Trusted Platform Module: Impact to Manufacturing & Testing

Zorba Manolopoulos
Senior Design Engineer
Intel Corporation
September 18, 2003

Safer Computing Track – Fall IDF

Tuesday

- LT Overview
  SCMS-16
- TCG & TPM v1.2
  SCMS-17
- LT Architecture
  SCMS-18
- Tech Showcase
  Every Day
  Birds of a Feather Lunches
  Tuesday & Wednesday

Wednesday

- Privacy Method for Assuring Trust
  SCMS-19
- Opt-In Strategy
  SCMS-156
- Trusted Mobile KB Controller
  SCMS-24
- Software for LT
  SCMS-20
- Fundamentals of NGSCB
  SCMS-21
- Migrating Apps to NGSCB
  SCMS-22

Thursday

- If TPMs Go Bad
  SCMS-25
- TCG Credentials
  SCMS-157
- TPM Mfg & Testing
  SCMS-180

= Overview
= Medium Technical
= Highly Technical

Agenda

- Package Type and Pin out
- TPM Delivery
- In Circuit Test
- Functional Test
- Maintenance
- Managing Credentials
- Manufacturing Security
- Returns and Repairs

Manufacturing

Package Type and Pin out

- TPM 1.1 Package
  - different package per vendor
- TPM 1.2 Package
  - Common Footprint and Pin out for 1.2 TPM
  - 28 pin TSSOP -
  - 1 board, any TPM

TPM Delivery

- With or Without Endorsement Keys (EK)
  - Differs between TPM vendors
  - Pre-Generated EKs are stored in the silicon
  - EKs are set only once
- Endorsement Key
  - Single, Permanent Public/Private key pair (Controlled uniqueness)
  - The Endorsement Key is used in the Endorsement Credential (establish trust)
  - Only used by Owner-selected agents to obtain Attestation Identity Keys (AIK)

TPM Delivery (cont)

- Activated or Deactivated

In Circuit Test (ICT)

- 1.1 TPMs currently do not support XOR, Boundary Scan
  - No method to logically remove TPM from motherboard
- Working with TPM vendors to implement for TPM 1.2

Functional Test

- **Functional Testing only**
  - **This is not security testing**
  - **Test basic functions and operation of the TPM**
- **Activation and Deactivation**
  - **TPMs are delivered from TPM Vendor deactivated**
  - **Addd activation info**

Maintenance Key

- Platform Manufacturer owns Maintenance procedure because they own the Maintenance Key
- Key is programmed during manufacturing
  - Key can be same for all platforms, or unique per model
- Key is used to encrypt the Maintenance blob out of TPM and load into another TPM
- If TPM is enabled for Maintenance, must populate with Zero to disable Maintenance

What is Maintenance

- Maintenance is the event of moving the Storage Root Key from one TPM to another TPM
  - SRKs are not meant to be moved
- TCG Specification allows for Platform Manufacturer to move SRK
- Maintenance is an optional feature
  - TPM Manufacturer owns the method
  - Platform Manufacturer owns procedure
  - Not performed on the manufacturing line

Situations for Maintenance

- Maintenance is moving non-migratable keys, whereas Backup and Migration are moving migratable keys
- Moving from one platform to another of the same type
- Not used for moving keys if upgrading

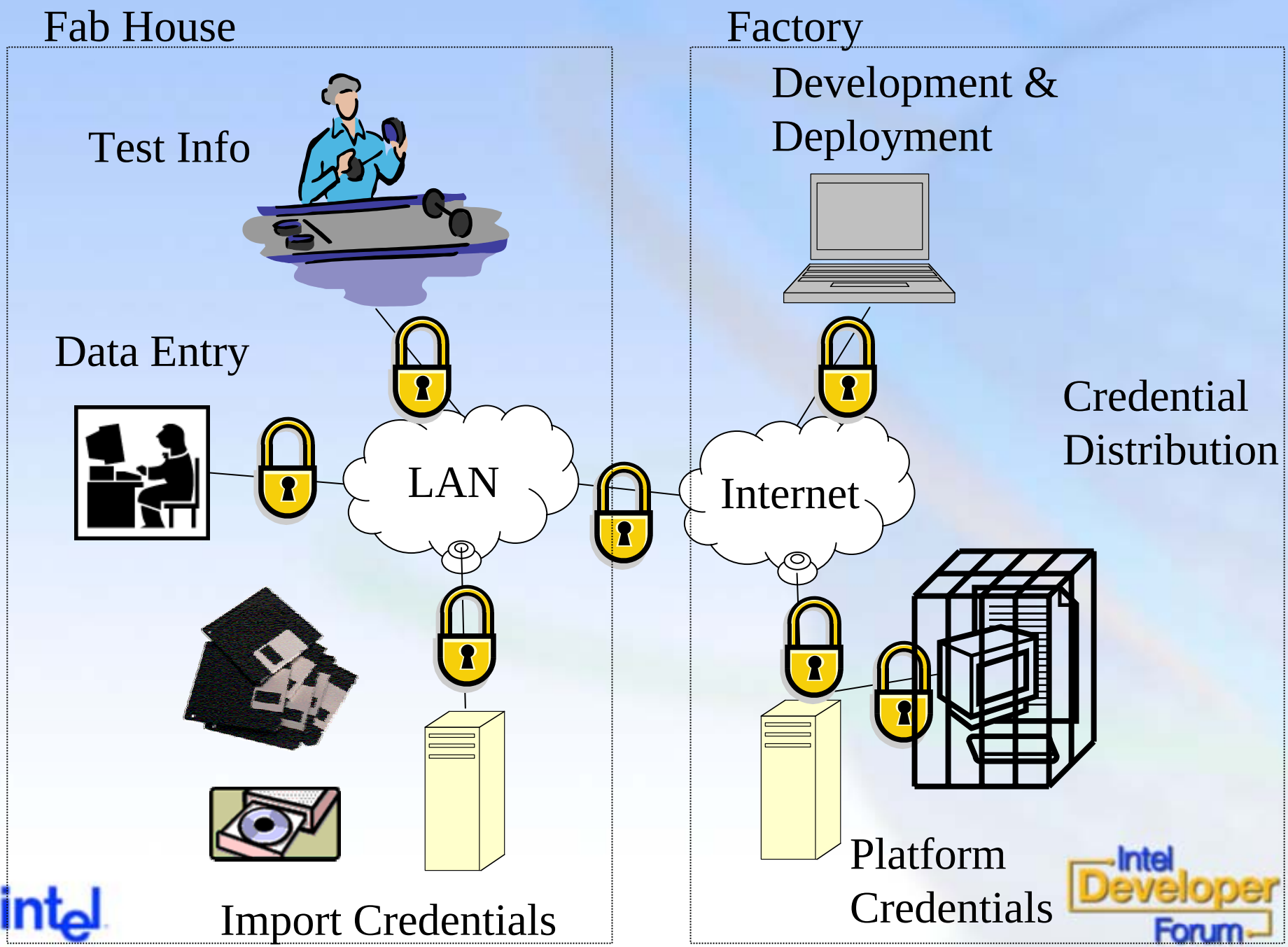
- Multiple Platform OEMs = Multiple Keys

Managing Credentials

- Credentials
  - Managing the EK and Credential
  - Managing Platform Credentials
- Credential Delivery and Distribution
  - On CD/Floppy/board, On Web, On Chip?
- Do you customers need TPM Credential?
- Do your customers need your Credentials?
- Rebranding Credentials
  - Protecting the Process

Manufacturing Security

- Physical, System, Process Security
- Do you create Credentials
  - Endorsement or Platform
- Where are your data input points
- Where do you create credentials
- Who has access to the system?
  - To the data entry
  - To the credential creation


Fab House
Factory
Development &
Deployment
Test Info
Data Entry
LAN
Internet
Credential
Distribution
Import Credentials
Platform
Credentials
intel
Intel
Developer
Forum

Support and Repair

Returns and Repairs

TPM	*Motherboard* Good	Failed
Good	If the motherboard is repaired and the TPM still works, the TPM owner can be cleared and reused	If the motherboard is not repaired but the TPM still works, the TPM is bound to that motherboard and cannot be removed and placed on to another motherboard. Even if the Owner is cleared. The TPM must be destroyed.
Failed	If the motherboard works and the TPM has failed, the TPM can be removed (and destroyed) and a brand new TPM (never before on another motherboard) can be put on the motherboard	If the motherboard isn't repaired and the TPM failed, then the platform isn't usable.

- **In no way can an already used TPM be used on any other motherboard other than that of the original.**

Maintenance issues

- How many platforms can the SRK be transferred to?
  - Must have process to ensure only 1 platform
- What happens to the old platform?
  - Should be physically destroyed to prevent further moving of keys
- What if maintenance fails?
  - Do not destroy original TPM until transfer is confirmed
- Failure Assessment
- Support and Procedures

Summary

- Functional Testing not Security Testing
- Credential/EK Management
- Maintenance Key and Support
- Build up Manufacturing Security

Questions

Thank you for attending.

Please fill out the Session Evaluation Form.