

**RIGHT
HERE
RIGHT
NOW**

Opal SSDs Integrated with TPMs

August 21, 2012

Robert Thibadeau, Ph.D.

waveTM

U.S. Army ... SSDs Must be Opal SEDs

- We also Studied using the TPM (Trusted Platform Module) with an Opal SSD SED (Self-Encrypting Drive)

Security Architecture Provisioning and Use

- **“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.
- **“Fielding Site”** **Trusted, secure location** where certain field provisioning, de-provisioning, and purging operations take place on the **SEDs**. -- NOT TPMS...which are on the motherboards
- **“PC”** **Moderately trusted, moderately secure location**. At this location all authorities and their credentials are fixed except a user can change his own password.
- **OPAL PRE-BOOT (MBR Shadow) is considered SECURE**

Trusted Computing Group (TCG)

2 SPECIFICATIONS

Self-Encrypting Drive
(SED)

Opal 1.0 & 2.0+

Data-At-Rest Protection

Trusted Platform Module
(TPM)

Versions 1.2 & 2.0e

Hardware Protected PC Identity
Key and Key Storage

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



Motherboard Drive Controller
(SATA)



SED

Drive I/O Interface (SATA)

Drive Electronics w/ Encryption
Circuits and Passcode Firmware

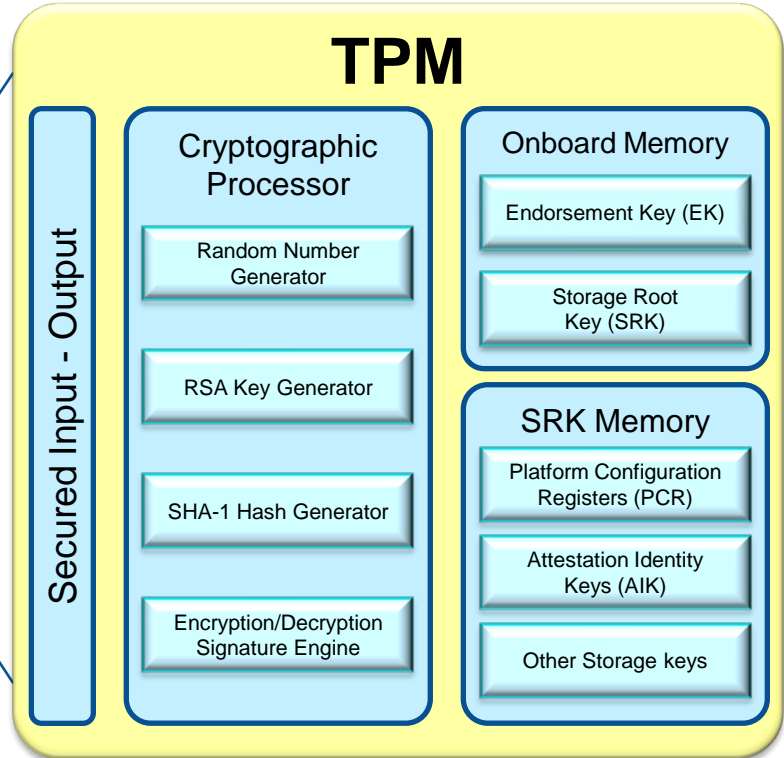
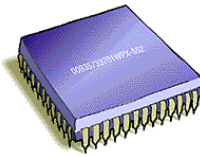
100% of Data Written Here is
Encrypted

What is a TPM? TPM Guards Cryptography and Data

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

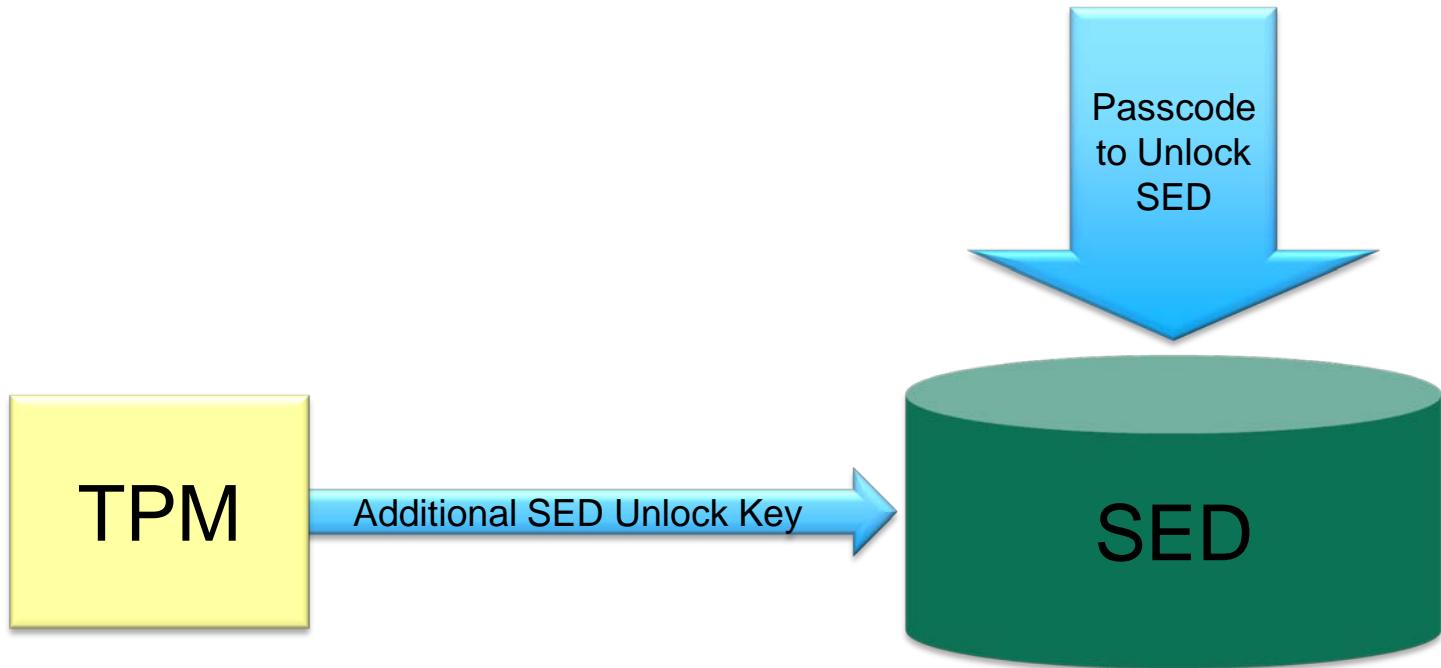
Public-Private Keypairs
Hardware Protected Private Key Operations

Platform Configuration Registers (PCRs)
For Guarded PC Health Measurements



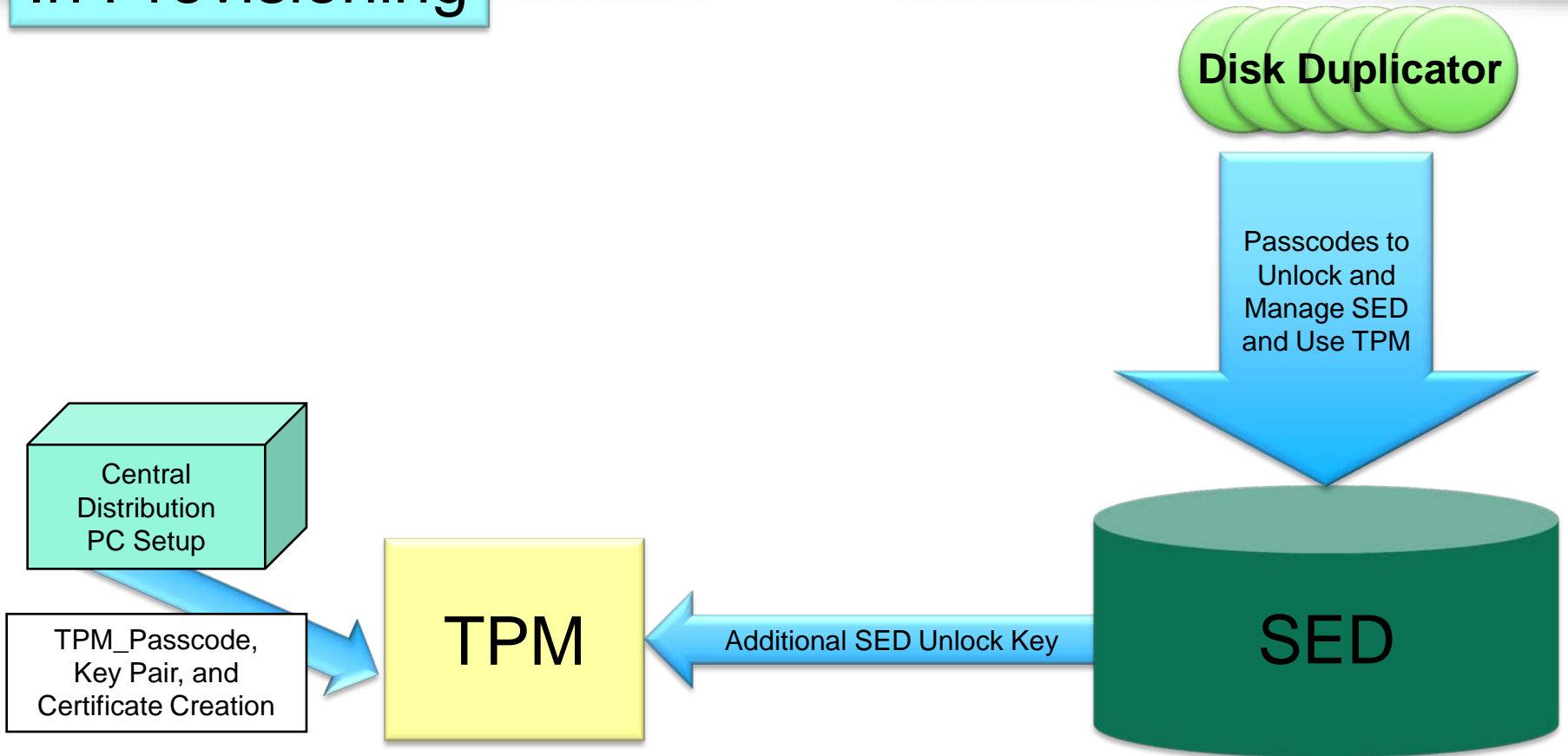
How do the two work together?

In Normal Use

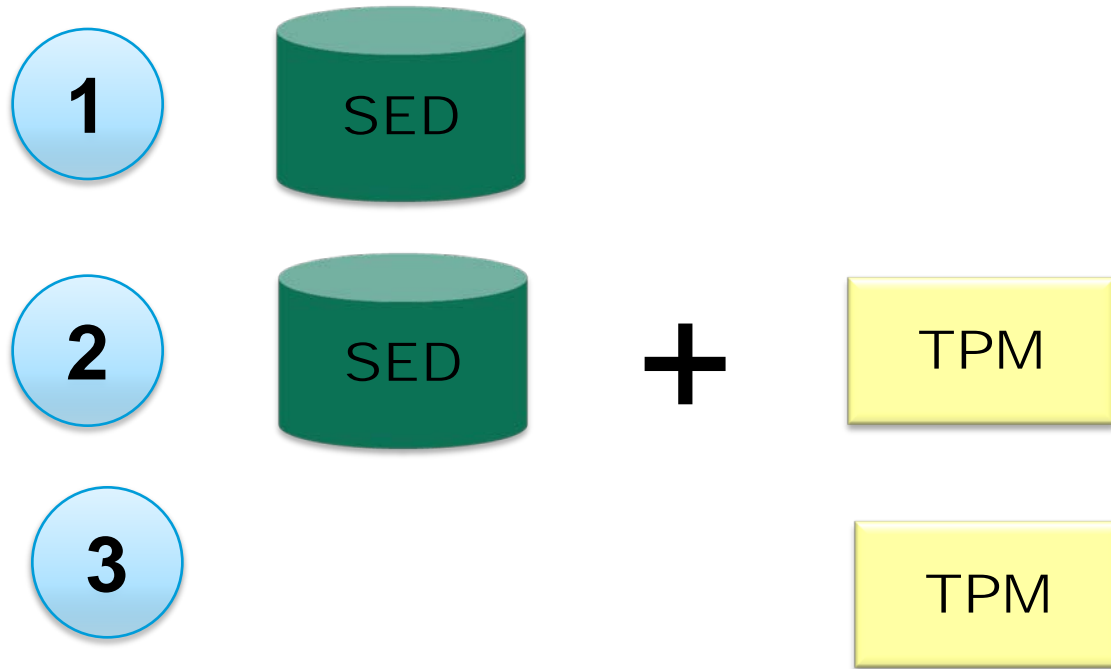


How do the two work together?

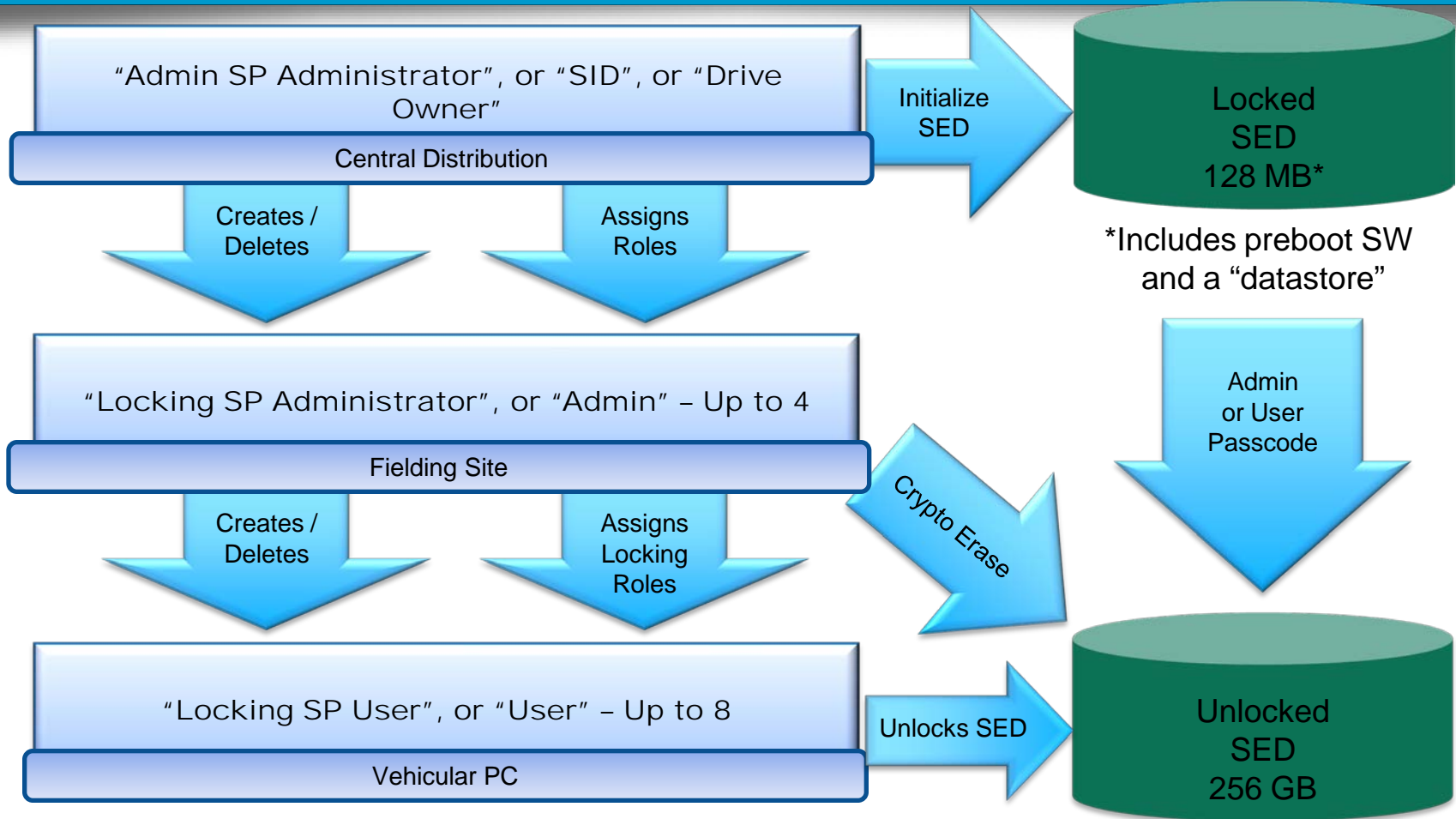
In Provisioning



Use Cases



Opal SEDs support Authority Hierarchy authenticated with 32 Byte Passcodes



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

Created Only Once in Central Distribution

"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

SK (Storage Key) - E.g., To Store SED Passwords

Needed to Certify

Non-Spoofable Device Identity

X.509v3 Certificates Certify Public Keys

Public (Puk) - Private (Prk) Keypairs

Private Keys held externally in high security

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

Signed by Manufacturer

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

Signed by org



**EK Certificate with Puk 2
Signed by Prk 1**

Proves real TPM



**AIK Certificate with Puk 4
Signed by Prk 3**

Proves Device ID



**SK Certificate with Puk 5
Signed by Prk 4**

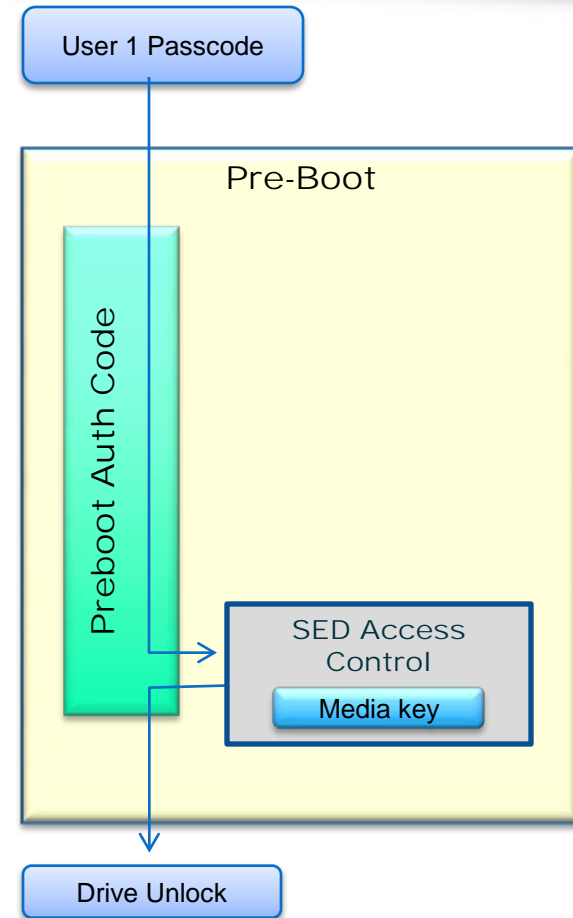
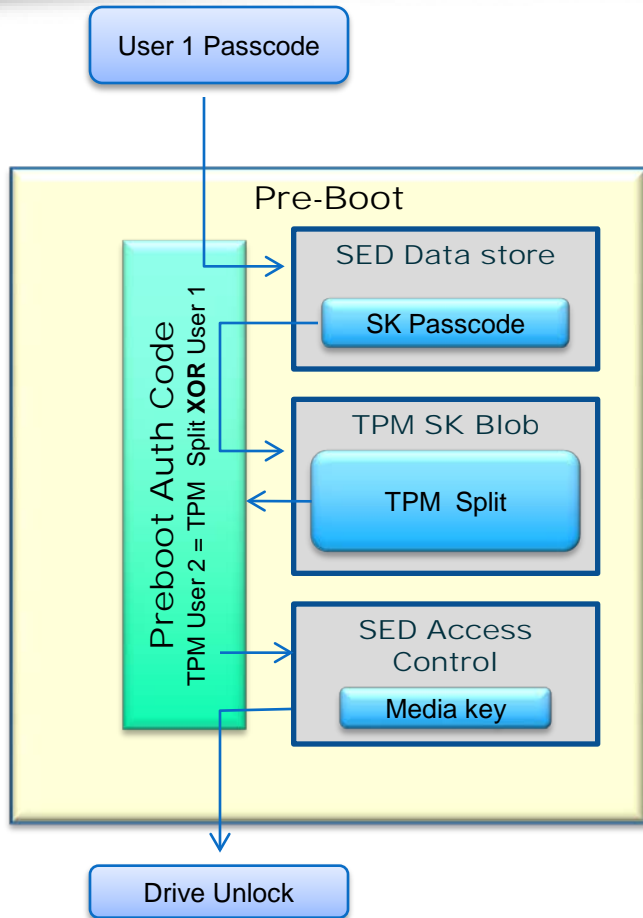
Stores SED Passcode Split

Created Only
Once in Central
Distribution

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

Operator Drive Unlock Sequence: TPM Bound & Non-TPM

TPM Binding Non or Unbound TPM



Thanks!

- **“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.
- **“Fielding Site”** **Trusted, secure location** where certain field provisioning, de-provisioning, and purging operations take place on the **SEDs**. -- NOT TPMS...which are on the motherboards
- **“PC”** **Moderately trusted, moderately secure location**. At this location all authorities and their credentials are fixed except a user can change his own password.
- **OPAL PRE-BOOT (MBR Shadow) is considered SECURE**