Recovering from Computer Failures, if TPMs Go Bad

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

intel

Intel Developer Forum

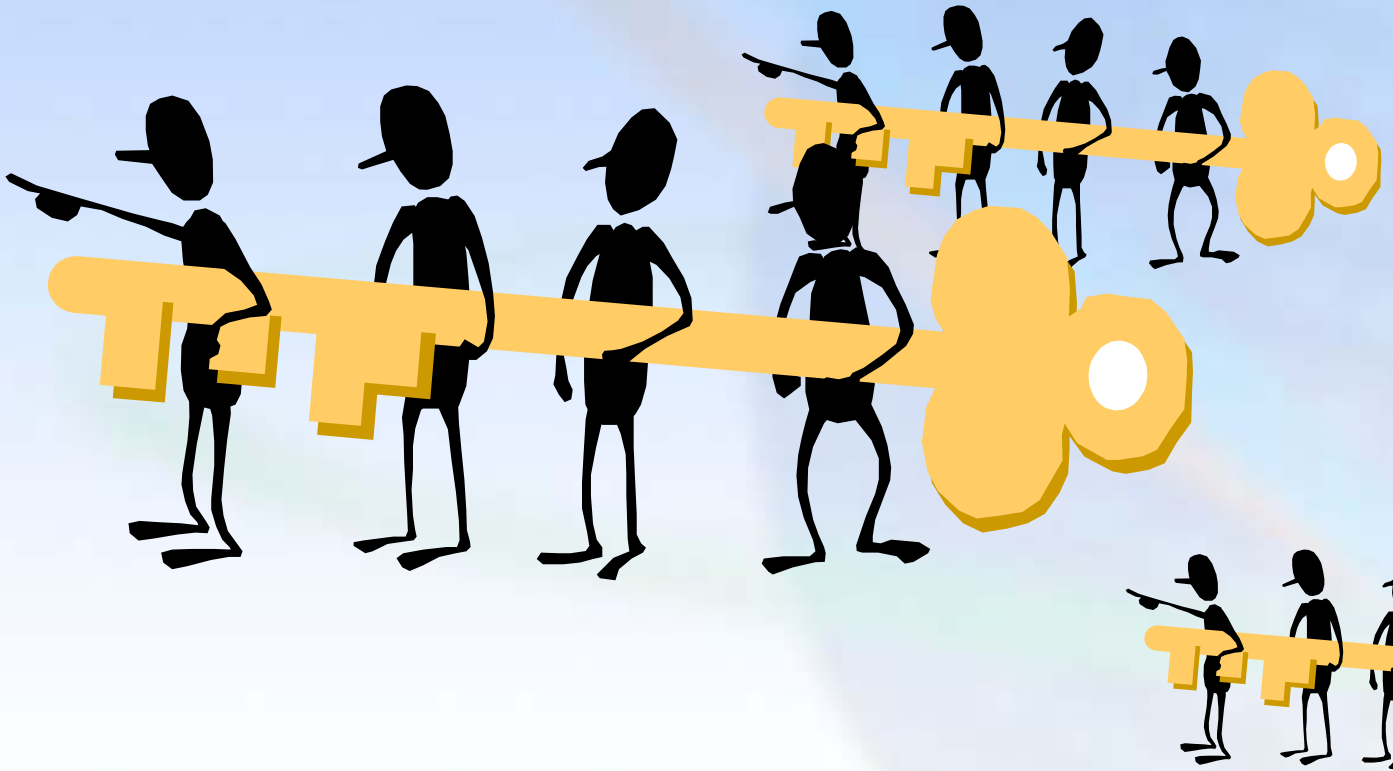
Agenda

- Situations for Recovery
- Solutions
- Backup
- Migration
- Maintenance
- Review

How things go wrong

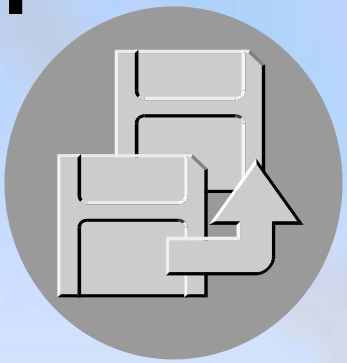
- Regular Issues
  - Loss of data files
  - Hard Drive Failure
  - Motherboard Failure
  - System Failure
  - Computer Theft
  - Loss of keys
  - Loss of password
- TPM Related Issues
  - TPM Failure
  - Loss of keys
  - Loss of password

Solution - Replicate the Keys

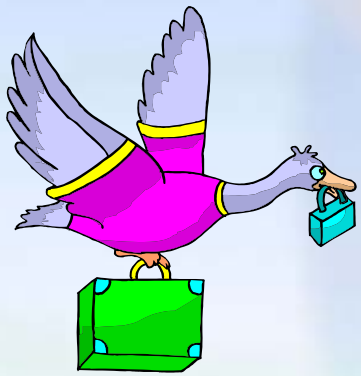


Methods of Replication

- Backup

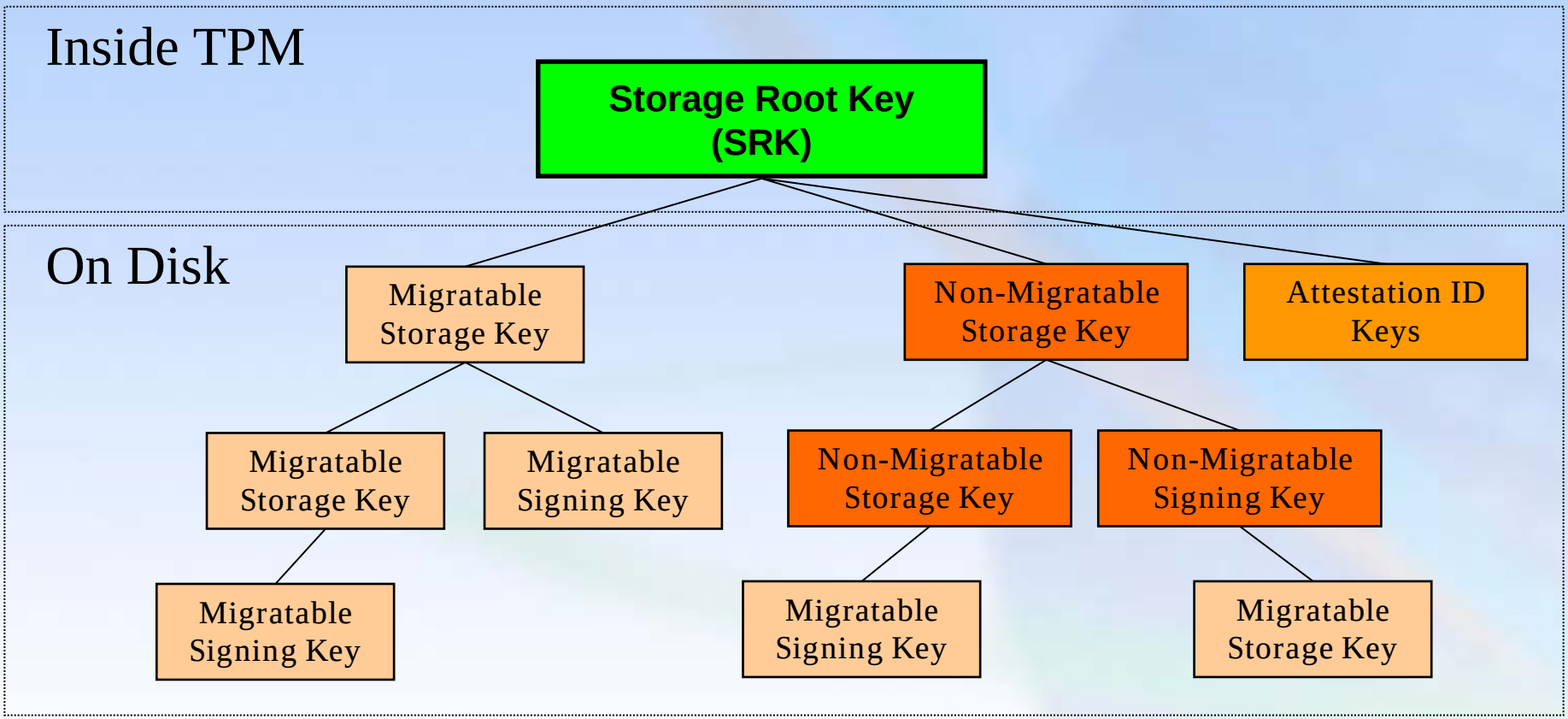


- Migration

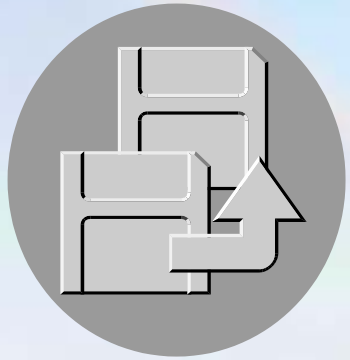


- Maintenance

Key Hierarchy

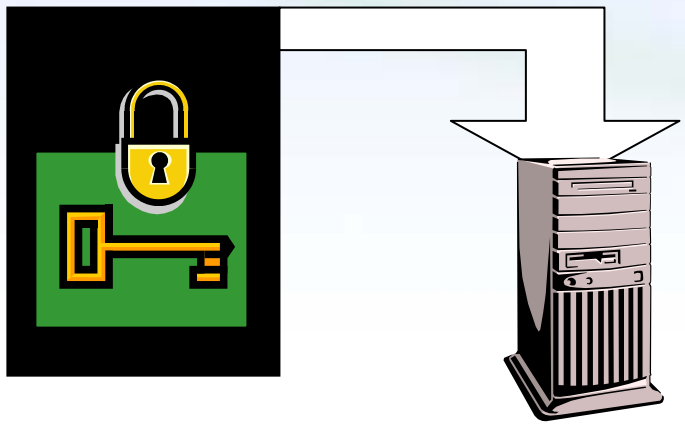


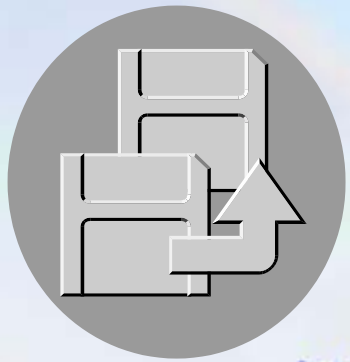
Backup



Key Backup

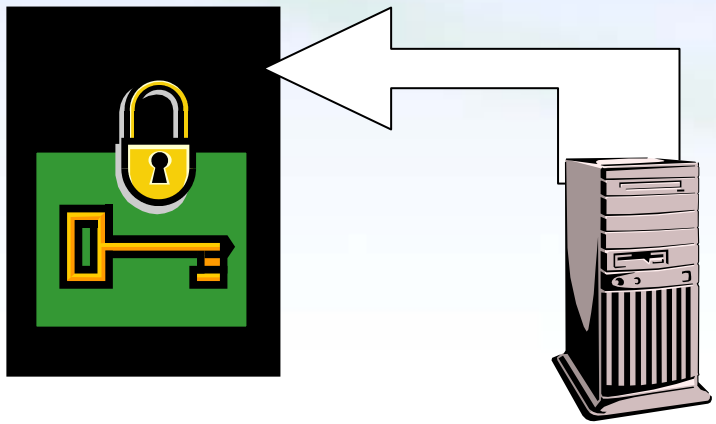
- Simply creating duplicates of data files
- Create copies of protected key blobs
  - Key blobs are stored on hard drive
- Backup utilities must make sure that all keys are currently available on hard drive when backups are made.

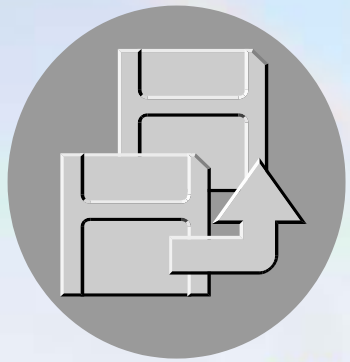




Restoring the Keys

- To restore the keys (or data files even)
- Move the backed-up files to the proper place on the harddrive.
  - The TPM will recognize the same key blobs as if they were the original





Key Hierarchy

Inside TPM

Backup and restore to the same TPM

Migration

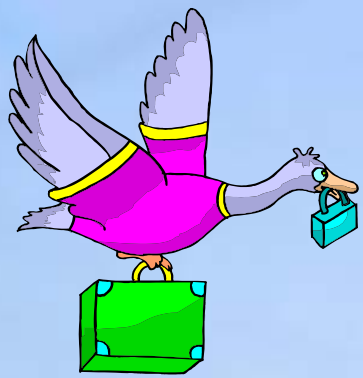
What is Migration

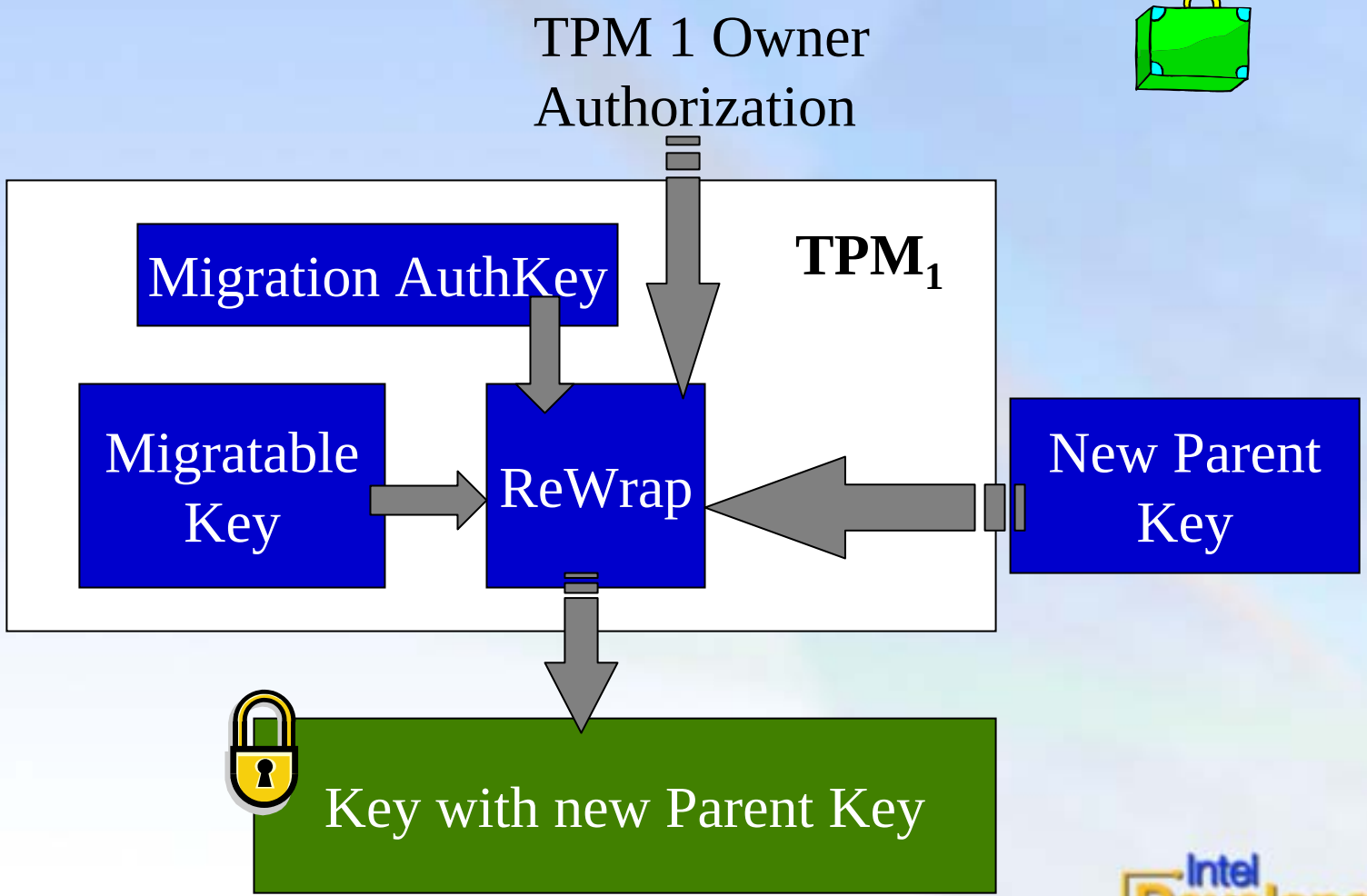
- Moving keys from one TPM to another
  - Only Migratable keys
- Required feature for all TPMs

Situations for Migration

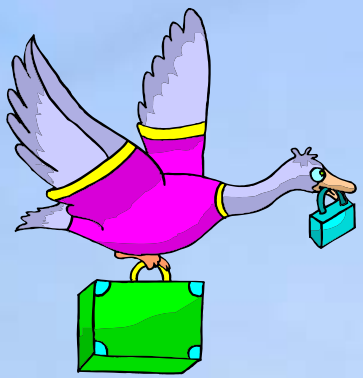
- Allows sharing the same key across multiple platforms
- Allows transferring keys to new computer
  - upgrading of users machine
- Easily move encrypted files to another machine

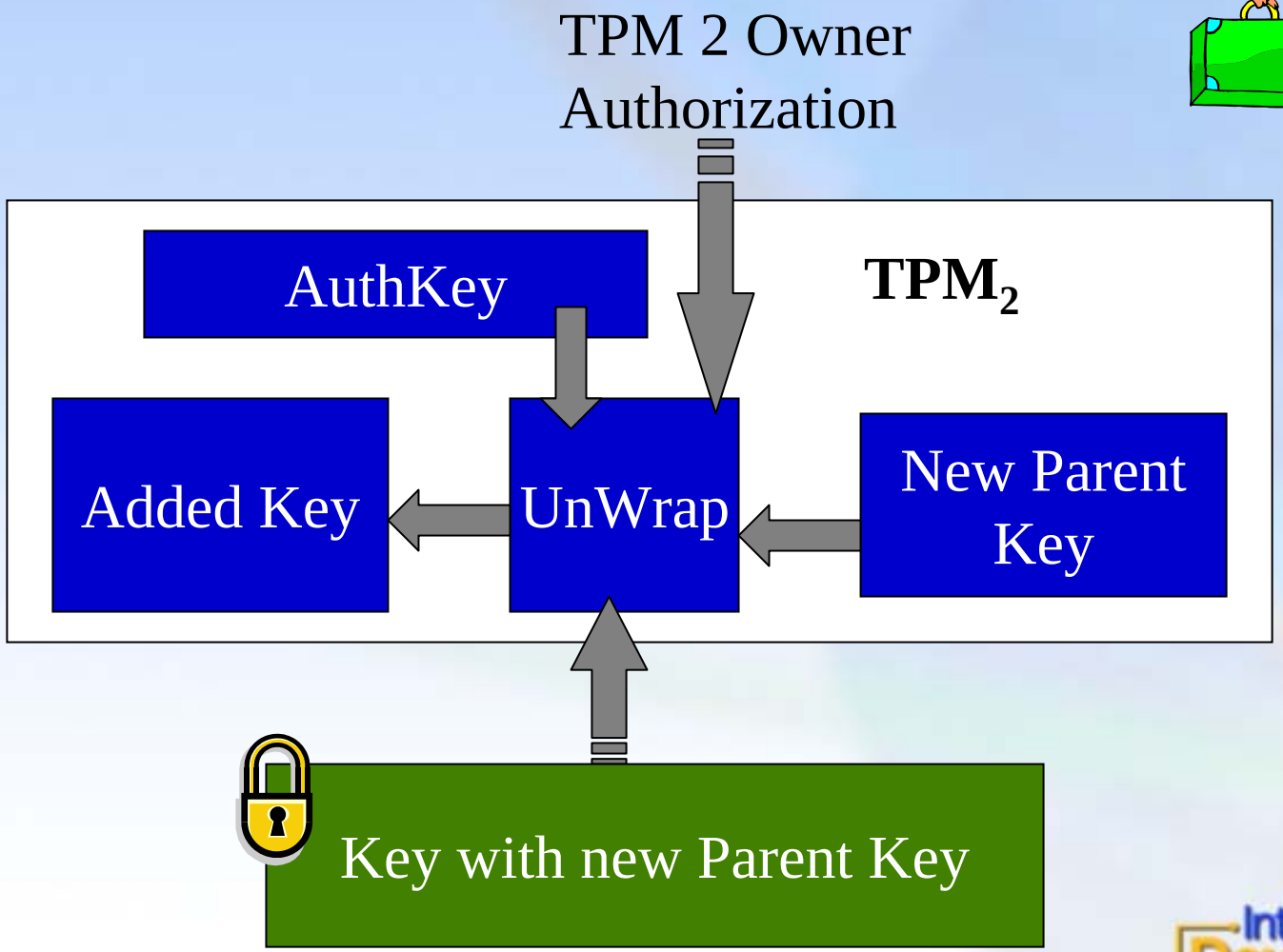
Create Migration Blob



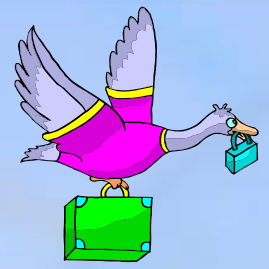


Migration of Keys





Key Hierarchy



Inside TPM1

Storage Root Key (SRK) 1

Migratable Signing Key

Migratable Signing Key

Migratable Storage Key

Inside TPM2

Storage Root Key (SRK) 2

On Disk

Migratable Storage Key

Migratable Signing Key

Migratable Storage Key

Migratable Signing Key

Migratable Signing Key

Migratable Storage Key

TPM Maintenance

What is Maintenance

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

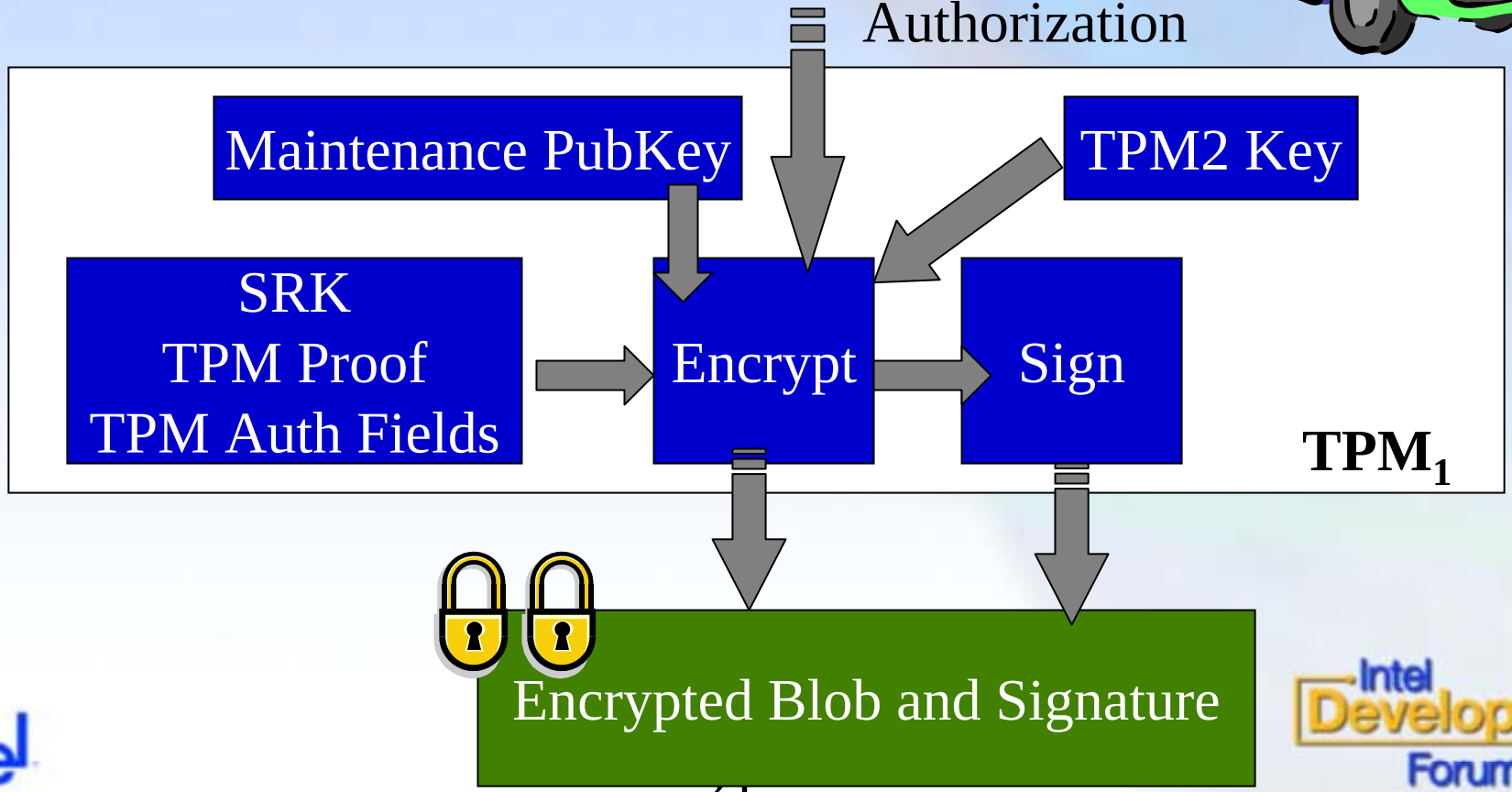
Situations for Maintenance

- 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

TPM Create Archive Command

- **Must be Authorized by TPM Owner not User**



TPM Load Archive Command

TPM 2 Owner Authorization

SRK2
TPM Proof2
TPM Auth Fields2

TPM2 Key

SRK1
TPM Proof1
TPM Auth Fields1

Decrypt

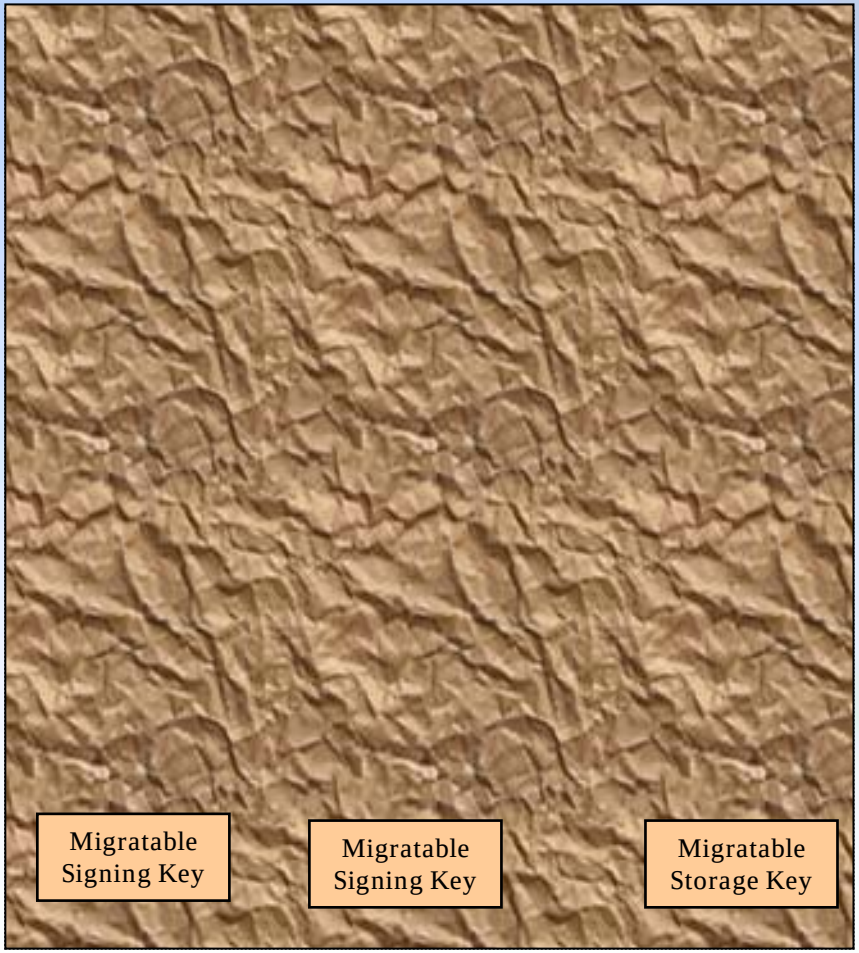
TPM_2

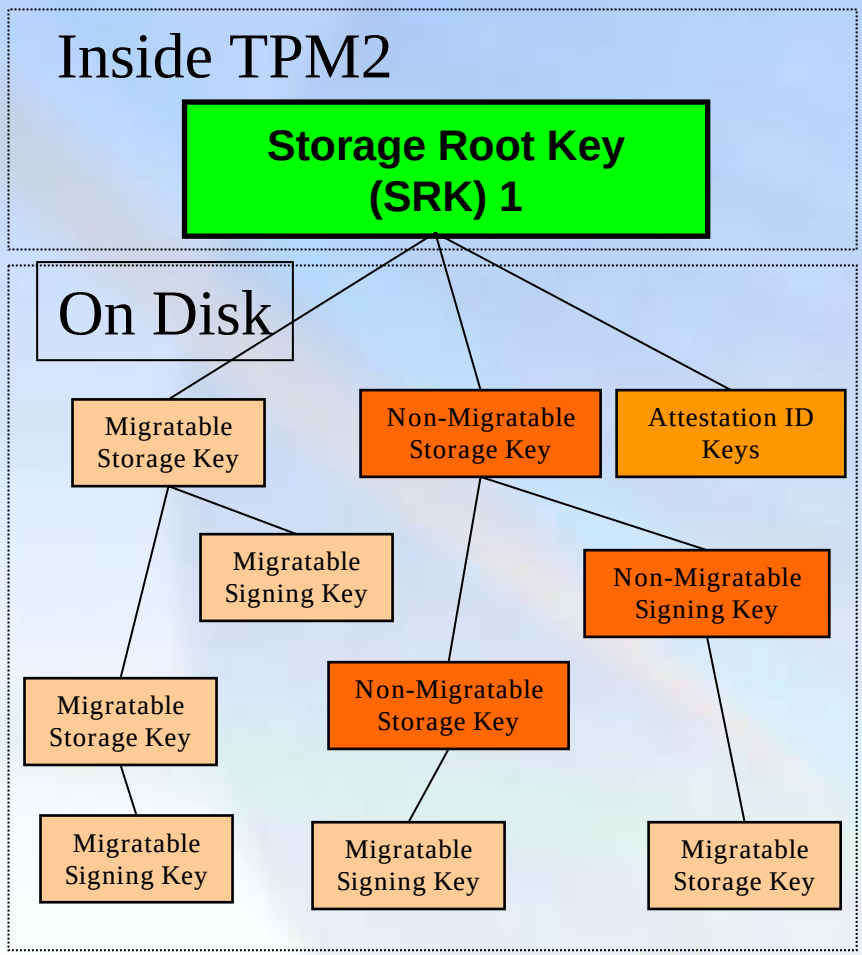
Encrypted Blob and Signature

Decrypt W/Maint. priv key

Encrypted For TPM 2

Key Hierarchy





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

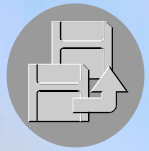
Maintenance Considerations

- How many platforms can the blob 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

Review

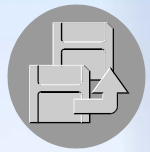
Scenarios

- Loss of data files



Restore from Backup

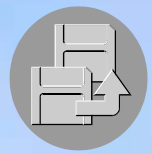
- Hard Drive Failure



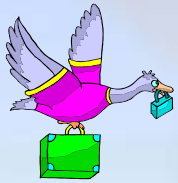
Insert new Hard Drive and restore from Backup

Scenarios

- **Motherboard Failure**



Backed-up encrypted files still need TPM keys to decrypt



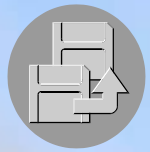
- **TPM Failure**

Migration does not restore encrypted files of non-migratable keys

Maintenance would restore all keys

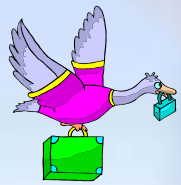
Scenarios

- System Failure



Backup – Encrypted or in the clear

- Computer Theft



Migration – Can't create migration blobs if you don't have the computer

- Disk Image Backup

Maintenance – create blobs before disaster

Summary

- Backup policies and procedures available today (this is not new)
- Migration for migratable keys
- Maintenance involves Platform Manufacturer and only method to restore non-migratable keys

- Policy, Practice, Execution

Questions

Thank you for attending.

Please fill out the Session Evaluation Form.