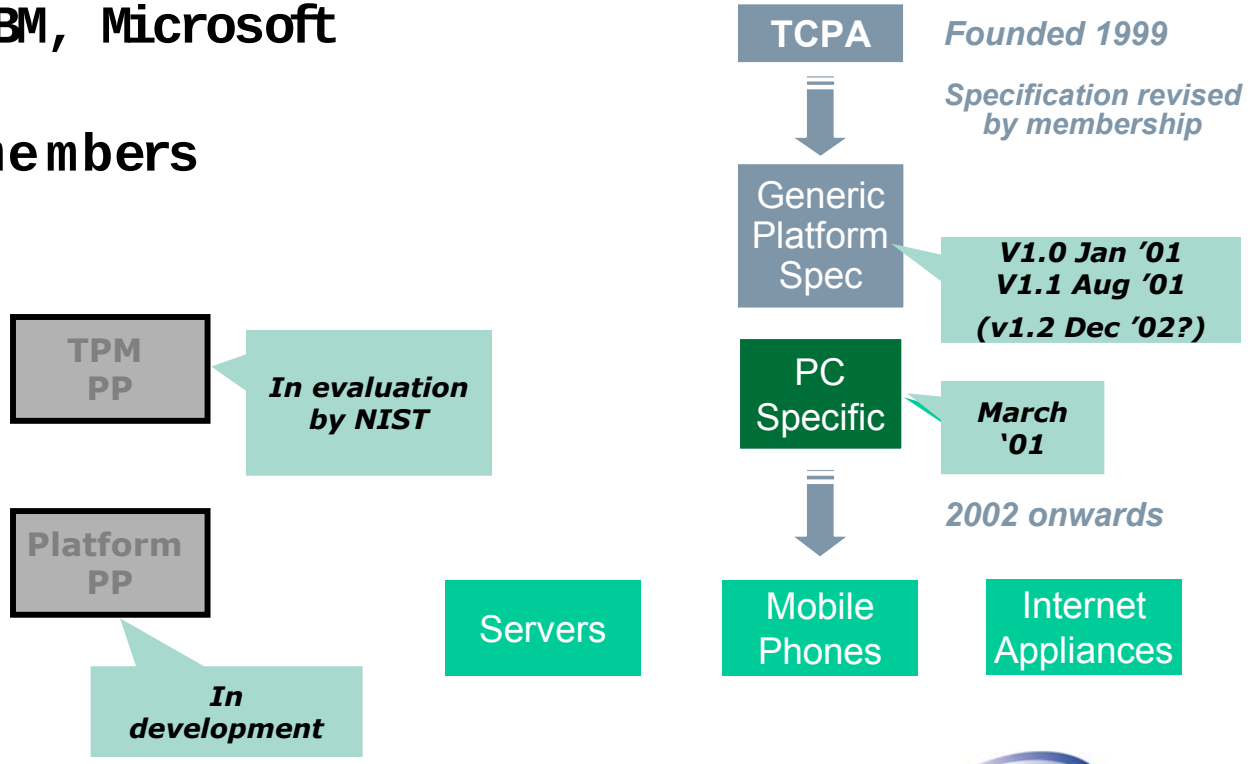
"Through the collaboration of platform, software and technology vendors, develop a specification that delivers an ***enhanced HW and OS based trusted computing platform*** that enhances customers' trusted domains."

- A platform can be trusted if it behaves in the expected manner for the intended purpose



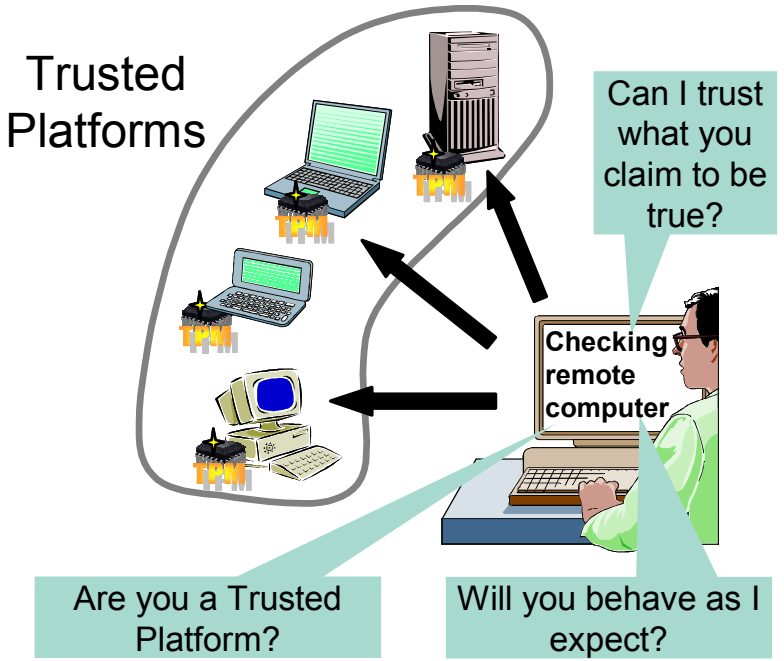
Evolution of TCPA

- **Original promoters: HP, Intel, IBM, Microsoft**
- **Over 150 members**



Why is TP technology being developed?

- Increased connectivity necessitates stronger trust and confidence in computer platforms
  - threats from Internet
  - in general, a third party knows nothing about environment and history of target platform
  - business-critical services
- Hardware integrity has been too expensive for mass market



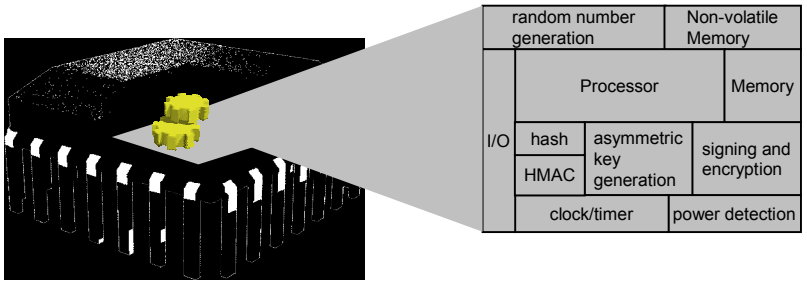
What are the main concepts?

- What TCPA provides
- Overview of Terminology
- Design features of TCPA platforms
- Roots of Trust
- Platform Identity
- Platform Integrity – Authenticated Boot
- Protected Storage

What TCPA provides

- ✓ **Evidence about the integrity of a platform to both the owner and arbitrary third parties**
- ✓ **Multiple pseudononymous identities**
- ✓ **Protected storage**
- ✓ **Cryptographic functions**
- ✓ **Cheap and standards based, therefore can be ubiquitous**
- ✓ **Important building blocks for distributed trust and trusted e-services**

How can I trust a remote system that is not under my control?



A fundamental change to the architecture of existing computers

The main mechanisms

- Trusted Platform technology provides mechanisms for:
  - Platform Identity
    - Identify the platform and its properties to a challenging party
  - Authenticated Boot
    - Reliably measure and report on the platform's integrity
  - Protected Storage
    - Protect integrity and identity information against subversion

Basic Definitions

- **Platform**

A computing device, usually one that communicates with other such devices

- **Trusted Computing Platform Alliance (TCPA)**

The organization that has specified how to produce Trusted Platforms

- **Trusted (Computing) Platform (TP)**

A platform that creates a foundation of trust for software processes

- **Trusted Platform Module (TPM)**

The hardware root of trust of a TP

- **Trusted Platform Subsystem**

A set of capabilities inside a platform that are defined by TCPA

- **Certification Authority (CA)**

Organization that vouches for an entity (e.g. for a cryptographic key, hardware or software component, platform or organization)

Overview of terminology

Trusted Platform Subsystem = (Trusted Platform Module + Core Root of Trust for Measurement + Trusted platform Support Service)

Design features of the TCPA Trusted Platform

- **Most cryptographic primitives** - but not bulk encryption
- **Privacy** - Fully "opt-in", with no identity correlation
- **No global secrets** - If a TPM is cracked, it reveals information relating to the associated platform and nothing further
- **Low cost protected environment outside a crypto coprocessor** - because it is uneconomic to do bulk processing in a coprocessor
- **Ubiquitous security** - at very low cost and without significant product export/import problems

Privacy

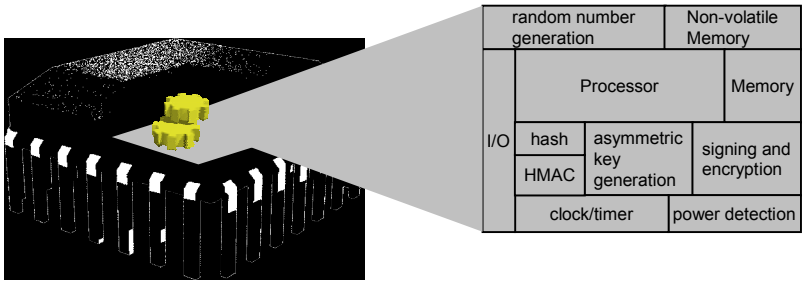
- Owner control over:
  - TPM activation
  - Generation of IDs
- Multiple pseudonymous IDs (limits correlation)
- User data kept private from everyone else – no superuser
- Can prevent the revelation of secrets unless the software state is in an approved state

Roots of trust (1)

- A root of Trust for Measurement:
  - First component of the boot process. Starts a chain of trusted measurements (Integrity Metrics) of the code executed during the boot process
- A root of Trust for Reporting:
  - Implements secure reporting mechanisms for securely stored Integrity Metrics

Roots of Trust (2): the TPM

- bound to computing platform
- records Integrity Metrics of the code executed during the boot process (BIOS, Option-Roms, OS Loader, OS…)
- More information logged to the TPM after boot process

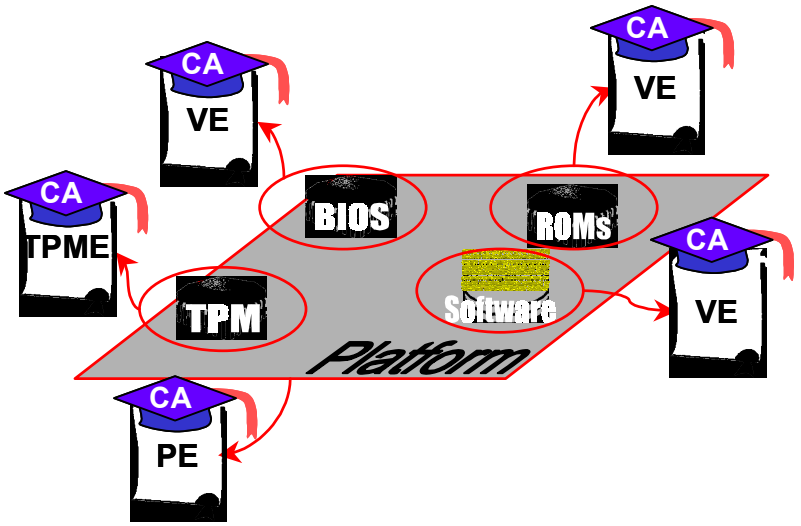


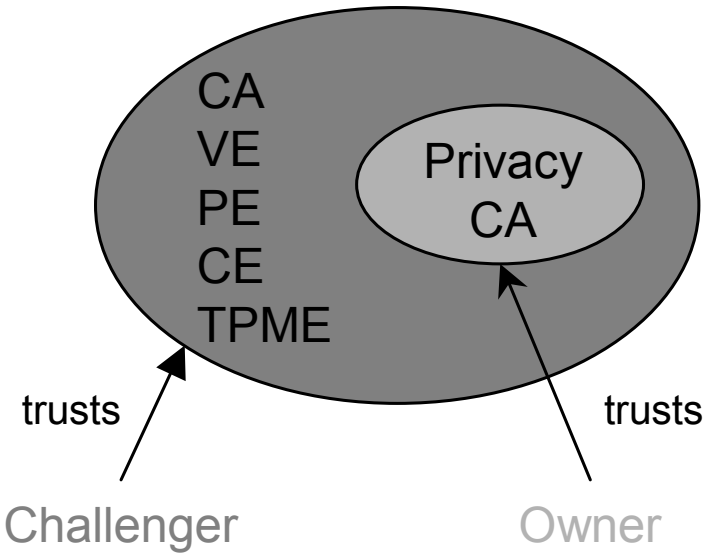
=> Report to a Challenger about software that has been executed on the platform

Roots of Trust (3): Attestation entities

- **Trusted Platform Module Entity (TPME)** vouches that the Trusted Platform Module (TPM) is genuine by attesting for the Endorsement key inside the TPM
- **Validation Entity (VE)** certifies the values of integrity measurements that are to be expected when a particular part of the platform is working properly
- **Conformance Entity (CE)** vouches that the design of the TCPA Subsystem in a class (type) of platform meets the requirements of the TCPA specification
- **Platform Entity (PE)** vouches for a platform containing a specific TPM
- **Privacy Certification Authority (Privacy-CA; P-CA)** attests that an ID belongs to a TP

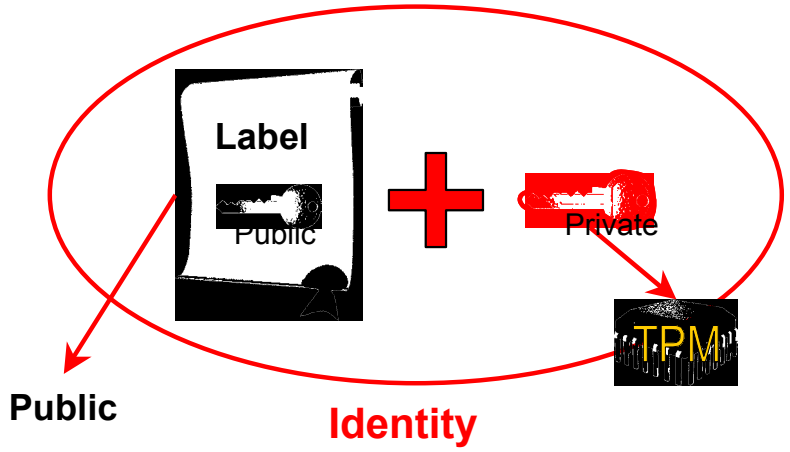
Roots of trust (4)



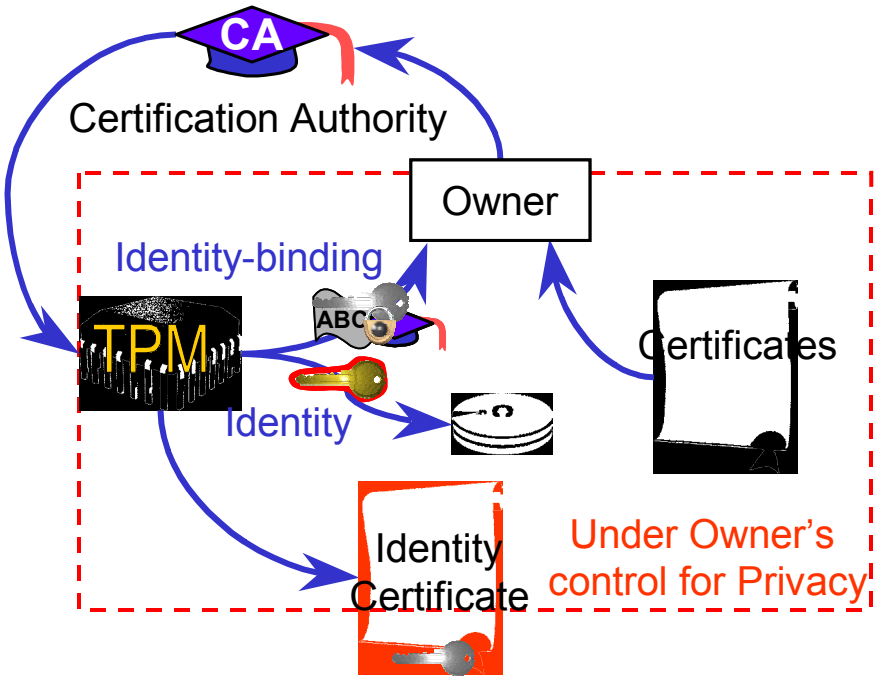


Trusted Platform Identity: Attestation

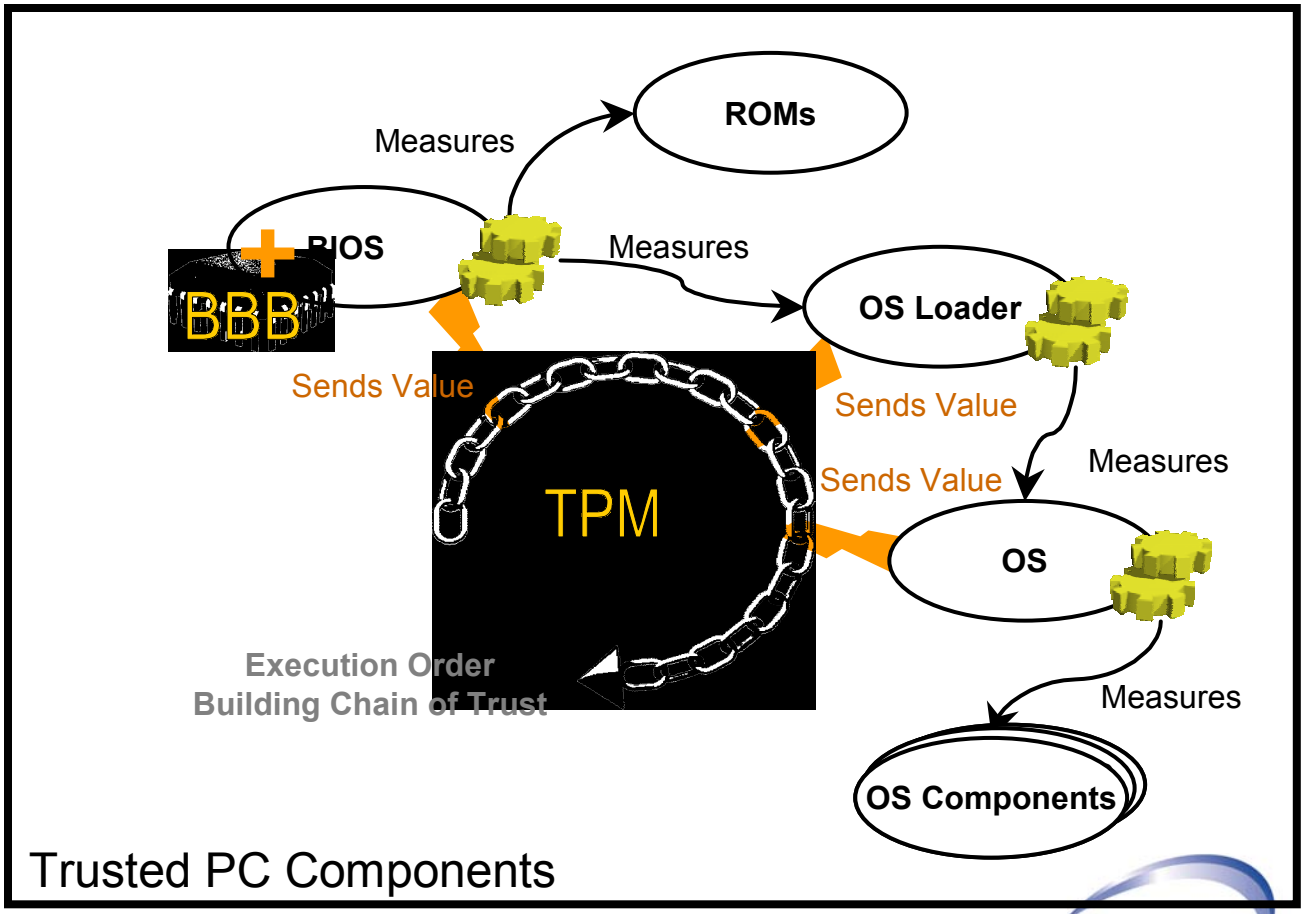
- A Trusted Platform can have multiple certified attestation Identities (TPM Ids)
  - A TPMId is certified by a Certification Authority (Privacy-CA, or CA) that vouches for the Trusted Platform implementation
  - A TPMId Certificate can be anonymous, it is a TPM identity, not a user identity
  - TPMIds are used to authenticate the platform as a genuine Trusted Platform, when reporting Integrity Metrics to a Challenger



Generating an identity



Platform Integrity Measurement: Authenticated Boot



Platform Integrity Reporting

- TPM reports on Integrity Metrics and signs them using a cryptographic identity: TPMId
- The reporting information will contain
  - Integrity Metrics: IM_1, IM_2, …, IM_N
  - Metrics Information: $Info_1$, $Info_2$, …, $Info_N$
  - $\Sigma_{TPMId}(IM_1)$, $\Sigma_{TPMId}(IM_2)$,…, $\Sigma_{TPMId}(IM_N)$
  - Certificate for TPMId by CA_{Id}: $Cert_{CA_{Id}}(TPMId)$
  - Certificates for Integrity Metrics

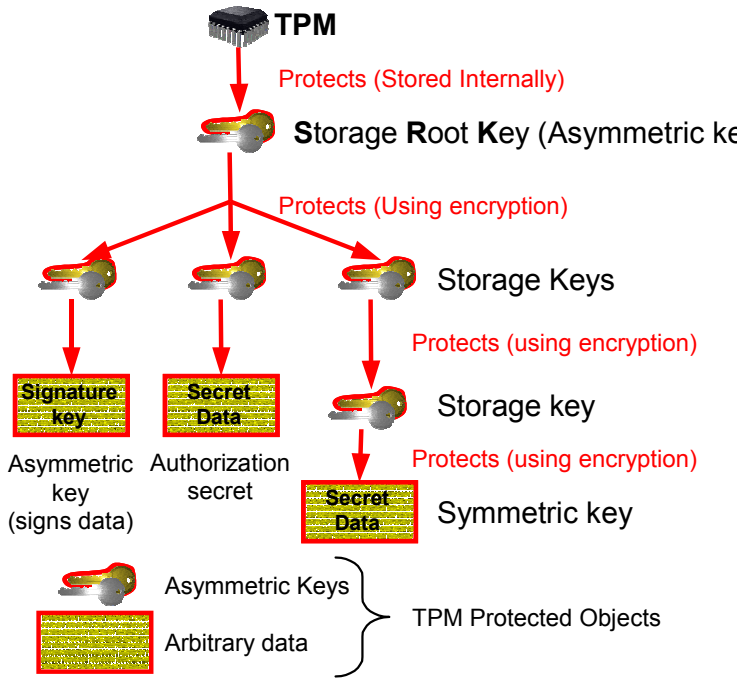
TO INTERPRET:

- Validate CA_{Id} and verify $Cert_{CA_{Id}}(TPMId)$
  - ➞ Trust in the Trusted Platform, based on CA_{Id} trust
- Verify signatures on Integrity Metrics
  - ➞ Trust in reported Integrity Metrics values
- Verify Integrity Metrics Certificates and compare certified metrics to reported metrics
  - ➞ Trust that these metrics correspond to certified software

BUT!!!

Protected Storage

- Data can be stored using the TPM, that can only be retrieved using this same TPM
- A specific software configuration can also be specified, that will be required for the TPM to allow this data to be retrieved
  - ➞ Sealing operation: parameters define which Integrity Metrics the data should be sealed to



Benefits

- TCPA brings new functionality to the client platform (PC, mobile, PDA). The potential of TCPA will be released in phases, because some features require more supporting software and infrastructure than others.

Short term TCPA benefits – protected storage

(Platform with a TPM, associated software provided by the TPM manufacturer)

Customers can encrypt the data on their hard disks in a way that is much more secure than software solutions.

- **The TCPA chip is a portal to encrypted data.**
- **Encrypted data can then only ever be decrypted on the same platform that encrypted it.**
- **TCPA also provides for digital signature keys to be protected and used by the embedded hardware chip**

Middle term TCPA benefits – integrity checking

(Short term solution plus additional software)

Protection against hackers, by automatically preventing access to data if unauthorised programs are executed.

- **TCPA provides for the measurement of integrity metrics of the software environment on the TCPA platform.**
- **Allows for a remote party to verify what the software environment on a TCPA platform is.**
- **The TCPA chip can then be used to encrypt data to disk so that this data can only ever be decrypted on that same platform, and ONLY if the platform has a given set of software environment integrity metrics.**

Long term TCPA benefits – e-commerce

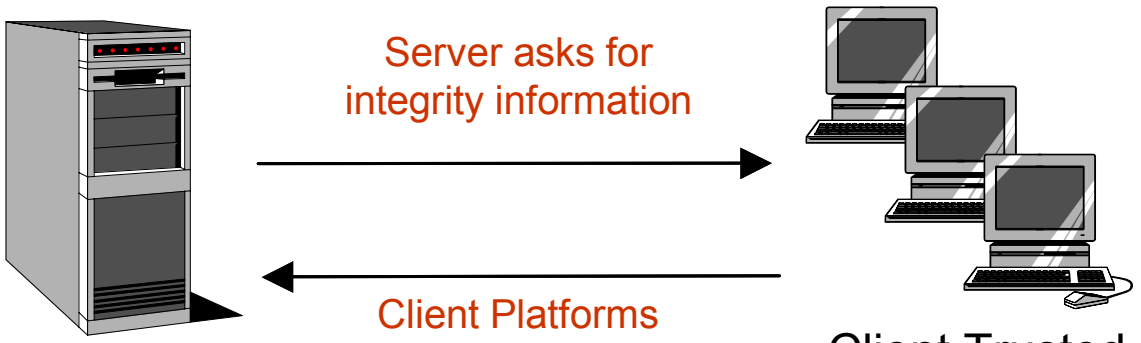
Customers and their partners/suppliers/customers can connect their IT systems and expose only the data that is intended to be exposed.

- **TCPA is designed so that platform identities and Integrity Metrics can be proven reliably to previously unknown parties.**
- **Secure online discovery of platforms and services: confidence in the information about the software environment and identity of a remote party, enabling higher levels of trust when interacting with this party.**

Where can this technology be applied?

- Existing applications benefit from enhanced security
- Encourages the development of new services that require higher security levels
- e.g. electronic cash, email, hot-desking, platform management, single sign-on, VPN, web access, etc.
- We will consider 3 examples.

Scenario One

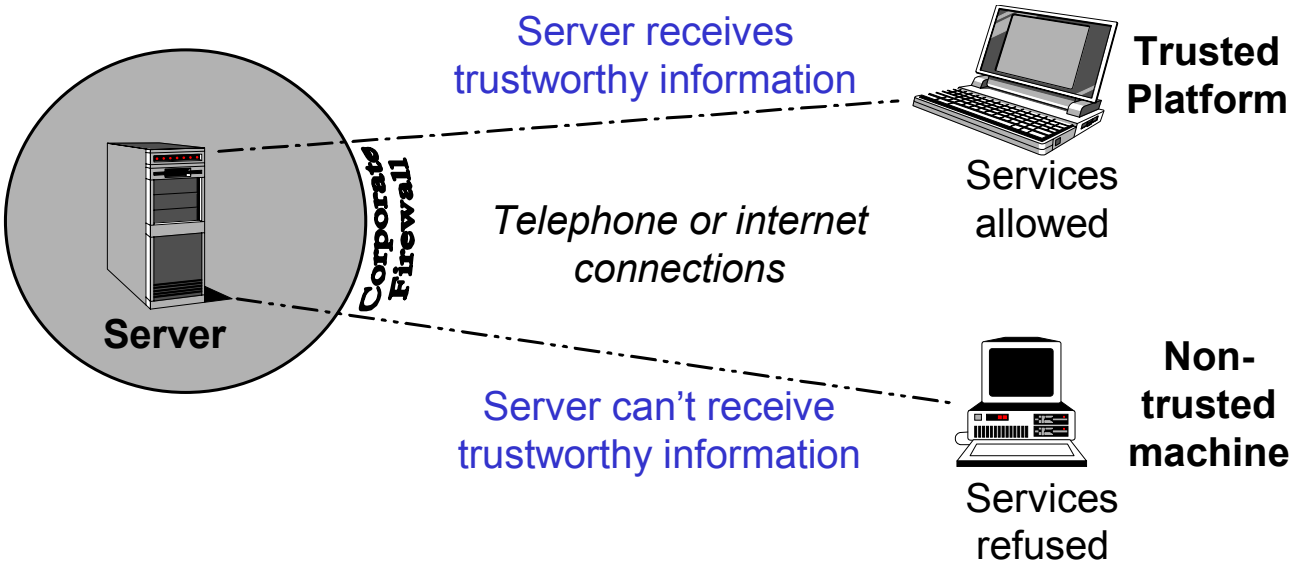


Server

Checks that unauthorized modifications have not been made to the client platforms

Client Trusted Platforms

Scenario Two



Scenario Three

Further Information

- TCPA specification v1.1 is publicly available, and is already implemented in at least three hardware products (Atmel, Infineon, NationalSemi).
- www.trustedcomputing.org