Stitching Together the TPM and Opal SED

Robert Thibadeau, Ph.D.
SVP & Chief Scientist
Wave Systems Corp.
rthibadeau@wave.com
www.cs.cmu.edu/~rht
Table of Contents

• Overview and Background
• Details on Security Architecture
Stitching these together

3 SPECIFICATIONS

Self-Encrypting Drive (SED)
Opal 1.0 & 2.0+
Data-At-Rest Protection
Independent of OS and OS-Present Software

Trusted Platform Module (TPM)
Versions 1.2 & 2.0e
Hardware Protected PC Identity
Key and Pre-OS-Boot Environment

Trusted Network Connect (TNC)
Version 1.5+
Identity, Pre-OS-Boot, and other PC Health to Grant Access to Secure Network
As with any architectural design, there are general principles that facilitate the integration of the architecture into real-world contexts (since these contexts can change). For this reason we have created three security zone types.

- **“Central Distribution”** Highly trusted, highly secure location where PCs and SEDs are provisioned with security configurations and secrets that will not change over the life of the PC and SED. If change is required for an unanticipated reason, it can be effected since the credentials needed are retained by the Central Distribution database. Per PC, and per SED, these credentials do not exceed 10KB.

- **“Fielding Site”** Trusted, secure location, where certain field provisioning, de-provisioning, and purging operations take place on the SEDs. This site may also have access to means to update the BIOS, Firmware, or Security Settings on the PCs (including the TPMs).

- **“End User PC”** Moderately trusted, moderately secure location. At this location all authorities and their credentials are fixed. The TCG architecture simply permits end-users passcode authentication to use the PC.
What is an SED? Secure Data Storage

Self-Encrypting Drive (SED)
Opal 1.0 & 2.0+
Data-At-Rest Protection
Independent of OS and OS-Present Software

100% of Data Written Here is Encrypted
TPM Security on the PC Motherboard

Trusted Platform Module (TPM)
Versions 1.2 & 2.0e
Hardware Protected PC Identity
Key and Pre-OS-Boot
Environment

Motherboard

I/O
CPU
Memory
SATA
Other Chips

TPM Chip

Public-Private Keypairs
Hardware Protected
Private Key Operations

Platform Configuration
Registers (PCRs)
For Guarded PC
Health Measurements
TPM Guards Cryptography and Data

Trusted Platform Module (TPM) Versions 1.2 & 2.0e
Hardware Protected PC Identity Key and Pre-OS-Boot Environment

Public-Private Keypairs
Hardware Protected Private Key Operations

Platform Configuration Registers (PCRs)
For Guarded PC Health Measurements

TPM

Cryptographic Processor
- Random Number Generator
- RSA Key Generator
- SHA-1 Hash Generator
- Encryption/Decryption Signature Engine

Persistent Memory
- Endorsement Key (EK)
- Storage Root Key (SRK)

Versatile Memory
- Platform Configuration Registers (PCR)
- Attestation Identity Keys (AIK)
- Storage keys
How do the three work together?

In Normal Use

TPM
- Non Spoofable Device ID
- Device Preboot Health

TNC

Additional SED Unlock Key

Passcode to Unlock SED

SED
How do the three work together?

In Provisioning

Device Health Params

Central Distribution PC Setup

TPM_Passcode, Key Pair, and Certificate Creation

Provisioning with Access Policies

TNC

Disk Duplication

Passcodes to Unlock and Manage SED and Use TPM

Additional SED Unlock Key

SED
Deployment and Provisioning Cases Solved

1. SED
2. SED + TPM
3. SED + TPM + TNC
4. TPM + TNC
Levels of Trust

“Central Distribution”

This is where the PC and SED are brought together and Secrets are securely provisioned **JUST ONCE for the entire life of the PC-TPM and the SED**. The “ownership” credentials need to be stored in a secure database, but should never have to be used.

“Fielding Site”

This is where certain (TPM and SED unique) administrative credentials can be employed **and user credentials can be changed administratively**. It is also where forensic logs can be examined and an SED can be cryptographically erased.

“PC”

This is where the PC and SED are operating normally. The normal use is made to login to the PC. If the PC tries to join the secret network, it’s globally unique, non-spoofable, identity can be checked and it’s preboot health can be checked (including possible tampering with BIOS, boot configurations, a hypervisor, etc.)
Security Architecture Detail
Opal SEDs support Authority Hierarchy authenticated with 32 Byte Passcodes

- **“Admin SP Administrator”, or “SID”, or “Drive Owner”**
  - Central Distribution
  - Creates / Deletes
  - Assigns Roles

- **“Locking SP Administrator”, or “Admin” – Up to 4**
  - Fielding Site
  - Creates / Deletes
  - Assigns Locking Roles

- **“Locking SP User”, or “User” – Up to 8**
  - PC
  - Creates / Deletes
  - Assigns Locking Roles

---

**Locked SED 128 MB**
*Includes preboot SW and a “datastore”*

**Unlocked SED 256 GB**

---

14
TPMs Create their Own Public Private Keypairs and Protect Private Key Encryption(Signing) or Decryption(Exchange)

“Auth Owner” (20 Byte Passcode)
- Creates / Deletes
- Assigns Roles
- Can Assign Other Passcodes to Use Private Keys

Public Private Keypairs
- EK (Endorsement Key) – Unique to Every TPM
  - Needed to Make
- AIK (Attestation Identity Key) – Unique to Every TPM
  - Needed to Make
  - Needed to Certify
- SK (Storage Key) – E.g., To Store SED Passwords
  - Non-Spoofable Device Identity

Created Only Once in Central Distribution
TPMs also have PCRs that record the Hashes of Preboot Firmware – PC Health Check against Kernel Attacks on PCs

Preboot PC BIOS
Hash Preboot Firmware and Configuration Settings and Put into Appropriate TPM PCR

OS Booted
TPM Signs PCRs using AIK,
OS Sends This as a Certified (Non Spoofable) Preboot Health Measurement for TNC
X.509v3 Certificates Certify Public Keys

Public (Puk) - Private (Prk) Keypairs

- Root Certificate with Puk 1
  - Self-Signed by Prk 1
  - Signed by Manufacturer

- EK Certificate with Puk 2
  - Signed by Prk 1
  - Proves real TPM

- SK Certificate with Puk 5
  - Signed by Prk 4
  - Stores SED Passcode Split

- Root Certificate with Puk 3
  - Self-Signed by Prk 3
  - Signed by Org

- AIK Certificate with Puk 4
  - Signed by Prk 3
  - Proves Device ID

Note there are usually intermediary certificates in the chains shown.

Note current architecture can be made to work without certificates if Public Keys are held in failsafe secure databases.

Private Keys held externally in high security

TPM Non-Migratable Keypairs (Private Keys are created and Never Leave the TPM)

Created Only Once in Central Distribution

Security Architecture
The TPM protects the Private Keys, the SEDs protect the Media Encryption Keys, but… *How are Passcodes Protected?*

1. SED and TPM take-ownership operations in a high security *Central Distribution* environment. *Ownership credentials do not go out in the field.* These operations are effected by a server application (e.g., Wave ERAS is one such application) by plugging the target PC with TPM and SED into a local network for a few minutes.

2. *Fielding Site duplicator & purging station* will protect Administrator and User credentials needed to manage user passwords for SEDs and TPMs and for cryptographically erasing SEDs. The duplicator, or part of it, is a secure execution environment.

3. *Employees secure their login credentials* including Org approved PC login, central distribution login, and duplicator login.

4. *On PC: the preboot environment is a secure execution environment.* Preboot code performs various tasks including unlocking SED, gaining access to the TPM SK secret.
1. Once SED is installed on PC there is one secret passcode User 1, if there is no TPM binding, which is input by an operator of the PC. This opens other secrets required for unlocking the SED for operation.

2. If TPM is not present, provision is made to use this to unlock SED without a TPM. If TPM is present, it MUST be employed on next power up of PC.

3. If an SED is not present, the TPM can still be employed for network access control.

4. All secrets used on the PC have limited value (will work only on a limited number of PCs set by policy and the limits of the ability at the duplicator to know which SED will go to which TPM.)

5. Duplicators are equipped with Admin passcodes. The secrets are needed to seamlessly move TPMs (PC) or SEDs across local protection boundaries (where common secrets may be used across PCs).

6. Provision is made to enable low bandwidth augmentation (key split) of the User 1 so that only a network known device (TPM) will be allowed to fully boot. It is possible this can fully replace the need to have a remembered passcode at a future time.

7. With the exception of the User 1 passcode, which people must remember, all others are created as 256 bit random numbers, distributed, and employed without human intervention.
# TPM Key Pairs and Authentication Passcodes

<table>
<thead>
<tr>
<th>Name (Function)</th>
<th>Keypair Function</th>
<th>Where Created</th>
<th>Certificate</th>
<th>Passcode</th>
<th>Passcode Unique To</th>
<th>Where Passcode Held</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>EK Endorsement Key</td>
<td>Exchange</td>
<td>Central</td>
<td>Yes</td>
<td>Owner Auth</td>
<td>TPM</td>
<td>Central Distribution</td>
<td>Reset TPM, Create / Delete AIK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Distribution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRK Storage Root Key</td>
<td>Exchange</td>
<td>Central</td>
<td>Yes</td>
<td>Owner Auth to Create / Delete / Change Value Nulls to R/W</td>
<td>Not Unique</td>
<td>N/A</td>
<td>Internal (Protects AIK)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Distribution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIK Attestation Identity Key</td>
<td>Signing</td>
<td>Central</td>
<td>Yes</td>
<td>Owner Auth to Create / Delete / Change Value Nulls to Sign</td>
<td>TPM</td>
<td>Central Distribution</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Distribution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SK Storage Key</td>
<td>Exchange</td>
<td>Central</td>
<td>Yes</td>
<td>User Auth SK Passcode 1</td>
<td>Fielding Site Down to TPM</td>
<td>Fielding Duplicator / SED Datastore</td>
<td>Bind SED to TPM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(SK Passcode 1 Set in Field),</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note.** All Keypairs are Non-Migratable, unique to a particular TPM & PC and are created by the TPM
<table>
<thead>
<tr>
<th>Passcode 32 Byte</th>
<th>Opal Type</th>
<th>Scope</th>
<th>Crypto Requirement</th>
<th>Where Provisioned</th>
<th>Where Held</th>
<th>Protects What Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SID</td>
<td>Admin SP Admin / SID</td>
<td>Unique - Each SED</td>
<td>Random #</td>
<td>Central Distribution</td>
<td>Central Distribution</td>
<td>Ownership, Revert Admin SP</td>
</tr>
<tr>
<td>Admin 1</td>
<td>Locking SP Admin 1</td>
<td>Transfer Region</td>
<td>Random #</td>
<td>Central Distribution</td>
<td>Central Distribution</td>
<td>Transfer SED Control to Field Duplicators</td>
</tr>
<tr>
<td>Admin 2</td>
<td>Locking SP Admin 2</td>
<td>Fielding Site</td>
<td>Random #</td>
<td>Duplicator</td>
<td>Duplicator</td>
<td>Locking SP Erase, Provisioning</td>
</tr>
<tr>
<td>Admin 3</td>
<td>Locking SP Admin 3</td>
<td>Fielding Site</td>
<td>Random #</td>
<td>Duplicator</td>
<td>Duplicator</td>
<td>Backup for Admin 2</td>
</tr>
<tr>
<td>User 1</td>
<td>Locking SP User 1</td>
<td>Fielding Site down to Person</td>
<td>Memorable Passphrase</td>
<td>Duplicator</td>
<td>Duplicator and Person</td>
<td>Unlock ranges 1-3</td>
</tr>
<tr>
<td>TPM User 2</td>
<td>Locking SP User 2</td>
<td>Fielding Site down to PC - Person</td>
<td>Random # = User1 XOR TPM Split</td>
<td>Duplicator</td>
<td>Duplicator</td>
<td>Unlock ranges 1-3</td>
</tr>
<tr>
<td>Forensic User 3</td>
<td>Locking SP User 3</td>
<td>Fielding Site down to PC - Person</td>
<td>Random #</td>
<td>Duplicator</td>
<td>Duplicator</td>
<td>Unlock range 4 Write Only</td>
</tr>
<tr>
<td>TPM Split</td>
<td>Locking SP User 2 Split</td>
<td>Fielding Site down to PC</td>
<td>Random #</td>
<td>Duplicator</td>
<td>Duplicator and TPM</td>
<td>User 1 XOR TPM Split = User 2 Bind SED to TPM</td>
</tr>
<tr>
<td>Network Split</td>
<td>Locking SP User 2 Split</td>
<td>Fielding Site down to PC - Person</td>
<td>Random #</td>
<td>Duplicator</td>
<td>Duplicator and Network</td>
<td>Bind SED to Network Authentication</td>
</tr>
</tbody>
</table>
Operator Drive Unlock Sequence: TPM Bound & Non-TPM

**TPM Binding**

- User 1 Passcode
- Pre-Boot
  - SED Data store
    - SK Passcode
  - TPM SK Blob
  - TPM Split
  - SED Access Control
    - Media key
- Drive Unlock

**Non or Unbound TPM**

- User 1 Passcode
- Pre-Boot
  - SED Access Control
    - Media key
- Drive Unlock
SED and Disk Duplicator Pre-conditions

1. SED must be a TCG Opal 2.0 256GB+ SATA SSD, preferably FIPS-140 Level 2+, supporting a minimum of 3 Users, 3 Admins, and 4 ranges, a SecretProtect Table with ProtectionMechanism Column set to 1 (which enforces media key wrapping), and a DataStore table of at least 10MB. TCG Opal 1.0 SSDs may be employed assuming the manufacturer will provide assurance on the SecretProtect attribute. The DataStore table size in Opal 1 & 2, fulfills the size requirements (10 MB).

2. SED has a minimum of four Opal ranges. These must correspond perfectly to OS File System Disk Partitions.
   a) Range 1 OS Boot / RW / : This is the main boot partition
   b) Range 2 / RW / UTO Provisioning Data : Note, this MAY require a different User for Write privilege. UTO may only write this range.
   c) Range 3 / R / Valid OS Boot and Executable Code Backup (Alt Boot) : This is only if needed to confirm integrity of range 0 boot data. This range is optional.
   d) Range 4 /W OR R / Forensic Logging : Needs a dataformat that does not require reading at the time of writing. No Passcode needed to Write in Preboot, Passcode set and not guessable during OS present. We would prefer to make this range mandatory.

3. SED must be provisioned with the following 32 Byte Authorities
   a) The SID must NOT be the same as the OPAL MSID value. This is set once by the central distribution system.
   b) Admin Authorities (Admin 1, 2 & 3)
   c) Two User Authorities ranges 1-3 (User 1 is for local range Unlocking, TPM User 2 is for local TPM-bound Bound Unlocking)
   d) Forensic User 3 will unlock range 3 for writing but not reading and only in SED Pre-boot. At the end of SED preboot, this range will be locked. The writing offset (and circular buffer size) will be kept in the SED Datastore table.

4. The ranges/partitions for all SED drives will be fixed and constant size with fixed LBA offsets on 4096K boundaries suitable for efficient (high speed) use in the disk duplicator.
TPM Pre-conditions

1. TPM 1.2+ with an IEFI BIOS that supports PCR Health Measurements conforming to the TCG PCClient Specification. If a TPM 2.0 is employed, it must be 2.0e which can operate as a TPM 1.2. ACPI Motherboard memory set aside for TPM related information (key blobs, certificates, and logs) can comfortably be a low as 30KB and need not be more than 80KB in our estimation.

2. In central distribution before the PC is deployed to a PC, the TPM must be provisioned with an EK (Endorsement Key), one AIK (Attestation Identity Key) to be employed for PCR and compressed PCR quoting along with corresponding public key certificates as defined by TCG. The SRK (Storage Root Key) will have all nulls as the passcode for sealing and unsealing SRK blobs. Finally, a non-migratable SK (Storage Key) will be generated for SED – TPM binding.

3. The Owner Auth passcode that can reset the TPM otherwise add/delete AIKs is only on level 3+ systems or better and must be unique to every TPM (bound to the EK public key value).

4. The TPM SK require User 1 as the SK Passcode, for retrieving the hidden TPM User 2 Passcode which is XORed with User 1 to provide TPM Binding to unlock the SED. This passcode can be changed (on PC) by knowledge of the previous passcode. The SK blobs and other SRK blobs are stored in persistent storage on the motherboard. It is estimated the minimum storage is 30KB and it more than 80K would not be needed. The SK blob stores a 32 byte passcode. We estimate that the TPM PCR values and logs will not exceed 20KB.

5. In PC Operation:
   a) In DataStore (which requires no passcode to read), RootSecret decrypts User Auth Passcode 1 if TPM is present.
   b) Passcode 1 Unseals TPM Split which is XORed with User 1 to yield TPM User 2, and employed for unlocking ranges 0-3
   c) Forensic logging in preboot is enabled by User 1 unlocking before unlocking ranges 0-2
   d) User 1 is employed to disable User 1 from unlocking SED bands 1-3 to bind the SED to this particular TPM
   e) If TPM is not present, User 1 will unlock the ranges. We trust the preboot to not to use this on first boot if valid TPM is present.
   f) Forensic logging range is locked before OS boot. This range is only available for preboot and duplicator logging.
   g) If SED is not present, Only the AIK is valid for non-spoofable PC identity, PC Preboot Health, and Trusted Network Connect. No preboot User 1 passcode is requested on boot. First Boot Screen is different for Non-SED equipped PCs.
TNC Sequence 1: Provisioning at Central Distribution

Main: Database/Server

- Get AIK
- AIK Certificate
- Save AIK Info
- Request Medium Report
- Report
- Save valid machine state

PC

- A URI can be added to the cert to point to a list of known good states. Might be useful if outside resources are required to have access to the information. Also can contain PCR info.

Options:
1. Generate Report and pull info out of it and assign the PCR values to that particular machine.
   A. 1-1 mapping between states and machines
   B. Harder to manage

2. Use a collection of known states (configurations). Assign the configuration to that particular machine and use the report to verify the state.
   A. Easier to manage if the number of configurations are minimal.
   B. Harder to manage if BIOS configurations vary widely.
   C. Easier to manage configuration updates if a set of known good PCRs available already.

3. Add PCR info to the certificate.
   A. Eliminates need to touch the database
   B. Harder to update in the field. May require the disk to be swapped out.

Configuration States are affected by:
- BIOS type/version
- TPM type/version
- Machine type
- BIOS configuration
- SED state and version (if in the Transitive Trust Chain)
- And if using PCR 6, hibernation information.

Save
- AIK public key
- ID - hash of AIK (20 bytes)
- Number of PCRs (2 bytes)
- PCRs selected (1xnumber)
- PCR value (20*number)
- TPM cap version (15+?)
TNC Sequence 2: Generate Small Report

Main: Database/Server

<table>
<thead>
<tr>
<th>PC</th>
<th>Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect Info about PC</td>
<td>Verify Report</td>
</tr>
<tr>
<td>Request Initial Report</td>
<td>Report</td>
</tr>
</tbody>
</table>

IF-M Message Header (8 Bytes)

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1</td>
</tr>
<tr>
<td>Reserved</td>
<td>3</td>
</tr>
<tr>
<td>Message Identifier</td>
<td>4</td>
</tr>
</tbody>
</table>

IF-M attribute Header (12 Bytes)

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags</td>
<td>1</td>
</tr>
<tr>
<td>Attribute Type Vendor Id</td>
<td>3</td>
</tr>
<tr>
<td>Attribute Type</td>
<td>4</td>
</tr>
<tr>
<td>Attribute Len</td>
<td>4</td>
</tr>
</tbody>
</table>

Value: (276 Bytes)

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>20</td>
</tr>
<tr>
<td>Signature</td>
<td>256</td>
</tr>
<tr>
<td>Total</td>
<td>296</td>
</tr>
</tbody>
</table>

Compute Composite from Known Value
Number of PCRs (2 bytes)
PCRs Selected (1 x number)

Compute Quote Info2 from Known Composite / TPM info
Tag (2 bytes)
Fixed (4 bytes)
Hash of Composite (20 bytes)
Nonce (20 bytes)
Number of PCRs selected (2 bytes)
PCRs selected (1*number) max 7 bytes
TPM locality (1 byte)
TPM Cap Version info (15 bytes + ?vendor data)

Use ID to find AIK and verify signature of it
**TNC Sequence 4: Generate Medium Report (TPM Version Info - recommended)**

*Main: Database/Server* | *PC* | *Cloud*
---|---|---
Collect Info about PC | Request Initial Report | Report

**IF-M Message Header (8 Bytes)**
- Version: 1
- Reserved: 3
- Message Identifier: 4

**IF-M attribute Header (12 Bytes):**
- Flags: 1
- Attribute Type Vendor Id: 3
- Attribute Type: 4
- Attribute Len: 4

**Value: (481 Bytes + ?) includes Composite**
- ID: 20
- Quote Info: 56

**Composite (149 Bytes)**
- Number of PCRs selected: 2
- PCRs selected (1*number) max 7 Bytes: 7
- PCR value (20*number) max 140 bytes: 140

**Total**
- 516 + ?

If we know the TPMs that will be used we will be able to fill in the ?'. Today it is variable data dependent on the TPM manufacturer.

If we know the TPMs that will be used we will be able to fill in the ?'. Today it is variable data dependent on the TPM manufacturer.

Use ID to find AIK and Verify signature of quote info
Verify hash of Composite.
Compare all required PCR values and their values from the composite.
Verify version of TPM.
TNC Sequence 4: Generate Large Report

Main: Database/Server ─―― PC ─―― Cloud

Collect Info about PC
Request Initial Report
Report
Verify Report

IF-M Message Header (8 bytes)
- Version: 1
- Reserved: 3
- Message Identifier: 4

IF-M attribute Header (12 bytes):
- Flags: 1
- Attribute Type Vendor Id: 3
- Attribute Type: 4
- Attribute Len: 4
- Value: (496 Bytes + ?) includes Composite
  - ID: 20
  - Quote Info 2: 56

Composite (149 Bytes)
- Number of PCRs selected: 2
- PCRs selected (1*number) max 7 Bytes: 7
- PCR value (20*number) max 140 bytes: 140
- TPM version 15 Bytes + Vendor info?: ?
- Signature: 256
- Integrity Measurement Log: ??
- Total: 516+?+??

Use ID to find AIK and Verify signature of quote info
Verify hash of Composite.
Compare all required PCR values and their values from the composite.
Verify version of TPM.

If we know the TPMs that will be used we will be able to fill in the ?'. Today it is variable data dependent on the TPM manufacturer.

Verify version of TPM.
Queries?