SNIA DSI '16 DATA STORAGE INNOVATION CONFERENCE
Innovation in Storage Products, Services, and Solutions
June 13-15, 2016 | Marriott San Mateo | San Mateo, CA

Deploying Simple Secure Storage Systems

Chris Allo

System and Drive Security Lead

SEAGATE

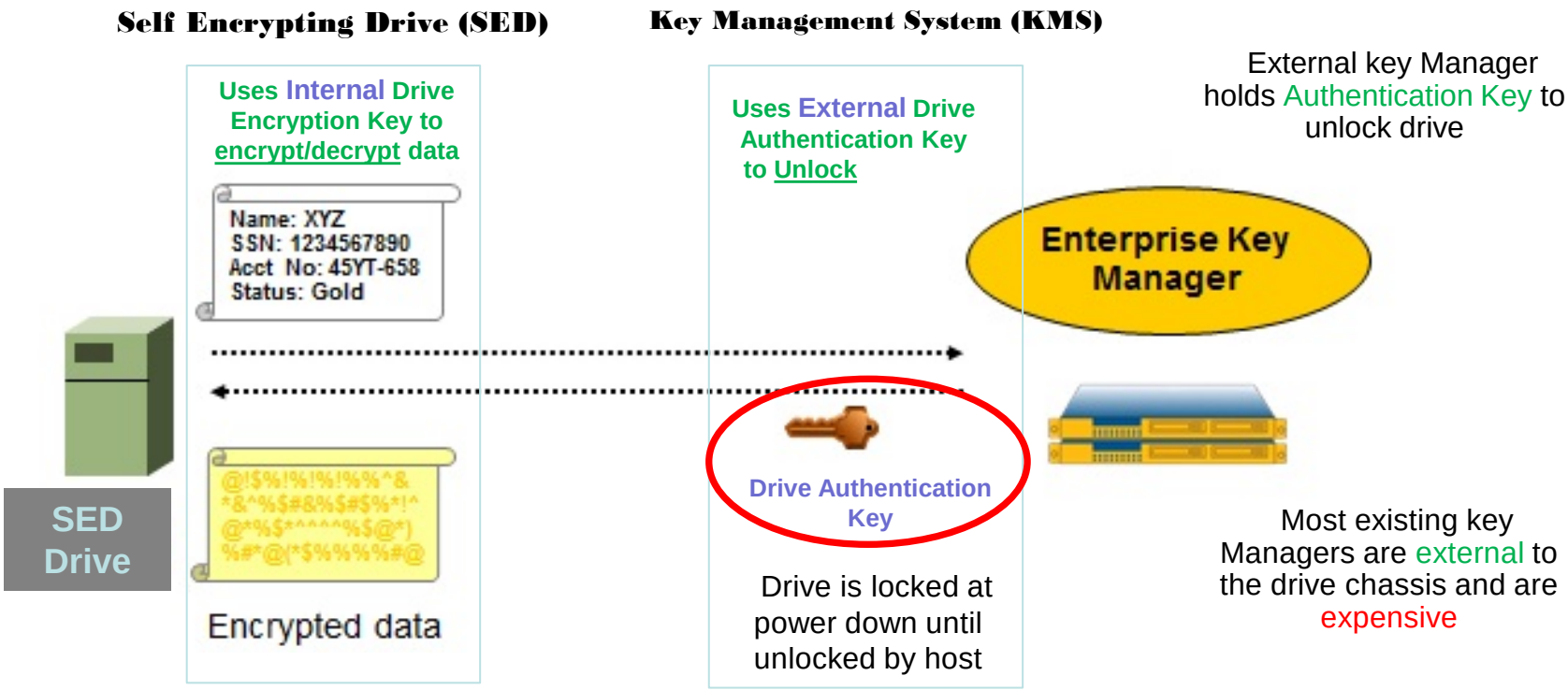
Overview

- Why Key Management?
- Key Management Landscape
- Conventional Key Management
- Problems Facing Simple Data storage
- Primary Use Cases
- Methods to Deploy a Simple Secure Solution
- Questions

Why Key Management ?

Background

Drive Unlocking through a Key Manager and Drive Data encryption



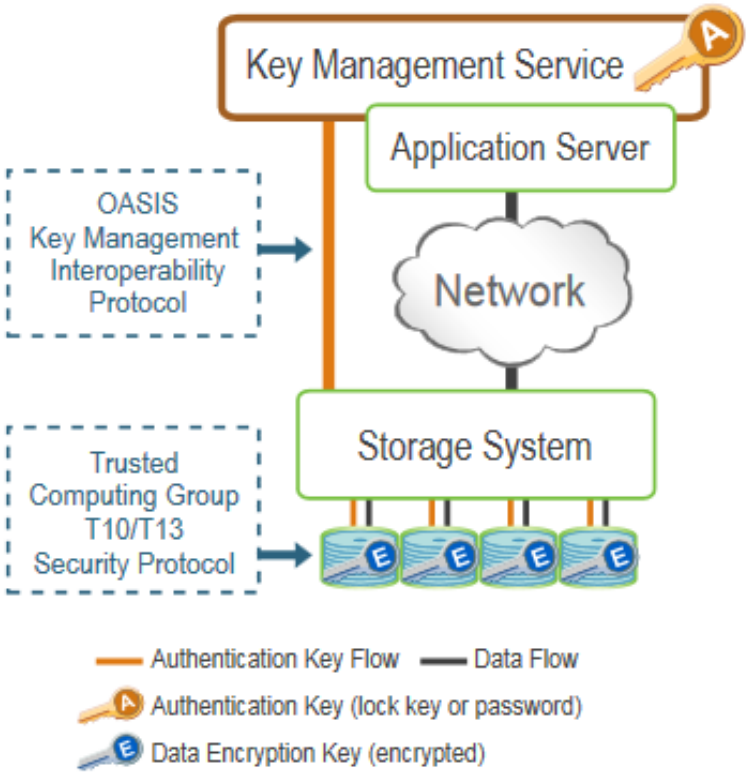
- Source: From CodePlex contributed by trotsia,,

Key Management Landscape

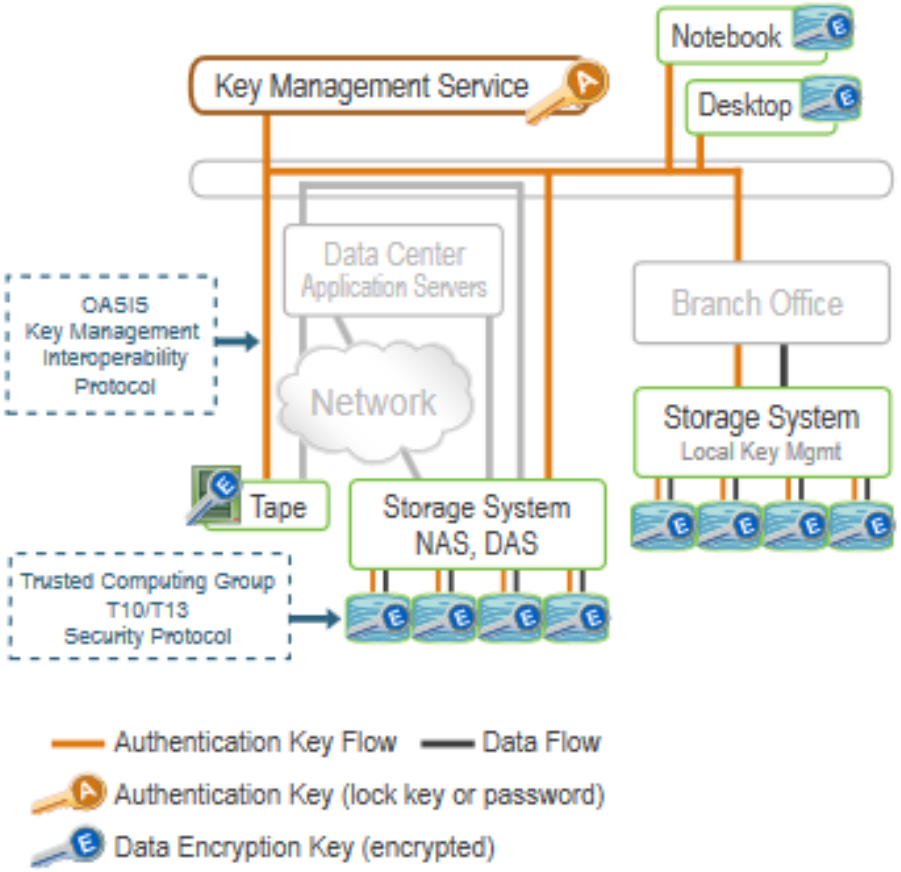
(Some of the Clients, Servers and SDK's)

* *From www.cryptsoft.com/data/DS-ALL-WEB.pdf*

Conventional Key Management Systems



Basic Key Management



Extended Key Management

Are data centers as secure as they want you to think?

* Though security is often a selling-point for many data centers, they aren't necessarily safe from theft. There have been plenty of incidents involving hardware theft from data centers.

A few examples:

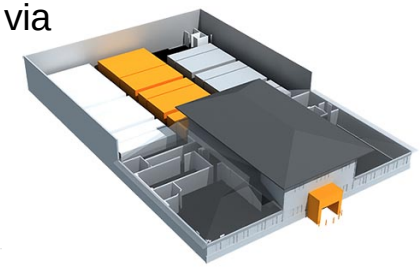
1. **Multiple robberies at a Chicago data center**
   The Chicago-based colocation company CI Host had its data center broken into on October 2, 2007. The intruders passed through a reinforced wall with the help of a power saw, attacked the night manager with a tazer, and stole at least 20 servers. This particular data center had at that time been burglarized at least four times since 2005.
2. **Fake police officers rob Verizon data center**
   A Verizon Business data center in northern London got $4 million worth of computer equipment stolen on December 6, 2007. The "heist" was done by between three to five men dressed as police officers. They managed to gain entry to the data center and tied up the five staff members before stealing the equipment....
3. **Dept-collection bureau server with personal data for 700,000 people stolen**
   On March 21, 2008, thieves broke into the Central Collection Bureau in Indiana and stole eight computers and one database server. The stolen database server contained personal information about approximately 700,000 Indiana residents, including their social security numbers.

* pingdom.com Forget about hacking – your servers might get stolen

Simple Key Management Primary Use Cases

- Smash and Grab
  - All storage units in a data center will require a security key on boot, preventing unauthorized drive start up. Boot key insertion will be transparent to the data center operator during normal operations. Drives require a key to unlock them making stealing a drive a useless proposition.
- Instant Erase Integration
  - Delivers “end-to-end” Instant Secure Erase (ISE) support to heterogeneous/white box storage environments.
  - If tied to an user interface such as System Manager, a validated log of data destruction meeting ISO spec 27040 by ISE/cryptoerase or traditional methods could be produced on demand.

- Simple Drive transport
  - The solution can provide the ability to move a drive with data within a data center or unit, perhaps for cold data storage, with minimal IT support. Transport can be via non-secure transport even with secure data on drive



- Human Expertise Hard to Find and Keep
  - Server protection methods using human overseeing can be difficult to staff. “Guns, Guards and Gates approach” not required. $$$ savings

Simple Secure Storage Applications

Remote Storage Rack
("Neighborhood PBX")

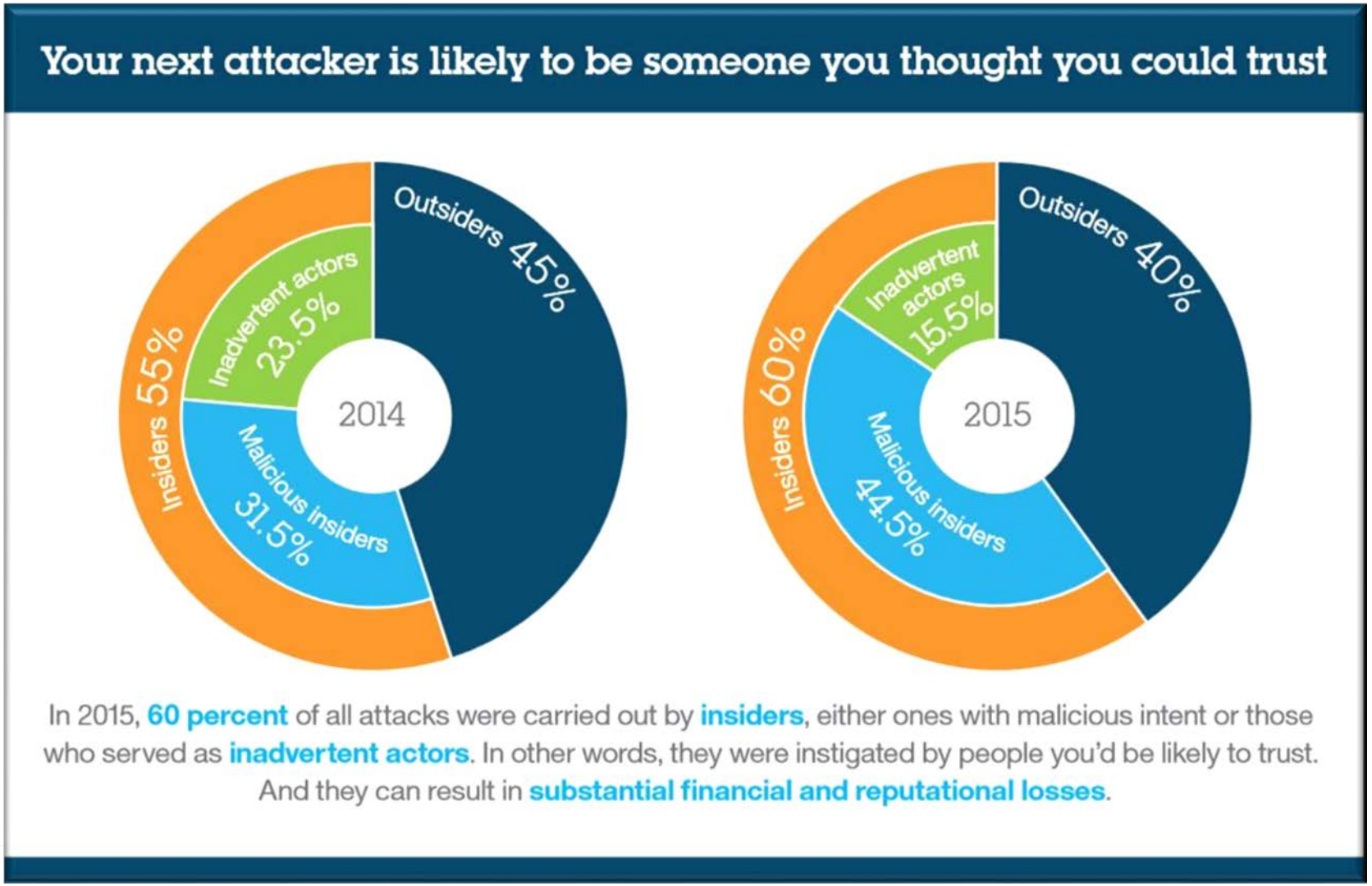
Incremental Storage Units

Storage Centers – Med Size
(Centralized CSP and Telecom)

Customer Deployed
"Local" Storage

Storage Center (Large size)

Unauthorized Access in 2015*



* Source IBM ® X-Force ® Research 2015.

A Simple Secure Solution Provides…..

"Smash and Grab" Protection with Drive and Band locking enabled

Full drive or band level locking

- **Utilizing full SED capabilities to provide full data protection at rest**
  - Requires *Key Management* to enable drive access control with drive/band locking
  - Software also manages encryption keys and security policy
- **Storage devices can leave the owner's control**
  - Nearly *all* drives leave the security of the data center
  - And the majority of retired and failing drives are still readable
- **Solution addresses regulatory requirements around data privacy**
  - Proof of encryption provides a "safe harbor" for disclosure requirements
    - Eliminates expensive costs related to public disclosure
    - Overcomes FINANCIAL, LEGAL, and REPUTATION risk related to data loss or theft
  - *Plus*, base instant erase capabilities when drives are retired, returned or repurposed
  - Drive/band locks are individually protected
  - Allows for remote secure storage arrays.
  - FIPS 140-2 certified SED models for advanced, government-grade security

TRUSTED COMPUTING GROUP™

We Self-Certify Compliance with:
U.S.-EU SAFEHARBOR
U.S. DEPARTMENT OF COMMERCE
For Illustration Only

FIPS VALIDATED 140-2 ™

* Safe harbor definition link

SNIA DSI '16 DATA STORAGE INNOVATION CONFERENCE

How to Deploy a Secure Storage Solution Simply…..

3 Basic Examples

- UEFI Based Control With Externally Generated Keys
- Local OS Based Solution with Externally Generated Keys
- Local OS Based Solution with a Self-Contained Key Management System

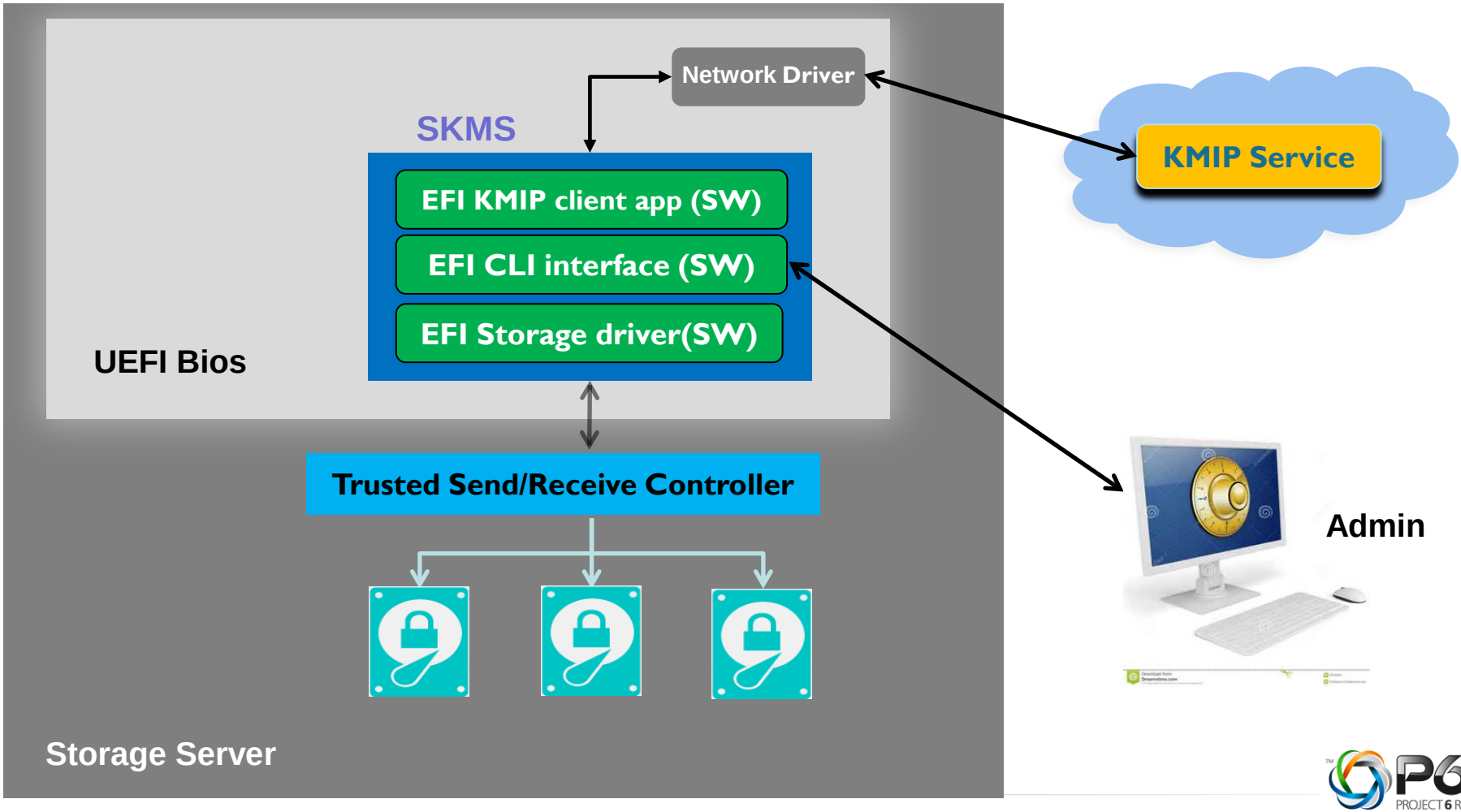
Deploying the Simple Secure Solution

Method 1

UEFI Controlled External Key Management Deployment

Simple Key Management Solution

Generic HBA controller + UEFI Bios and EXTERNAL KMIP Server



Deploying the Simple Secure Solution

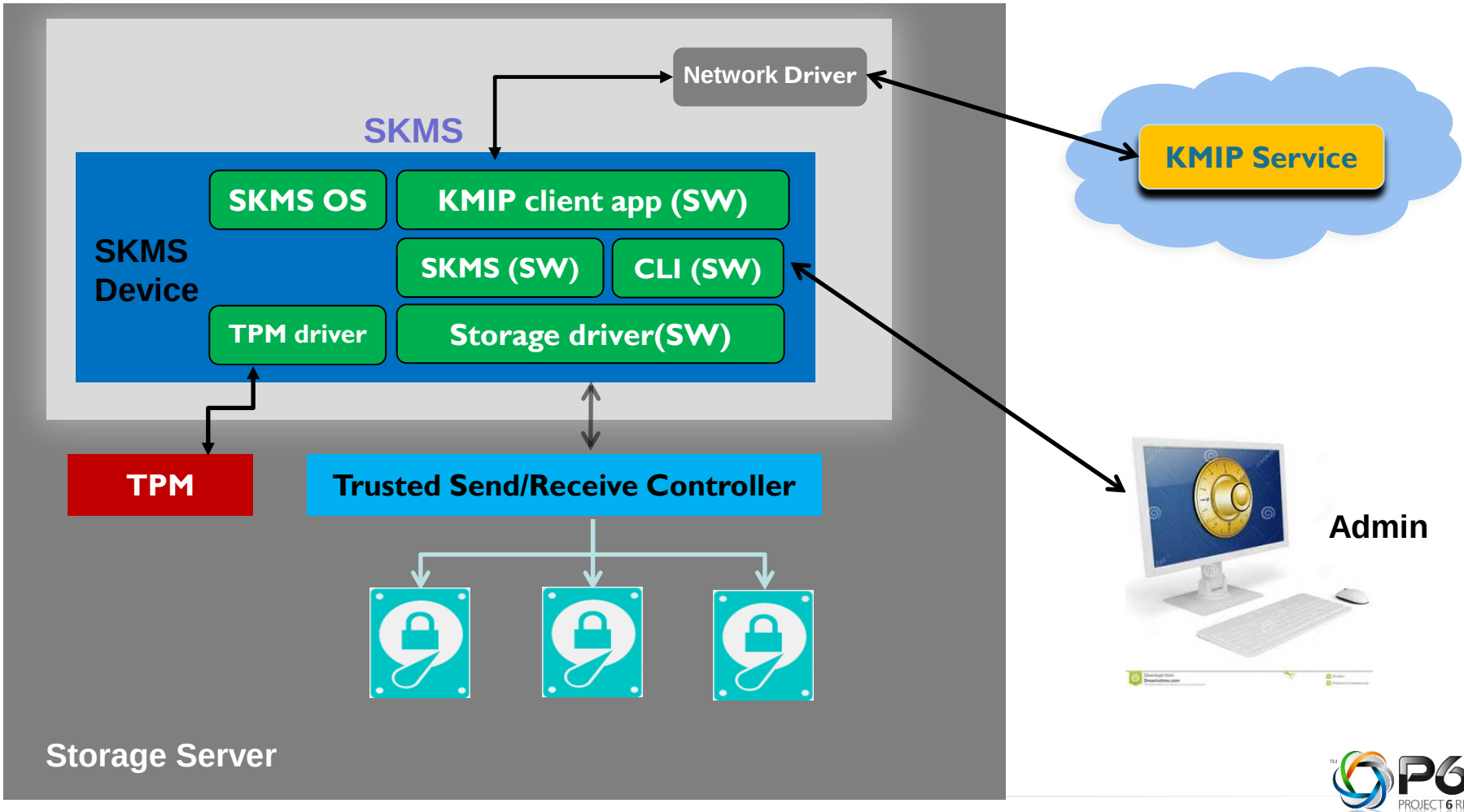
Method 2

Local OS controlled

External Key Management Deployment

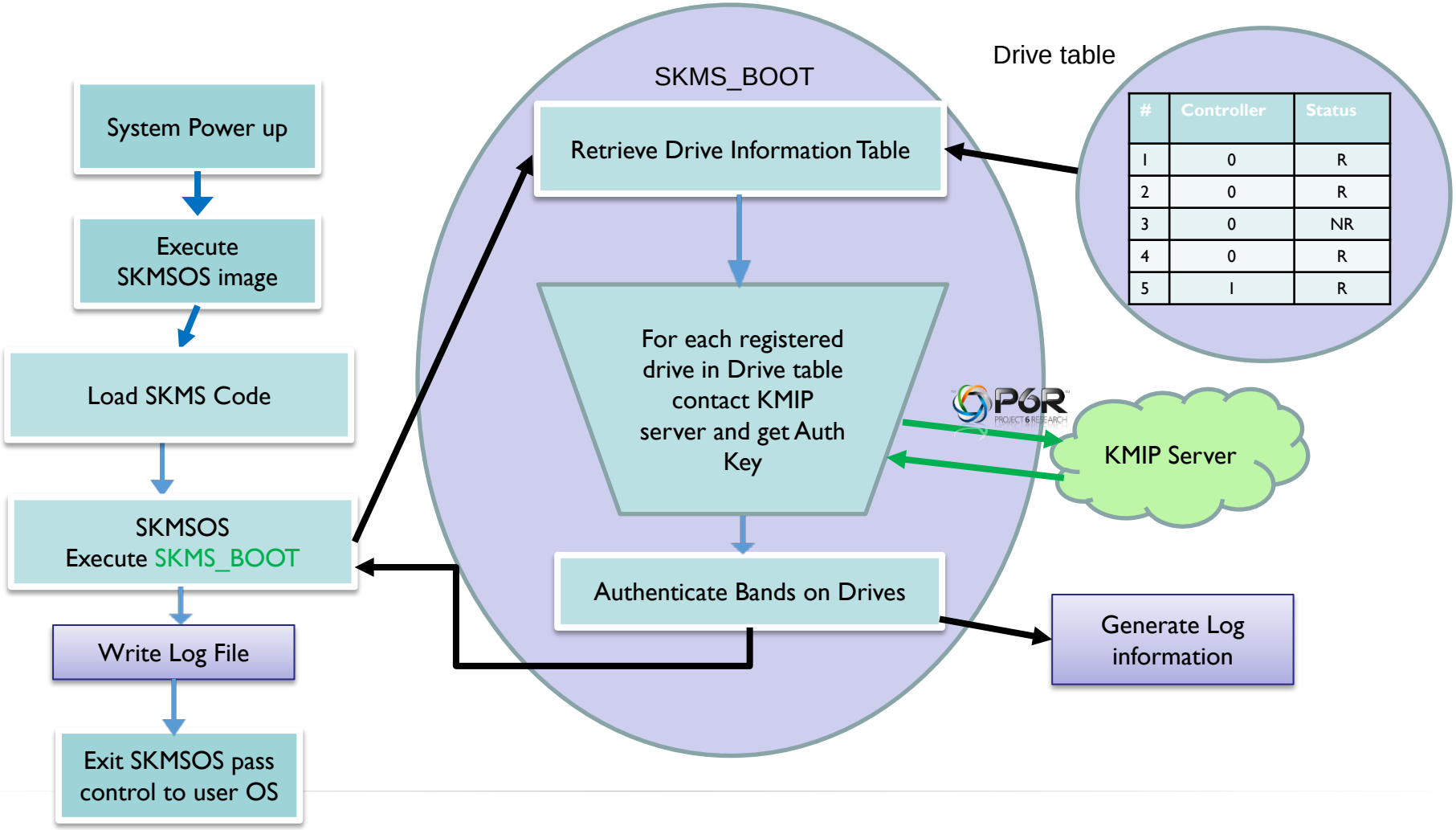
Simple Key Management Solution

Generic HBA controller + SSD or HDD and EXTERNAL KMIP Server



Simple Key Management Solution

Example startup



KMIP Interoperability

Secure KMIP Client (SKC) has gone through extensive interoperability testing against all of the leading KMIP servers

Cryptsoft C KMIP Server SDK	Cryptsoft Java KMIP Server SDK	Dell KMIP Server	Fornetix Key Orchestration Server
Townsend Security Alliance Key Manager	IBM SKLM Server	QuintessenceLabs qCrypt Server	Safenet KeySecure Sever
HPE ESKM Server	Thales KeyAuthority Server	Utimaco Key Server	Vormetric KMIP Server

Deploying the Simple Secure Solution

Method 3

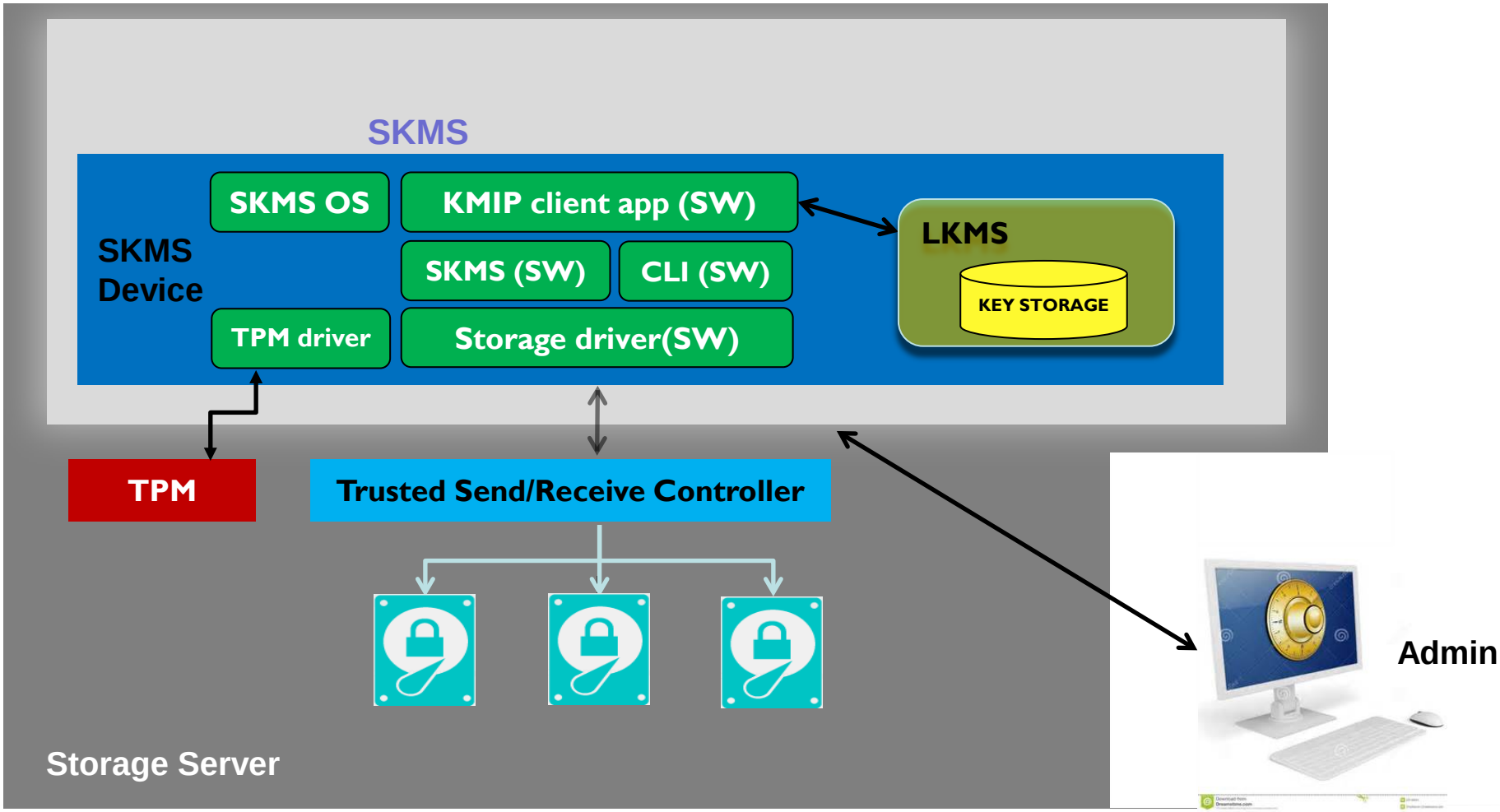
Self-Contained

Local OS Controlled

Internal Key Management Deployment

Simple Key Management Solution

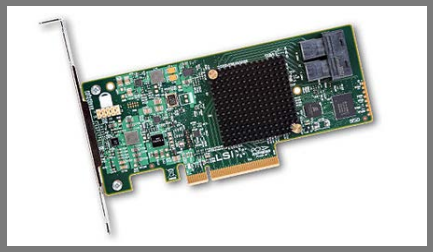
Generic HBA controller + SSD or HDD and INTERNAL KMIP Server



Seagate SKMS – Component list [Generic server Examples]

- Hardware Agnostic Solution

HBA controller with T10/T13 Security Pass Through



LSI 9300 or similar

+

SED SAS / SATA / NVME / M.2
SSD / HDD

Note:
Can be SED SSD or HDD
(SSD would also provide Drive Caching)

SNIA DSI '16 DATA STORAGE INNOVATION CONFERENCE
Innovation in Storage Products, Services, and Solutions
June 13-15, 2016 | Marriott San Mateo | San Mateo, CA

Deploying Simple Secure Storage Systems

Chris Allo

System and Drive Level Security

SEAGATE

Chris.allo@Seagate.com