

**SNIA**

STORAGE NETWORKING INDUSTRY ASSOCIATION

EDUCATION

# **Trusted Computing Group Trusted Storage Specification**

Michael Willett, Seagate Technology

# SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA.
- Member companies and individuals may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced without modification
  - The SNIA must be acknowledged as source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.

## Trusted Computing Group (TCG) Trusted Storage Specification

The Trusted Computing Group (TCG) Storage WorkGroup has published formal specifications for security and trust services on storage devices, including hard drives, flash, and tape drives. The majority of hard drive and other storage device manufacturers participated. Putting security directly on the storage device avoids the vulnerabilities of platform OS-based software security. The details of the Specification will be highlighted, as well as various use cases, including Full Disk Encryption with **enterprise key management.**



**Board of Directors**  
Mark Schiller, HP, President and Chairman

**Marketing Workgroup**  
Brian Berger, Wave

**Technical Committee**  
Graeme Proudler, HP

**Best Practices**  
Jeff Austin, Intel

**Advisory Council**  
Invited Participants

**Administration**  
VTM, Inc.

**Public Relations**  
Anne Price, PR Works

**Events Marketing Support**  
VTM, Inc.

**TPM Work Group**  
David Grawrock, Intel

**TSS Work Group**  
David Challenger, Lenovo

**Mobile Phone WG**  
Panu Markkanen, Nokia

**Peripherals WG**  
(dormant)

**Server Specific WG**  
Larry McMahan, HP

**Conformance WG**  
Manny Novoa, HP

**PC Client WG**  
Monty Wiseman, Intel

**Infrastructure WG**  
Thomas Hardjono, SignaCert

**PDA WG**  
Jonathan Tourzan, Sony

**User Auth WG**  
Laszlo Elteto, Safenet



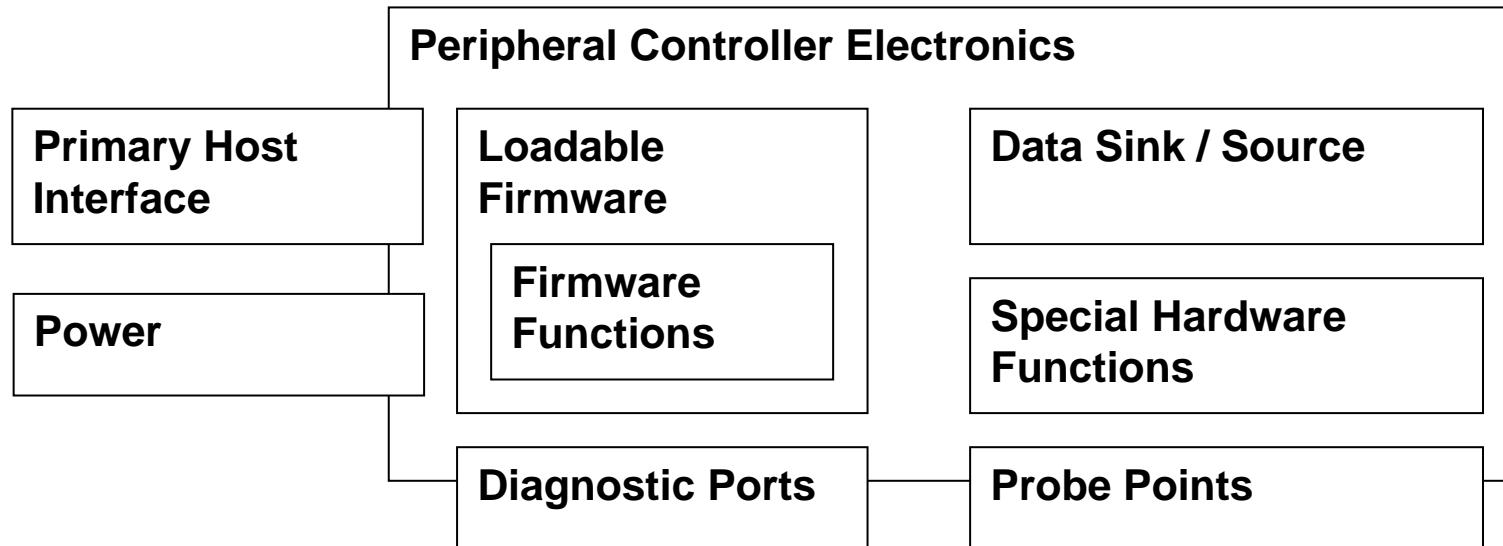
**BOLD:**  
Most Relevant  
to Storage Work

**Storage WG**  
Robert Thibadeau  
Seagate

**Enterprise Services**  
Walt Hubis  
LSI

**Storage Interface Interactions**  
James Hatfield  
Seagate

# General Risk Model: Storage



**Trust = systems operate as intended**

**Objective: Exercise control over operations that might violate trust**

**Needed: Trusted Storage commands**

# Joint Work with ISO T10 (SCSI) and T13 (ATA)

**TRUSTED SEND/IN**  
(Protocol ID = xxxx .....



**TRUSTED RECEIVE/OUT**



T10/T13 defined the “**container commands**”

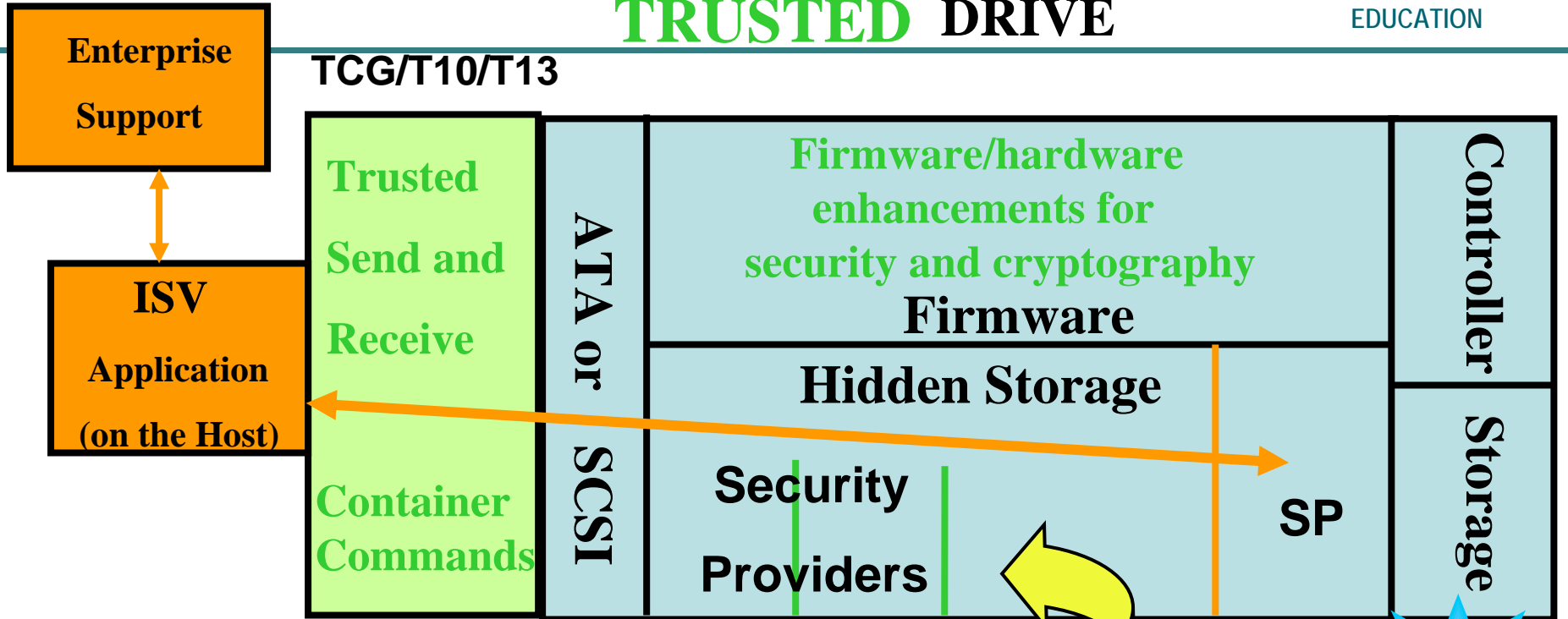
TCG/Storage defining the “**TCG payload**”

**Protocol IDs assigned to TCG, T10/T13, or reserved**

# Implementation Overview

## TRUSTED DRIVE

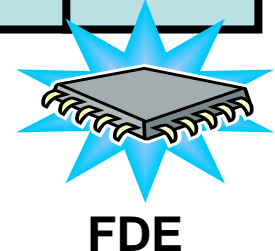
TCG/T10/T13



- (Partitioned) Hidden Memory
- Security firmware/hardware
- Trusted Send/Receive Commands
- Assign Hidden Memory to Applications

TRUSTED

Assign Hidden Memory to Applications



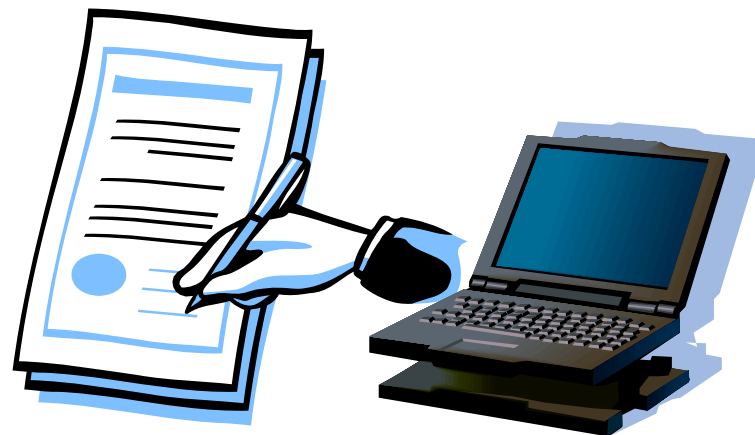


# TRUST

system behaves as designed

## Trust “Toolkit”:

Cryptographic **SIGNING**



**CREDENTIALS** (eg, signed X.509 Certificates)

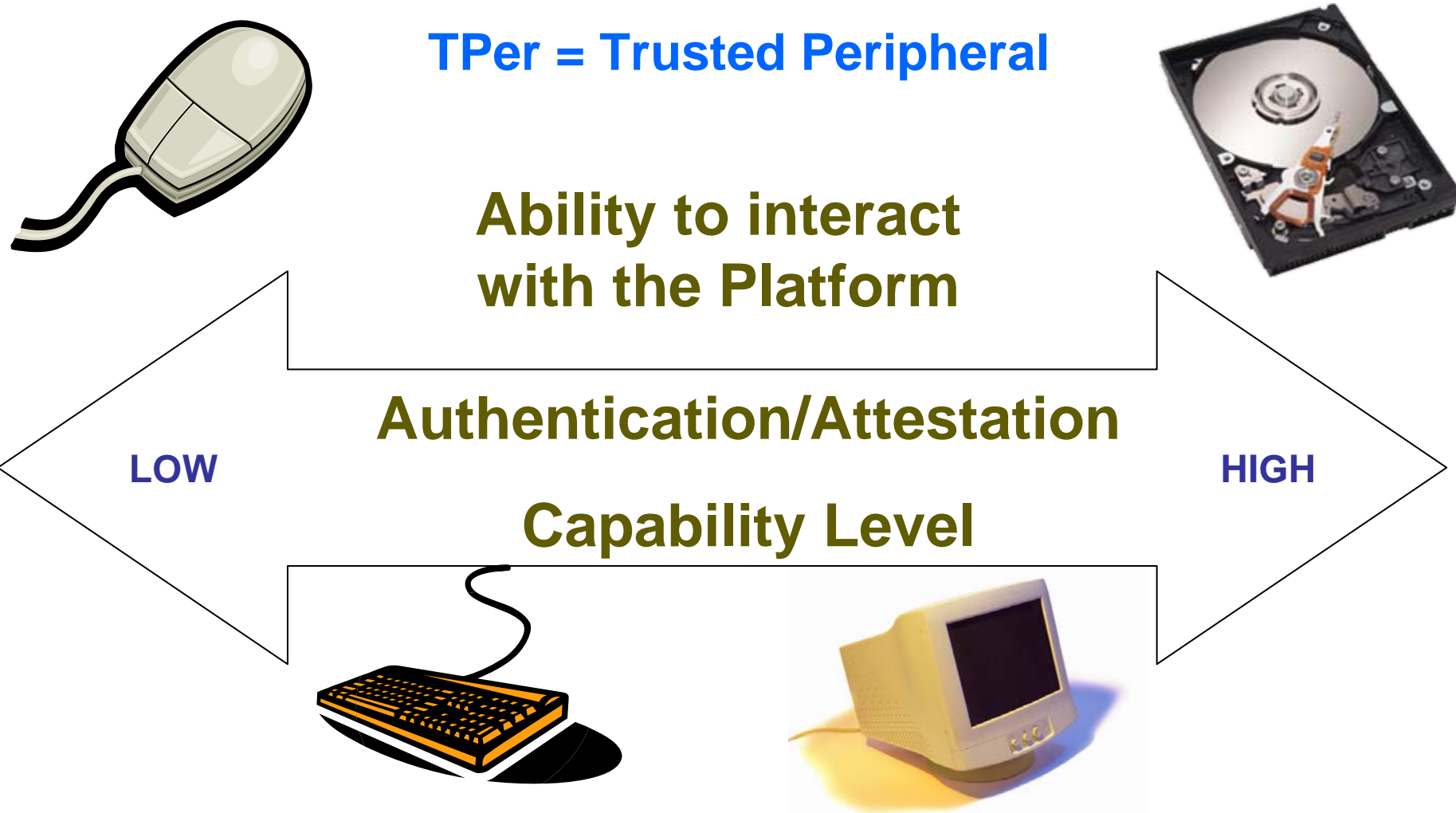


# Root of Trust

- **Hardware** that
  - **cannot change**
  - **can digitally sign**
  - and therefore initiate a **chain of trust**
- TPM (**trusted platform module**) is a tiny processor on the motherboard that can sign and whose firmware cannot be modified
- Storage Devices can be **roots of trust**

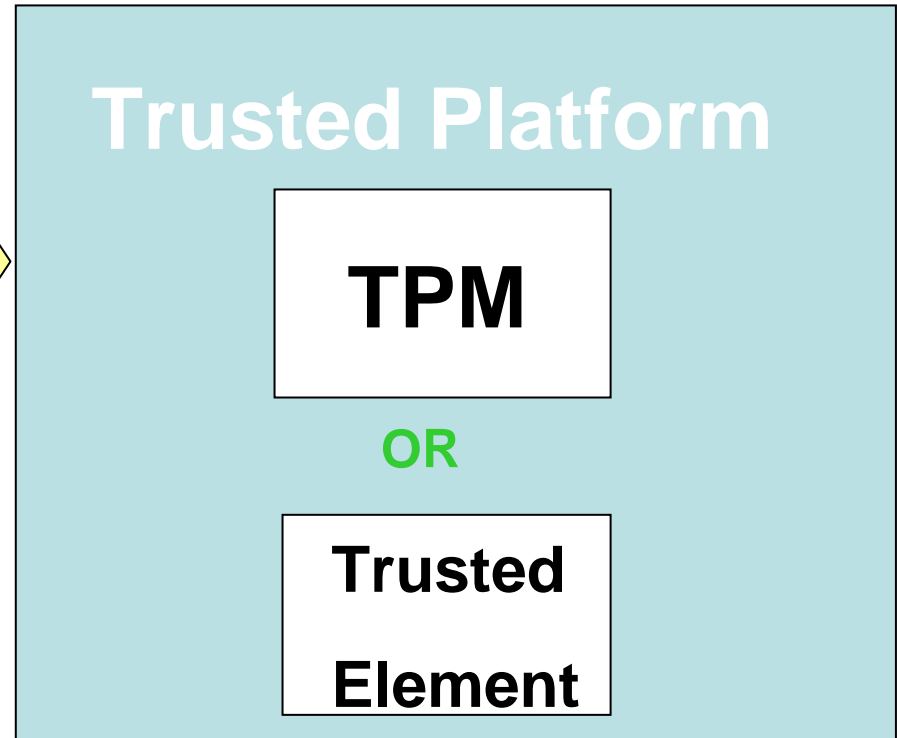
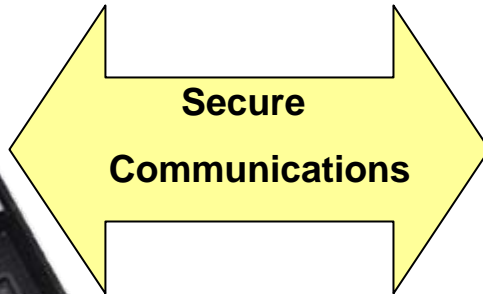
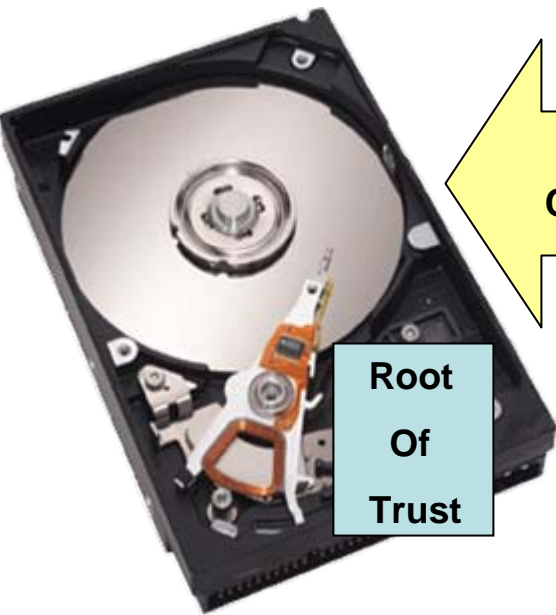


# Extending Trust to Peripherals



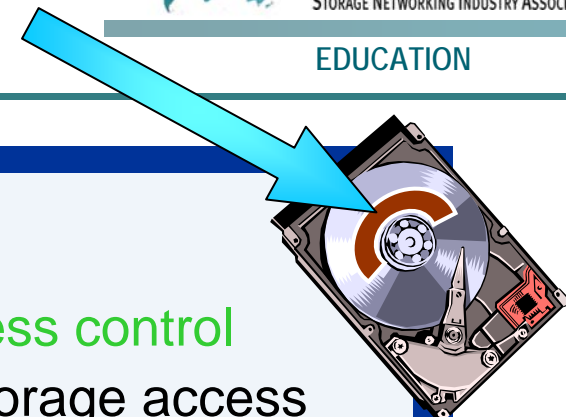
# Trusted Storage with Trusted Platform

## Trusted Storage



**Life Cycle:** Manufacture, Own, Enroll, PowerUp, Connect, Use, ...

# Why security in the hard drive



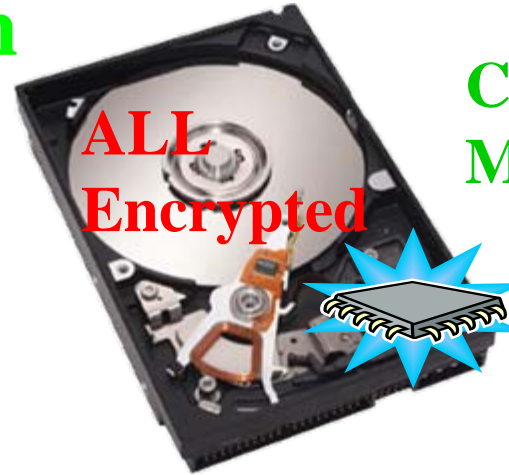
## • 3 Simple reasons

- Storage for secrets with strong access control
  - Inaccessible using traditional storage access
  - Arbitrarily large memory space
  - Gated by access control
- Unobservable cryptographic processing of secrets
  - Processing unit “welded” to storage unit
  - “Closed”, controlled environment
- Custom logic for faster, more secure operations
  - Inexpensive implementation of modern cryptographic functions
  - Complex security operations are feasible

# TCG Storage Use Cases (examples)

## Full Disc Encryption

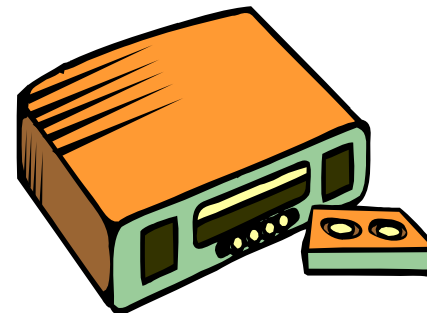
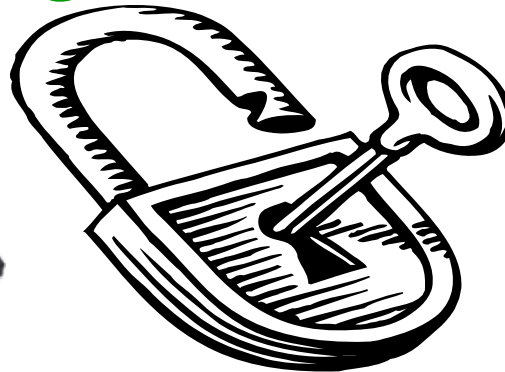
- Laptop Loss or Theft
- Re-Purposing
- End of Life
- Rapid Erase



## Crypto Key Management

Crypto Chip

## DriveLocking



## Personal Video Recorders

## Forensic Logging

## DRM Building Blocks

# Specification Overview

## TCG Storage Workgroup Specification Overview and Core Architecture Specification

**Specification Version 1.0**

**Revision 0.9**

**Q2 2007**



**Contact:**

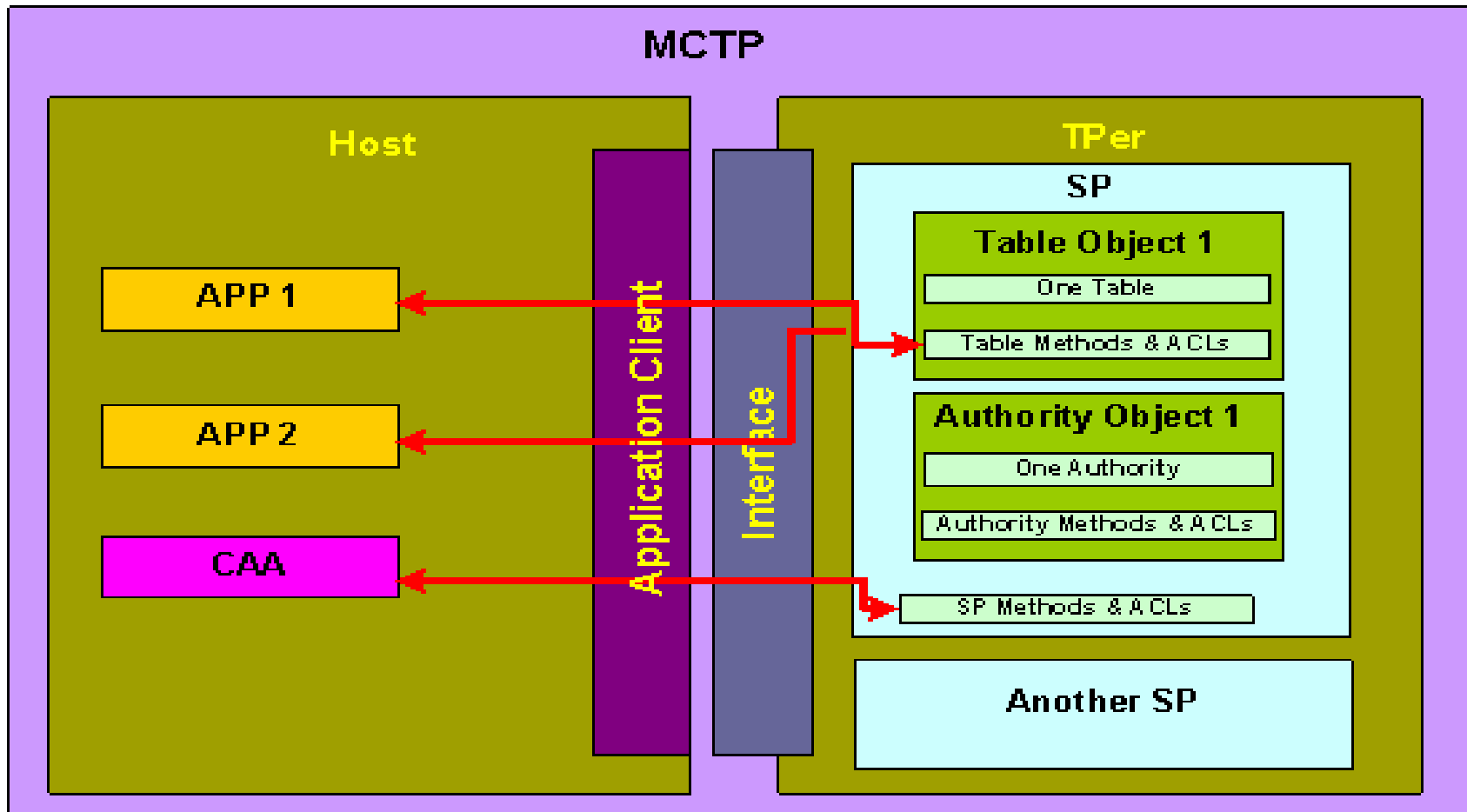
**Robert.Thibadeau@seagate.com (Chair and Editor)**

# TCG Storage WG Specification



- **SPs** (Security Providers)
  - Logical Groupings of Features
  - SP = Tables + Methods + Access Controls
- **Tables**
  - Like “registers”, primitive storage and control
- **Methods**
  - Get, Set – Commands kept simple with many possible functions
- **Access Control** over Methods on Tables

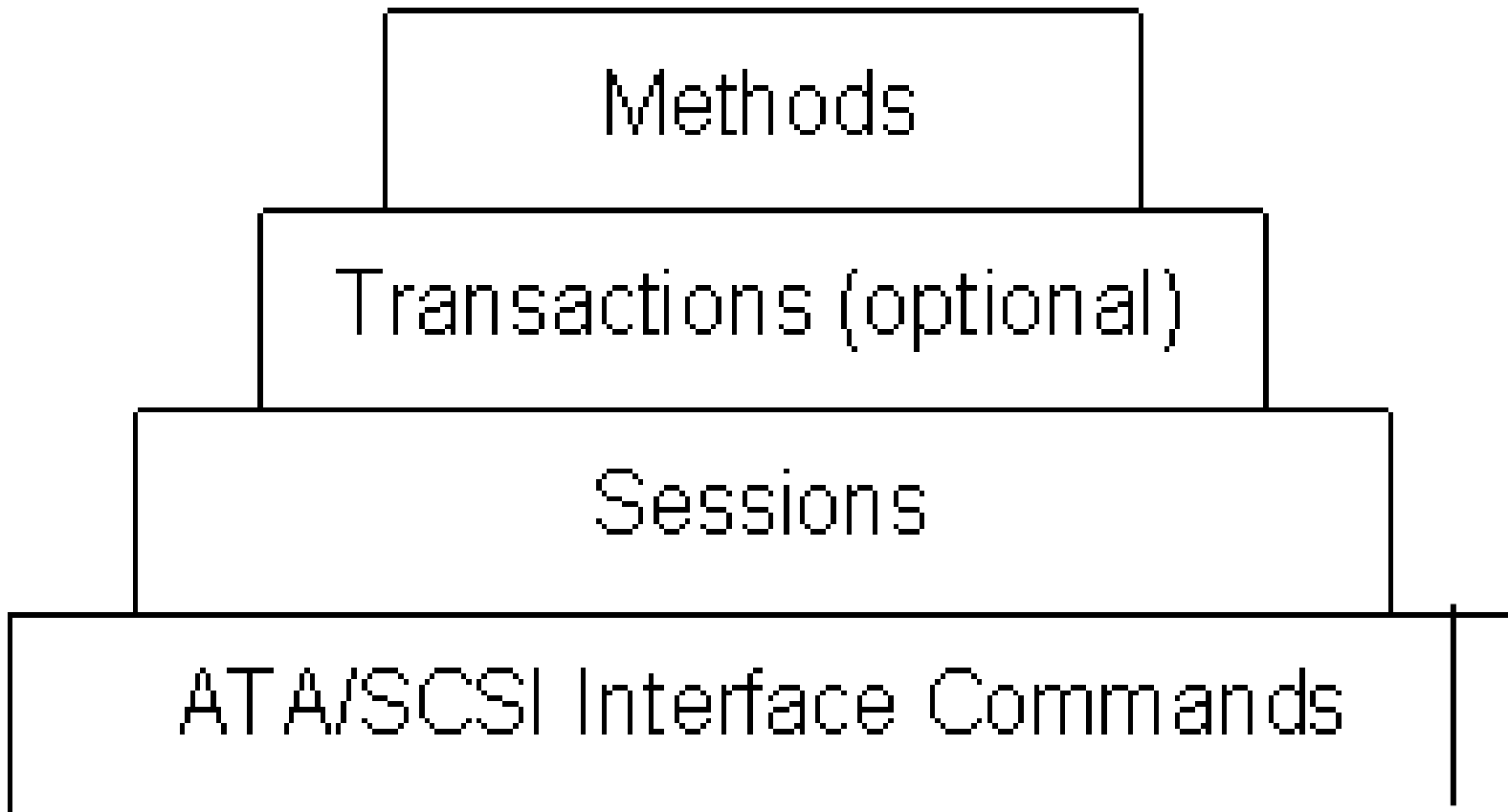
# Core Architecture



MCTP = Multi-Component Trusted Platform

TPer = Trusted Peripheral (eg, Storage)





# Security Provider (SP)

- **SPs have own storage, functional scope, and security domain**
- **Created by:**
  - 1) **manufacturer (during Storage Device creation) AND/OR**
  - 2) **Issuance Process**
- **Tables: rows = security associations, columns = related elements**
- **Persistent State Information**: remains active through power cycles, reset conditions, and spin up/down cycles
- **Methods** are actions such as: table additions, table deletion, table read access, and table backup
- **Authorities** are authentication agents. Authorities specify passwords or cryptographic proofs required to execute the methods in the SP
- **Access Control Lists (ACLs)** bind methods to valid authorities

# SP Issuance & Personalization Overview

## Issuance Server



**Issuance** is the act of creating a new SP (exchange/validation of credentials)

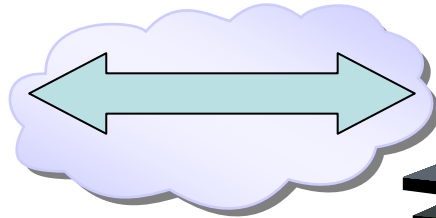
**Templates** define the initial tables and methods. All SPs = **Base Template** tables and methods + other Templates: **Admin Template, Crypto Template, and Templates for Forensic Logging and Locking/Encryption etc**

**Personalization** is the customization of a newly created SP: modify initial table data and/or admin authority, customization of the default access control settings

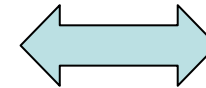
**Note: Admin SP** manages Templates, creates other SPs under issuance control, and maintains information about other SPs and the TPer as a whole. Admin SP cannot be deleted or disabled.

# Issuing an SP

Issuance Server



ISV application



REQUEST



ISSUANCE CREDENTIAL



(SESSION)



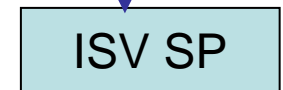
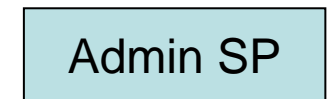
ISSUE SP



PERSONALIZE SP



USE SP



# Crypto Template



01100110110010101

- Cryptographic methods: utilize public and symmetric key store tables
- Credential tables + additional tables provided by Base and other Templates
- Encryption, Decryption, Signing, Verifying, Hashing, HMAC, and XOR
- AES, RSA, SHA, HMAC, Elliptic Curve, Random Numbers

# Host Interface: Packetization

ComPacket



Packet



SubPacket



Token



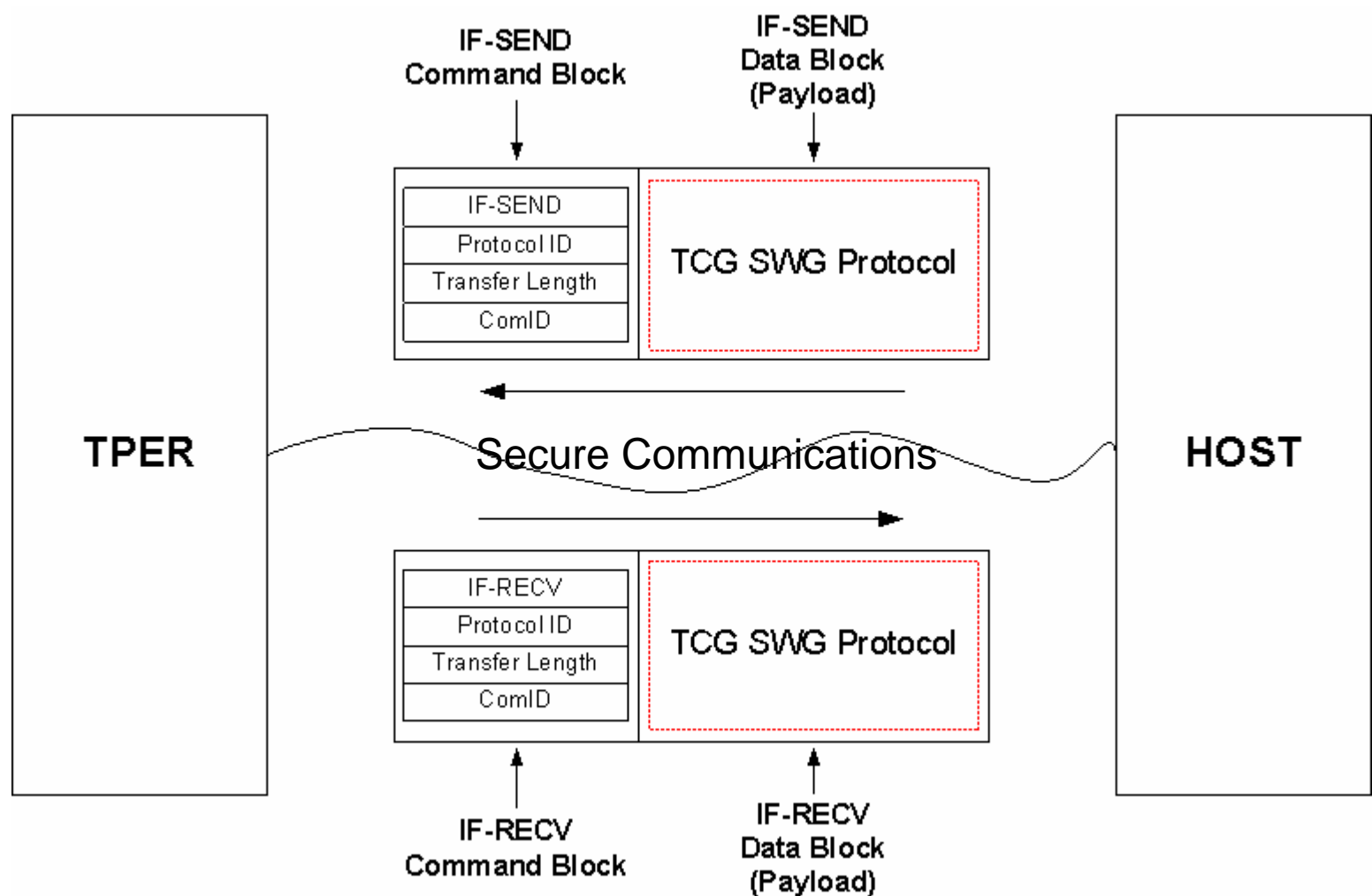
**ComPacket** is the **unit of communication** transmitted as the payload of an Interface command. A ComPacket is able to hold multiple packets in its payload.

**Packet** is associated with a **particular session** and may hold multiple SubPackets.

**SubPacket** may hold **multiple Tokens**.



# Storage-to-Host Communications



**ComID: allow TPer to identify caller of IF-RECV command**

# Access Control

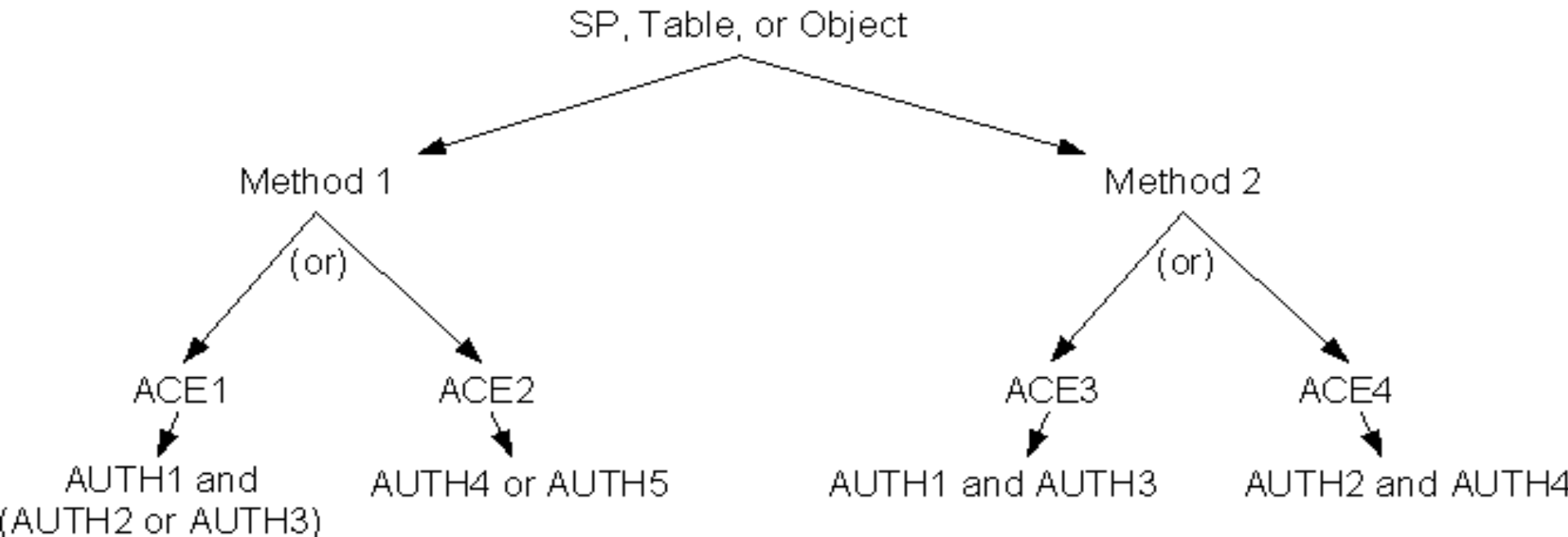
**Credentials:** Permission “secrets”

**Authentication Operation:** proof of knowledge of a secret

The `Authority` table associates specific Credential-Operation pairs together in **Authority** objects

**Access Control Lists (ACLs):** lists of **Access Control Elements (ACEs)**

ACEs are Boolean combinations of Authorities.





# Enterprise Management of (Full) Disk Encryption (FDE) Drives



## -Enterprise Server:

Key generation and distribution

Key/Password archive, backup and recovery

## -Laptop (Application):

Master/User passwords, multi-factor authentication, TPM support

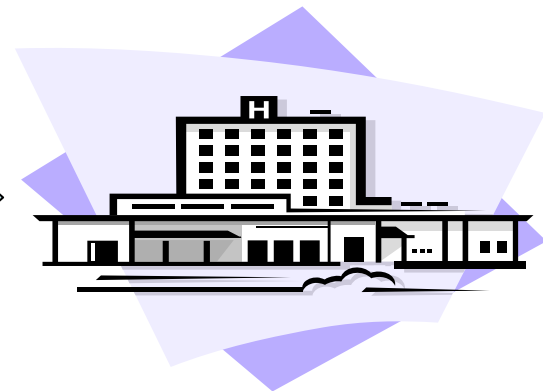
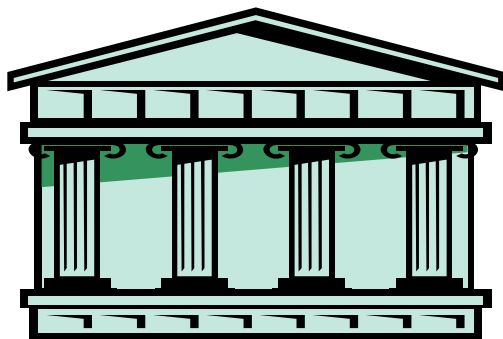
Secure log-in, "Rapid Erase"

## -FDE Trusted Drive:

Disk or sector encryption, sensitive credential store, drive locking

# Home Banking

(or, Remote Medical, or...)



Trusted Platform w/  
Trusted Storage

- Multi-factor authentication: password, biometrics, dongles
- Secure/hardware storage of credentials, confidential financial/medical data
- Trusted life cycle management of personal information
- Integrity-checking of application software
- Cryptographic functions for storage and communications security
- Trusted/secure computation of high-value functions (protection from viruses/etc)

# THANK YOU!



[www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org)

# Q&A / Feedback

- Please send any questions/comments on this presentation to SNIA:

**Security** [tracksecurity@snia.org](mailto:tracksecurity@snia.org) **LeRoy Budnik**

Many thanks to the following individuals  
for their contributions to this tutorial.

*SNIA Education Committee*

**Robert Thibadeau**  
**Jason Cox**