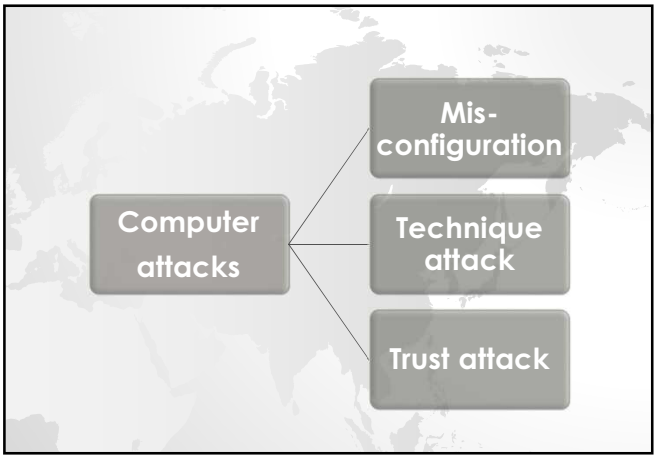
TRUSTED COMPUTING

Hardware-supported security



"TRUST" ?

TRUST

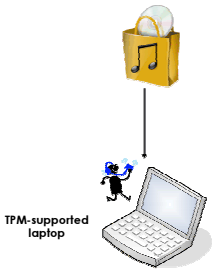
In Trust Computing

Trust is the expectation that a device will behave in a particular manner for a specific purpose.

DRM **DIGITAL RIGHT MANAGEMENT**

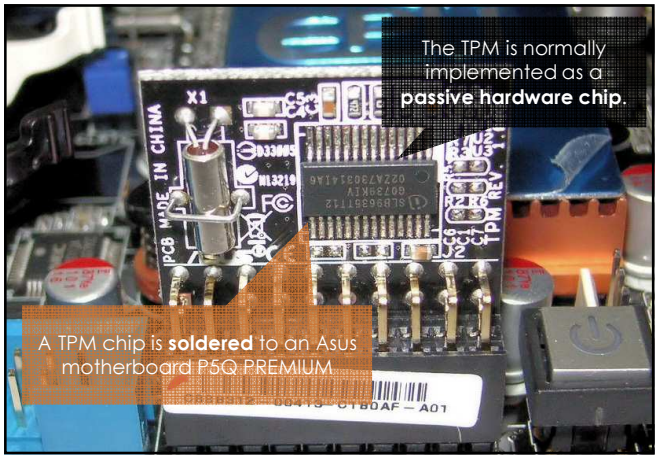
Software-supported DRM

DRM DIGITAL RIGHT MANAGEMENT

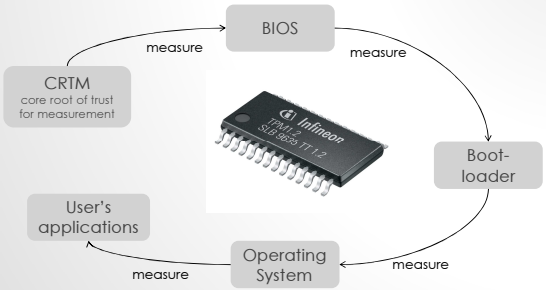


Hardware-supported DRM

Explain
the **Trusted Computing**

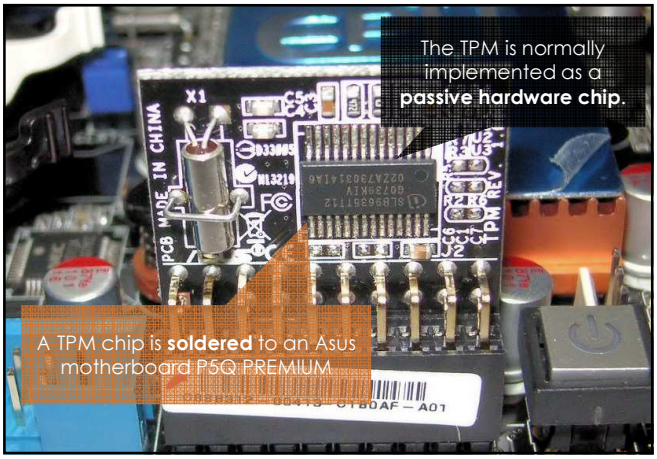


CHAIN OF TRUST

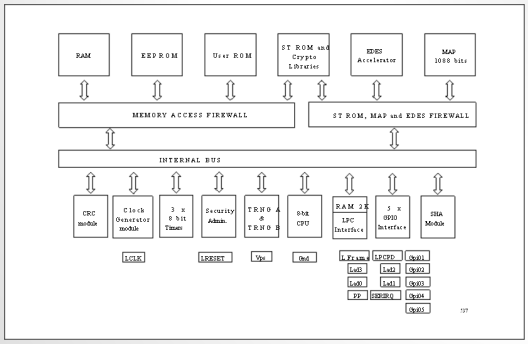


ROOT OF TRUST

- Trusted Platforms need components that act as a Root of Trust (e.g. CRTM) that must work properly. TCG defines three kinds of Roots of Trust:
  - **Root of Trust for Measurement (RTM/CRTM):**
    - **度量值保存，链式启动过程**
  - **Root of Trust for Storage (RTS):**
    - **密钥生成和管理**
  - Root of Trust for Reporting (RTR):
    - 验证流程管理

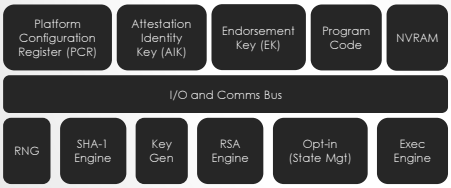


ST19NP18-TPM BLOCK DIAGRAM

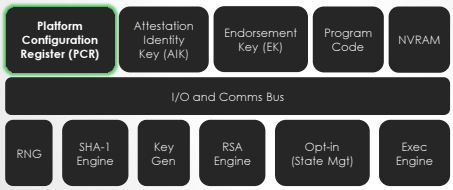


TMP chip manufacturers

INSIDE A TPM CHIP



INSIDE A TPM CHIP

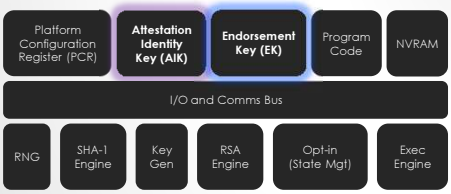


integrity measurements

Renew the PCR value:

$PCR_{new}=SHA1(PCR_{old} || \ measured\ data)$

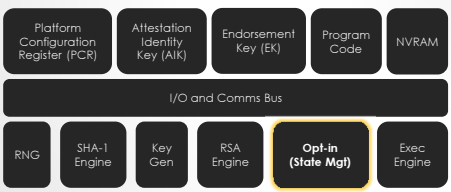
INSIDE A TPM CHIP



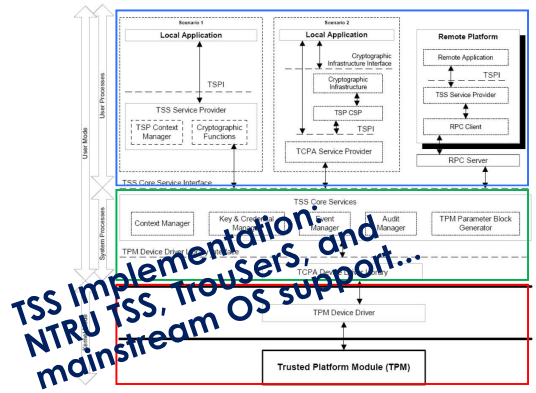
Attestation Identity Key (AIK) is used for signing **PCR** values.

Endorsement Key (EK is a RSA key pair normally generated and put inside the TPM by its manufacturer.

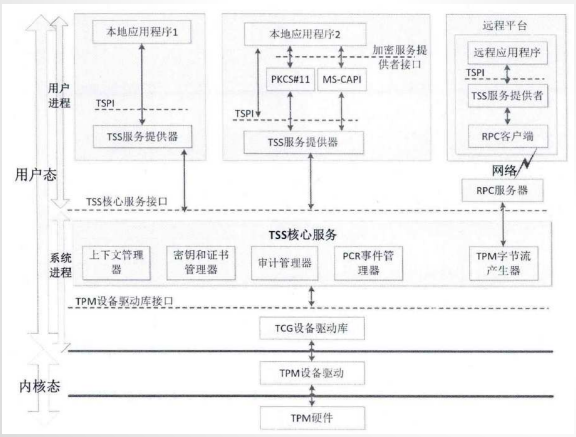
INSIDE A TPM CHIP

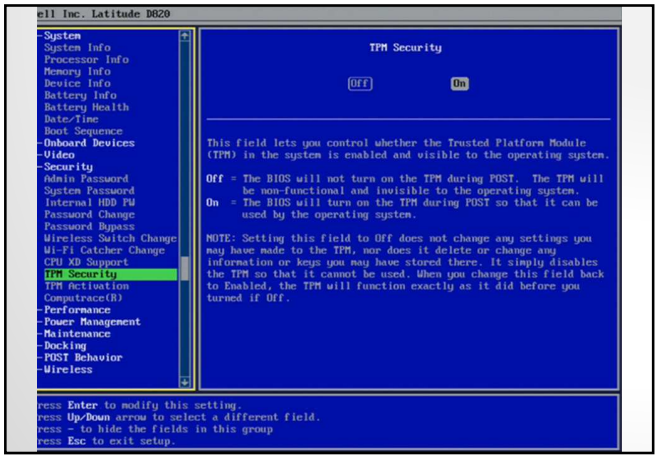


TRUSTED SOFTWARE STACK



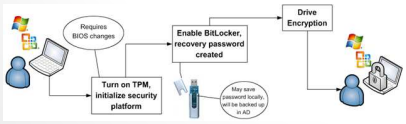
TSS Implementation, NTRU TSS, TrouSerS, and mainstream OS support…





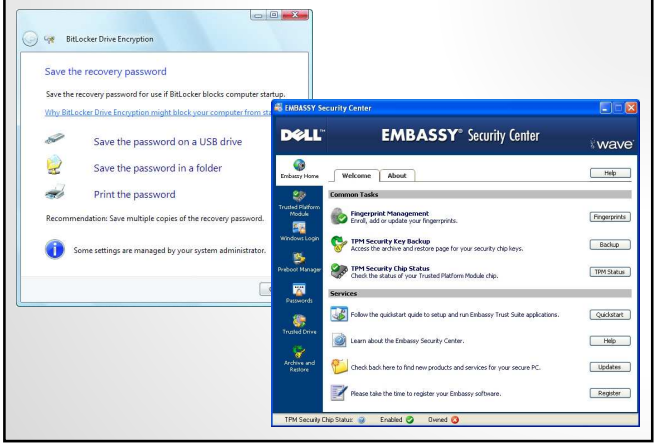
4 STEPS TO ENABLE AND USE THE TPM

1. Turn on the TPM from the BIOS
2. Load available TPM utility software.
3. Enable the TPM and take ownership.
4. Use the TPM to generate Keys for a specific need, such as encrypting hard drive disks



TPM-COMPLIANT PRODUCTS

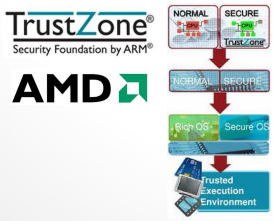
- PC manufacturers supporters
  - HP, Dell, Lenovo, Fujitsu ltd.
- Commercial software product
  - EMBASSY® Trust Suite (Wave)
  - Bitlocker (Microsoft)
  - PGP Whole Disk Encryption
  - CompuSec FDE
  - Securstar DriveCrypt Plus Pack



SIMILAR TECHNOLOGIES

Lenovo恒智® security chip (2005)

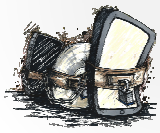
ARM TrustZone®



TCG: TRUSTED COMPUTING GROUP

- Infrastructure
- TCG Software Stack
- Storage
- Trusted Multitenant
- Mobile Platform
- Virtualized Platform
- Embedded System
- Trusted Network Connect
- Trusted Platform Module
- PC Client
- Server Specific

CONTROVERSIES



- Academia vs. Industry
- DRM
- Users unable to modify software
- Loss of anonymity
- Shutting out of competing products
- Trust on the Chip
  - Infineon TPM chip has been successfully reverse-engineered (Feb. 2010)

TRUSTZONE