DevID relationship to TPM

Mike Borza

mborza@ellipticsemi.com

November 2004

Recall: Objectives for DevID

- Provide strong means to identify and authenticate the identity of “devices” in a network (esp. LAN)
  - including during initial provisioning
    - possibly remotely
- Identity is permanently bound to device
- Each identity is unique
- Centralized infrastructure not required for DevID to be usable

Are TPM and DevID Equivalent?

- Necessity
  - Does TPM satisfy “requirements” of DevID?
- Sufficiency
  - Does TPM satisfy all requirements of DevID?
- Efficiency
  - Is TPM a minimal implementation of DevID?

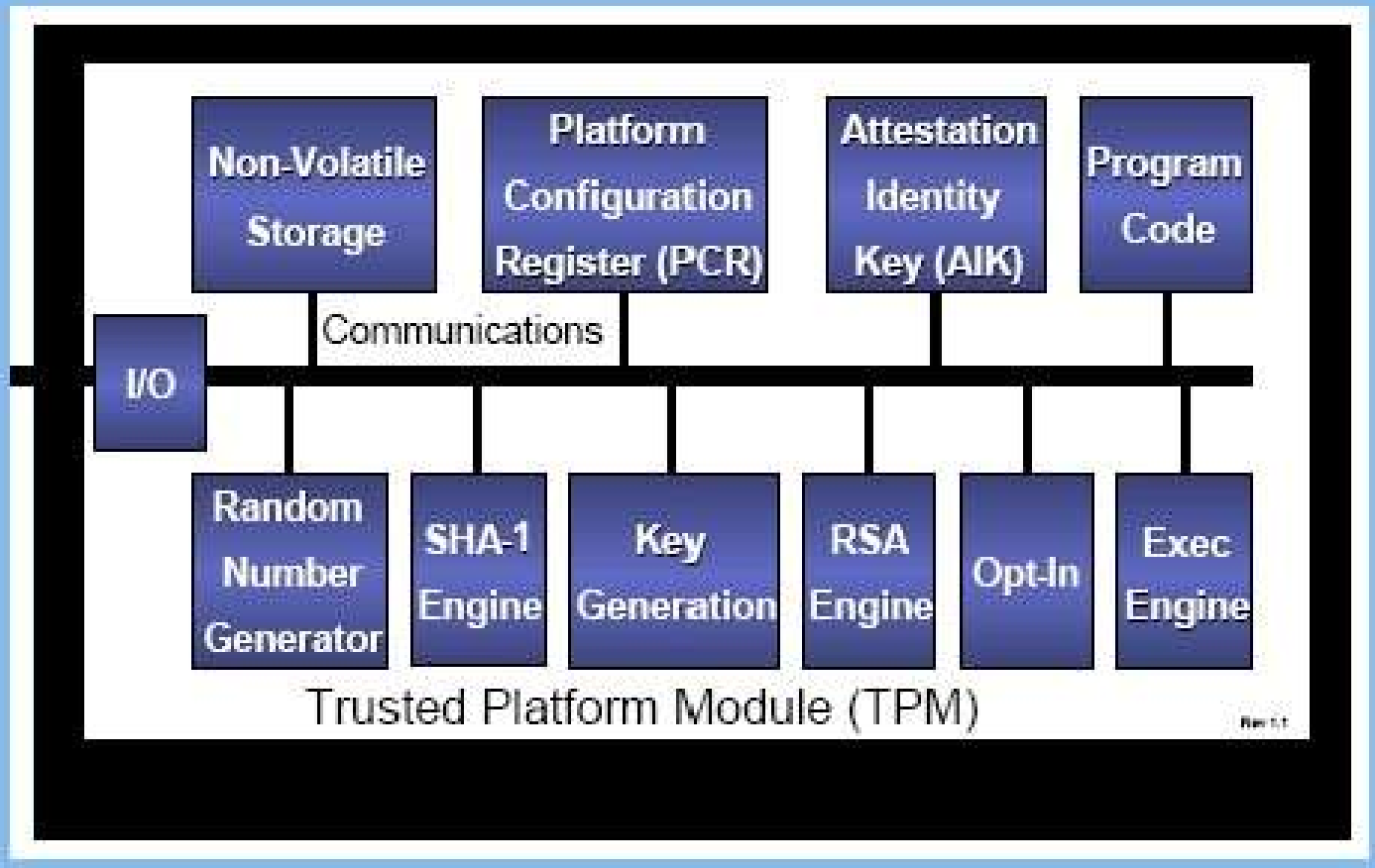
What is TPM?

- Trusted Platform Module
- Secure identity & key storage
- Cryptographic primitives
  - RSA, SHA-1, random numbers (no symmetric crypto)
  - “low” performance to avoid export restrictions
- Operational validity assurance
- Standard client interface functions

Who Specifies TPM?

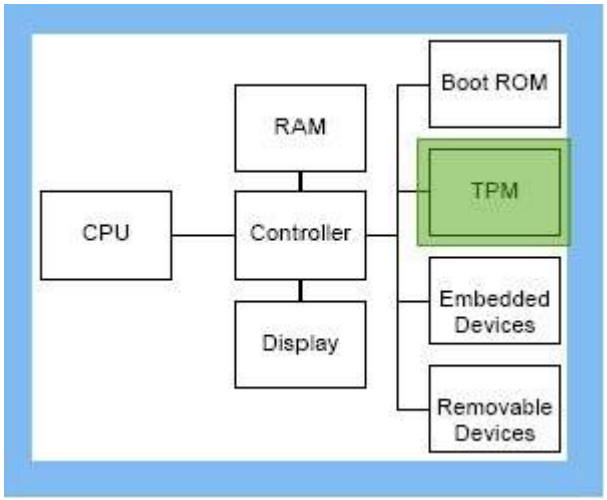
- Creation of Trusted Computing Group (TCG) – formerly TCPA)
  - ad hoc standard body to develop inter-operable secure identity capability for computing and networking platforms
- spearheaded by Intel, Microsoft, Sony, Hewlett-Packard, IBM, Sun, AMD
- applications to computer & network access control, asset management, DRM, ...

TPM physical Architecture



Typical System Architecture

- TPM is incorporated in a larger system
  - may be a separate subsystem, IC device, or embedded IP module
    - maybe even a network-attached peripheral or server?
  - includes functional components & private storage

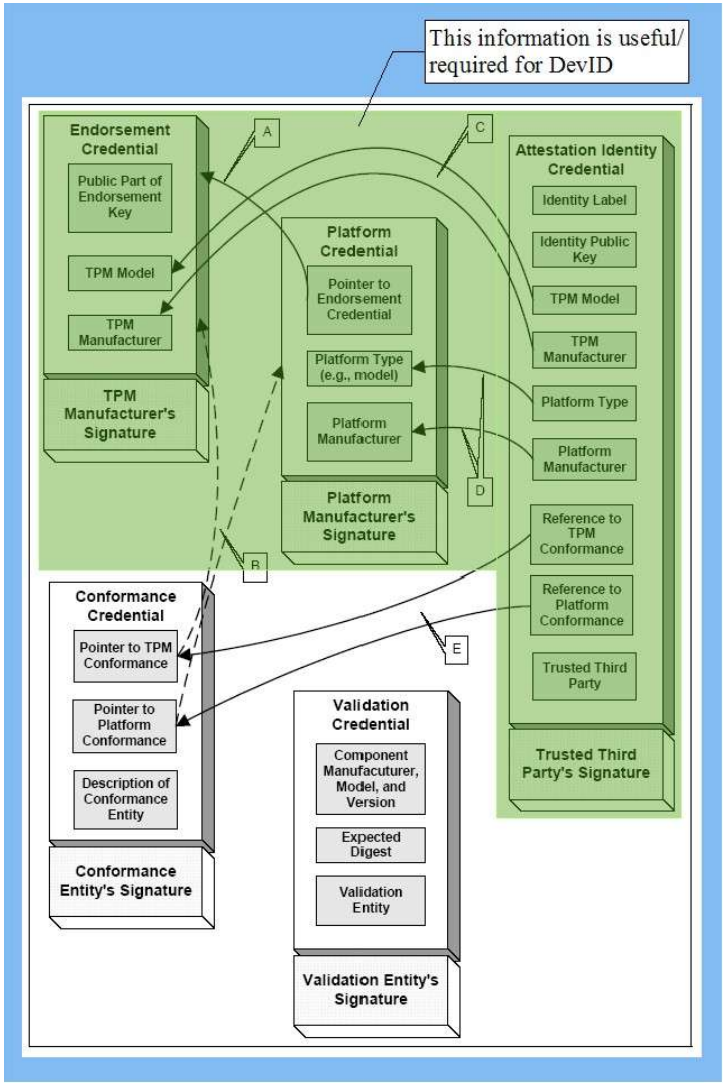


TPM PC Architecture

TPM Identity Credentials

- Endorsement Credential (Endorsement Key EK)
  - unique per TPM, generated in manufacturing
- Platform Credential
  - incorporates the EK public key, making it a unique identifier of the platform
- Identity Credential (Attestation Identity Key AIK)
  - signed by a CA, which distributes it anonymously
    - used to provide anonymous “attestation”

Relationships between Identity-Establishing Components



- Endorsement Credential
  - TPM manufacturer, model, revision
  - EK – unique per TPM
- Platform Credential
  - platform mfr, model, version
  - endorsement & conformance credentials
- AI Credential
  - privacy insensitive parts of EC, PC
  - TTP (trusted third party) signature

Some possible approaches to DevID with TPM

- Use the Platform Credential as a DevID
  - contains extra information not needed, but not necessarily prohibited
- Derive a DevID from the PC
- Derive a new credential unique to DevID, unrelated to the PC except by platform association
  - presumably stored as a protected BLOB outside the TPM

Necessity

- TPM provides the necessary components to implement DevID
  - strong asymmetric crypto
  - secure hashing
  - integrated secure storage
  - the PKI components necessary to implement AIK functionality (anonymous attestation) not needed ==> no central mgmt entity needed

Sufficiency

- The Platform Credential by itself meets the needs of DevID
  - EK public key is unique to at least the manufacturer (probably globally)
  - Manufacturer, Model and Revision are all included in the PC
  - Privacy Note: the PC is considered a possible privacy concern since it uniquely identifies the platform
    - for DevID, that's the point!

Efficiency

- TPM includes features well beyond what's required to meet the minimum requirements of DevID
- TPM in gates will be larger than desirable for the bottom tier of devices
- A full (compliant) TPM implementation presupposes the existence of a PKI with both distributed certificate authorities and a trusted third party to distribute and/or authenticate AIKs

Summary

- TPM can provide an implementation of DevID
- TPM provides more than DevID is likely to need
  - a class of devices will use this extra capability
  - a class of devices can't afford it
- DevID explicitly does not need the PKI capabilities that TPM implicitly requires