RIGHT HERE RIGHT NOW

Opal SSDs Integrated with TPMs

August 21, 2012

Robert Thibadeau, Ph.D.

wave™

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+

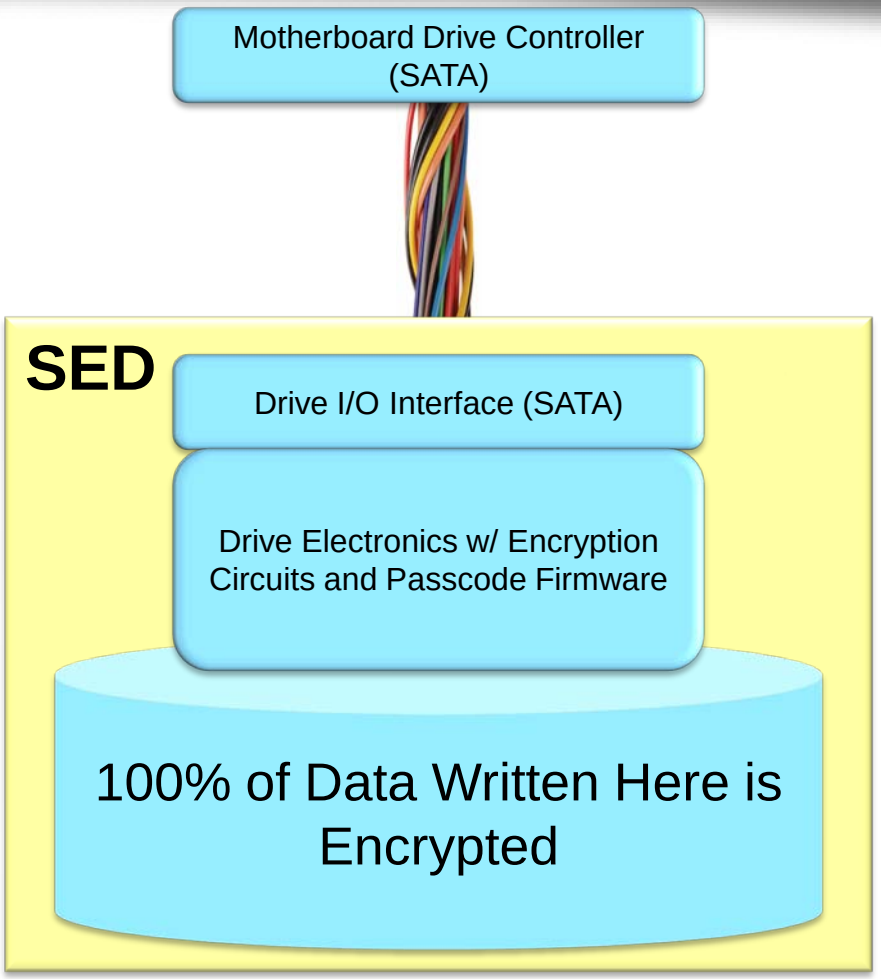
Data-At-Rest Protection

Trusted Platform Module
(TPM)
Versions 1.2 & 2.0e

Hardware Protected PC Identity
Key and Key Storage

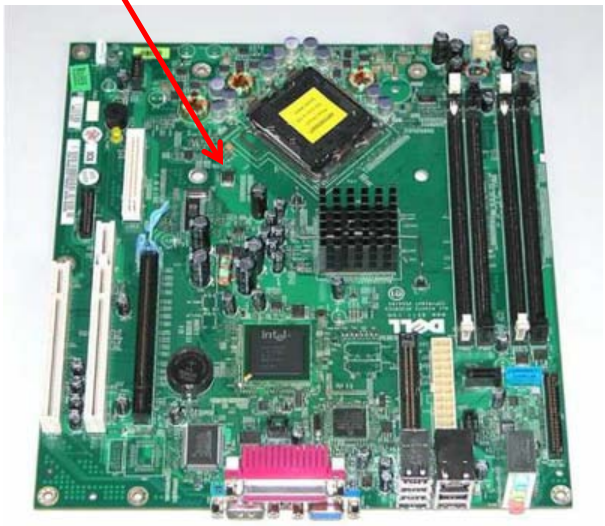
What is an SED? Secure Data Storage

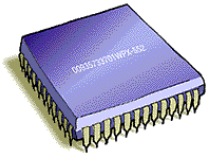
Self-Encrypting Drive (SED)
Opal 1.0 & 2.0+
Data-At-Rest Protection Independent of OS and OS-Present Software



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

TPM

Secured Input - Output

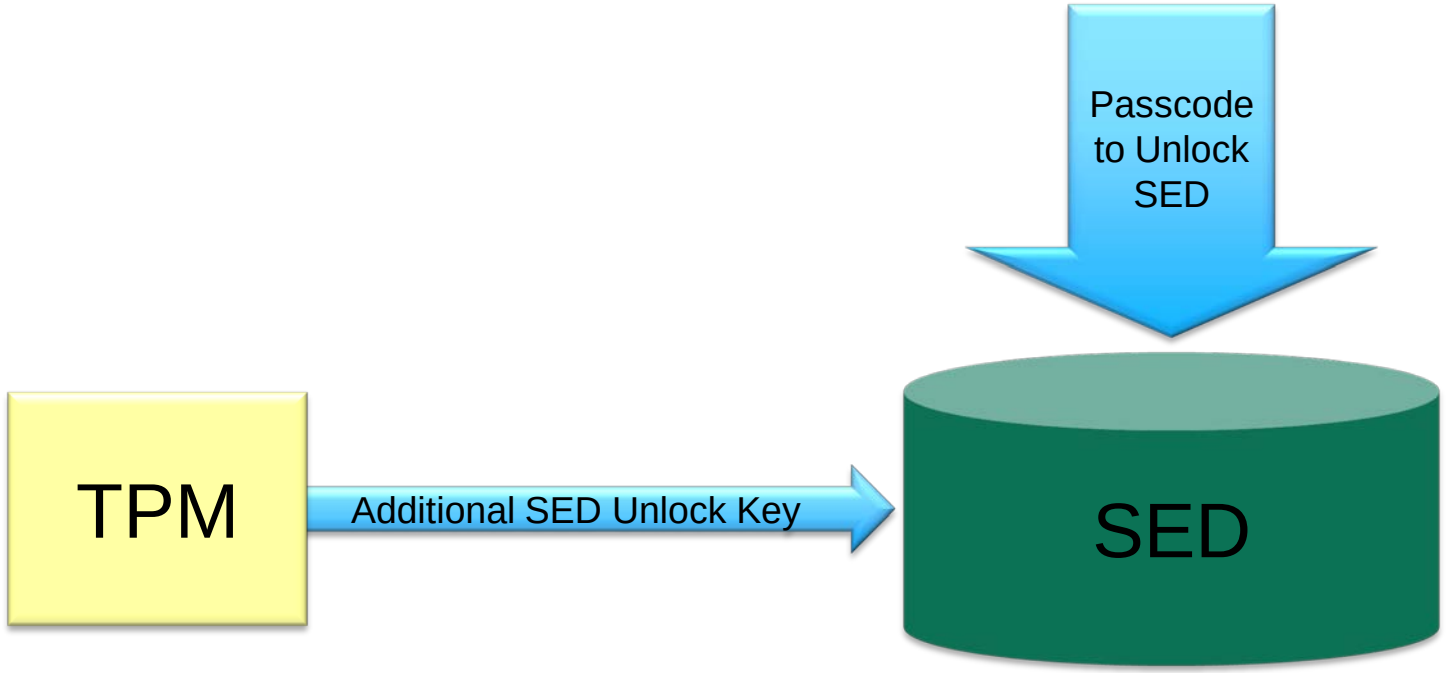
Cryptographic Processor
- Random Number Generator
- RSA Key Generator
- SHA-1 Hash Generator
- Encryption/Decryption Signature Engine

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

SRK Memory
- Platform Configuration Registers (PCR)
- Attestation Identity Keys (AIK)
- Other Storage keys

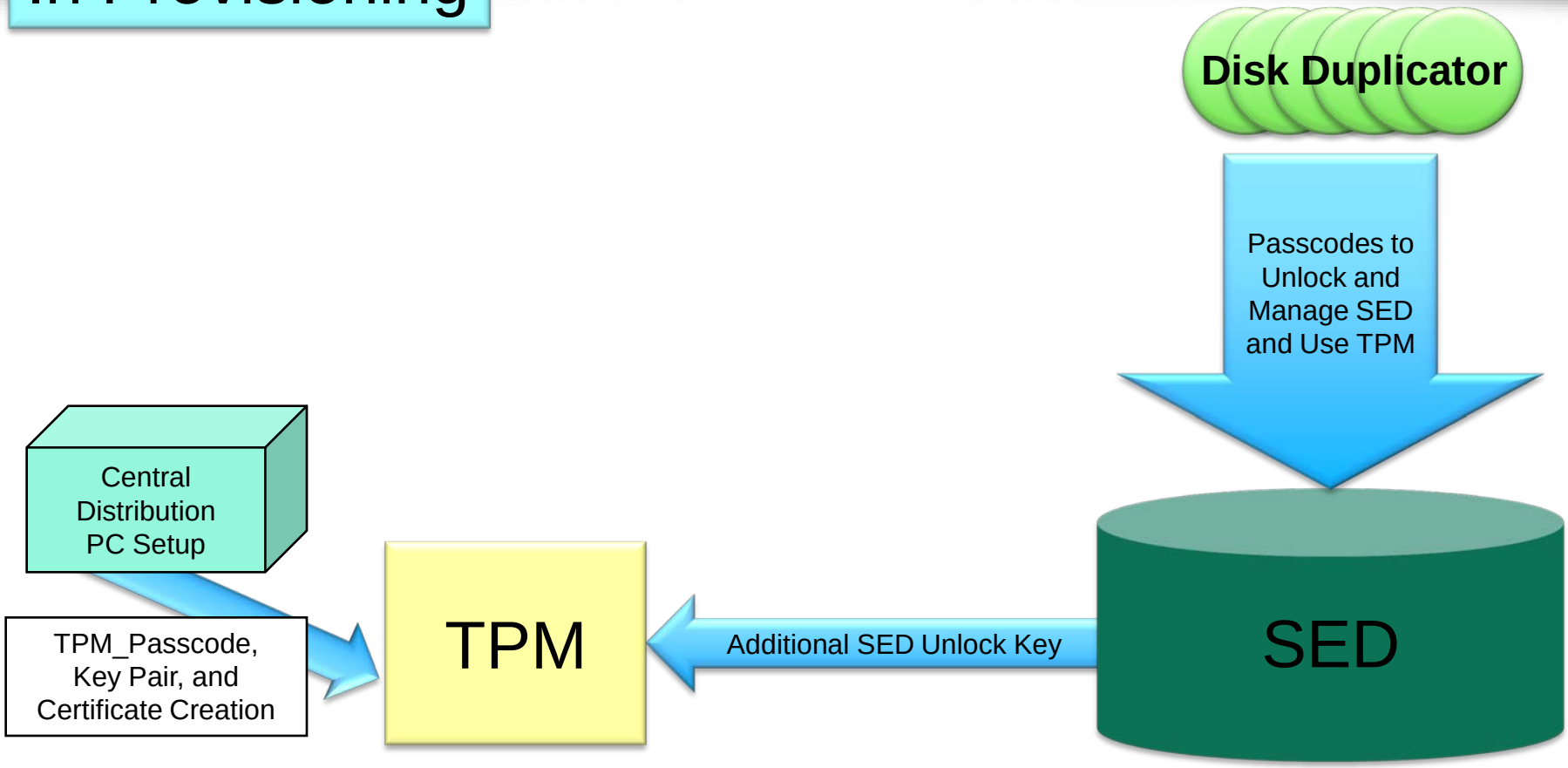
How do the two work together?

In Normal Use

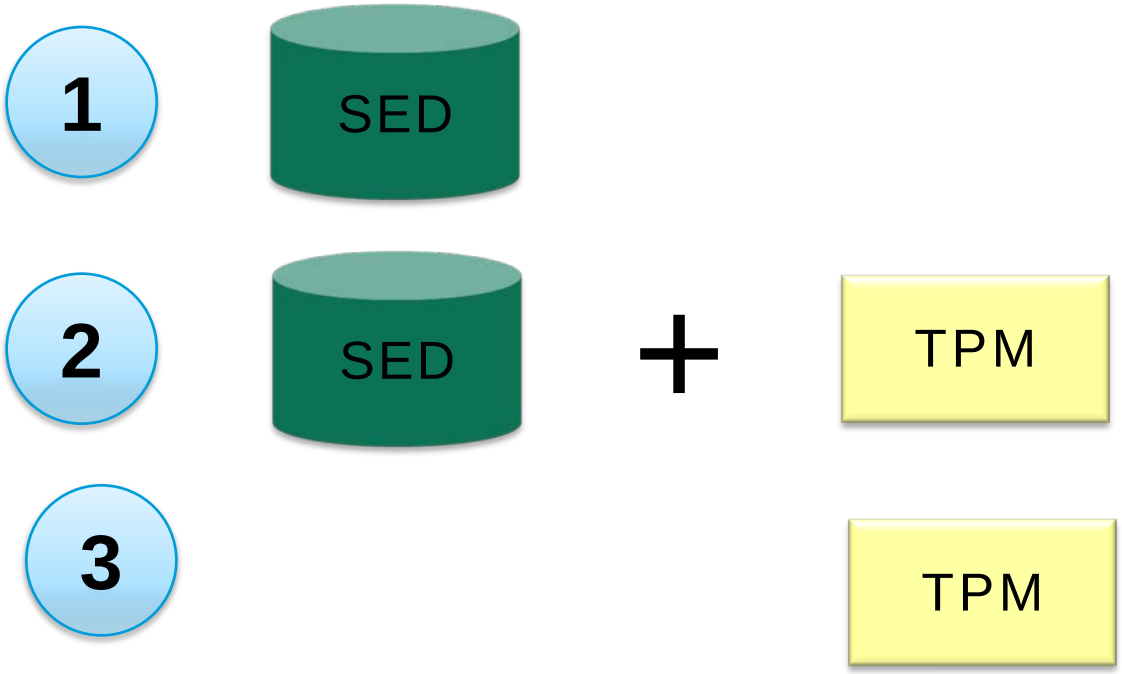


How do the two work together?

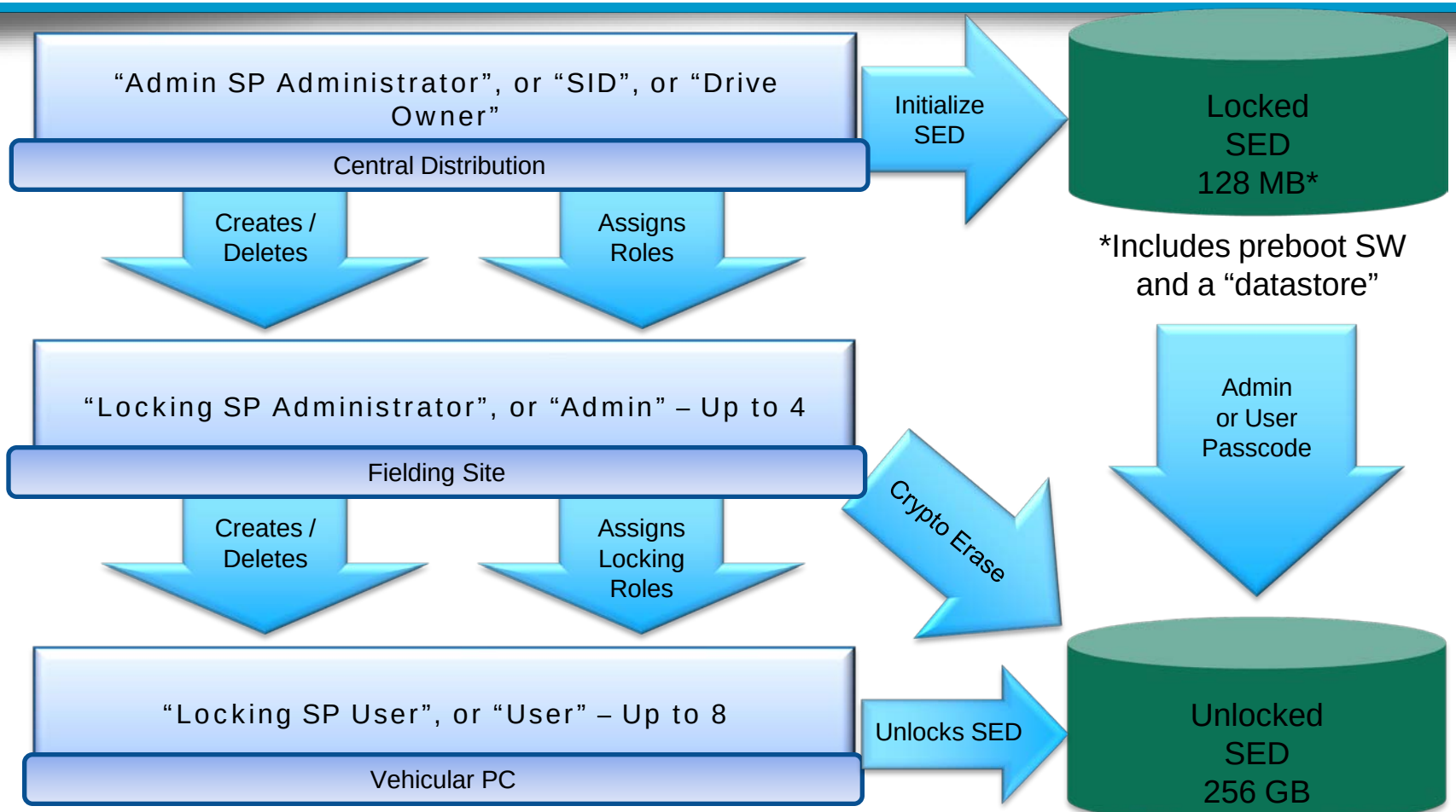
In Provisioning



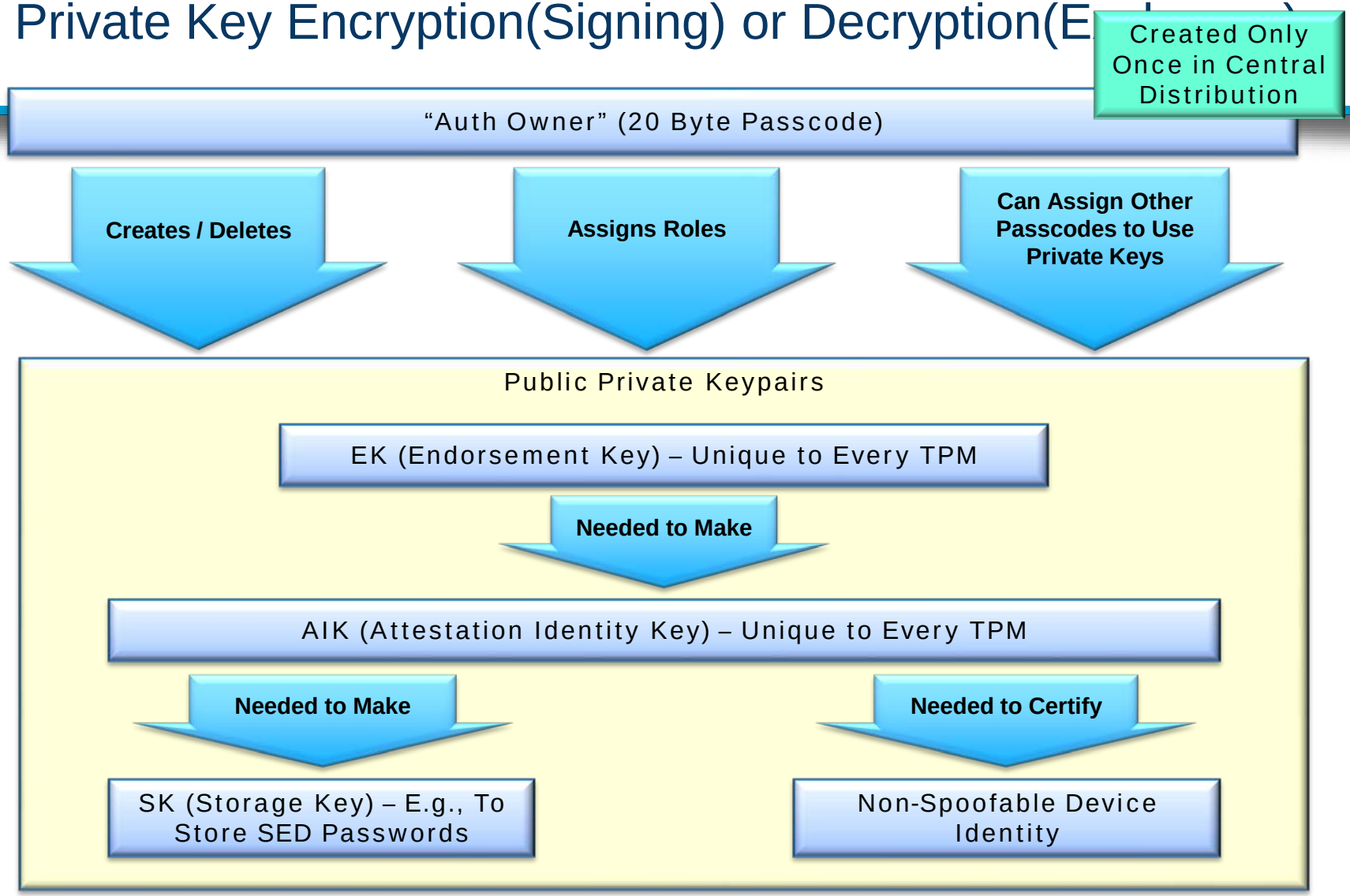
Use Cases



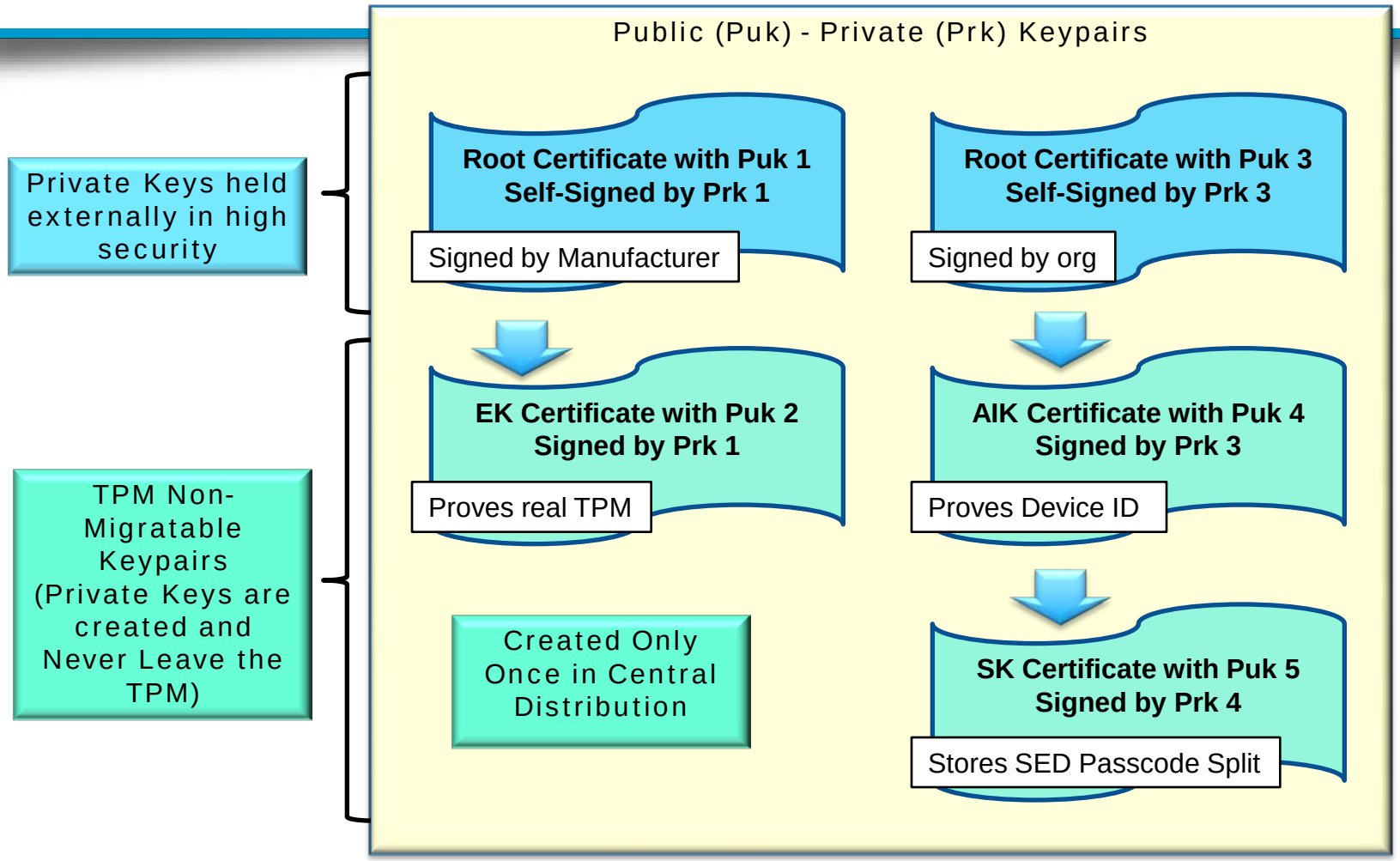
Opal SEDs support Authority Hierarchy authenticated with 32 Byte Passcodes



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

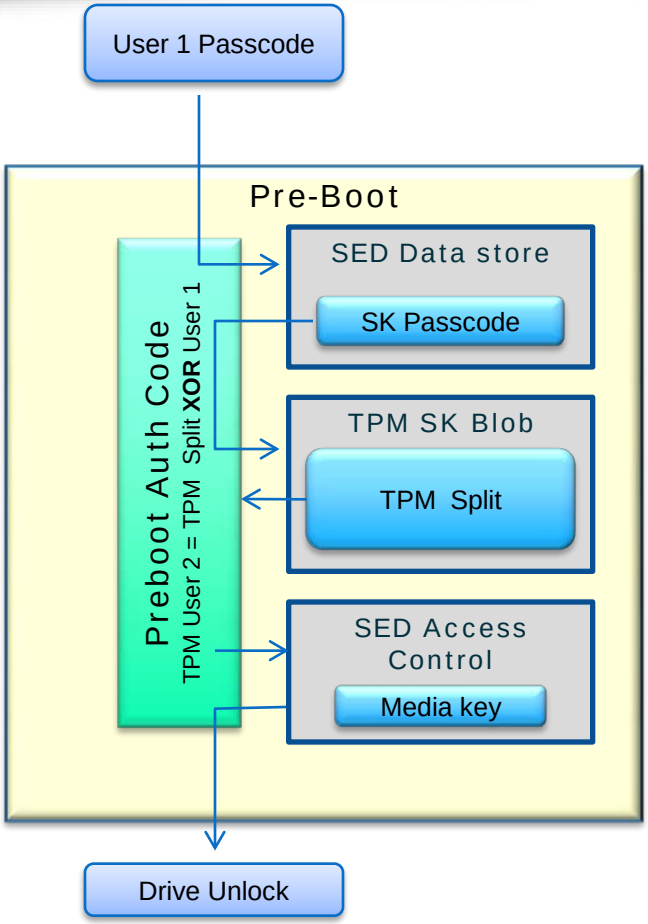


X.509v3 Certificates Certify Public Keys

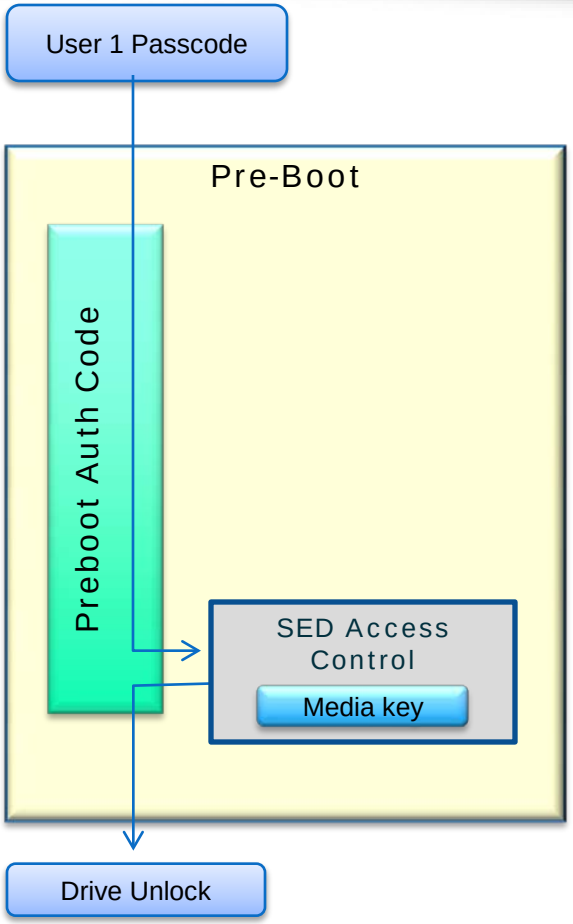


Operator Drive Unlock Sequence: TPM Bound & Non-TPM

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**