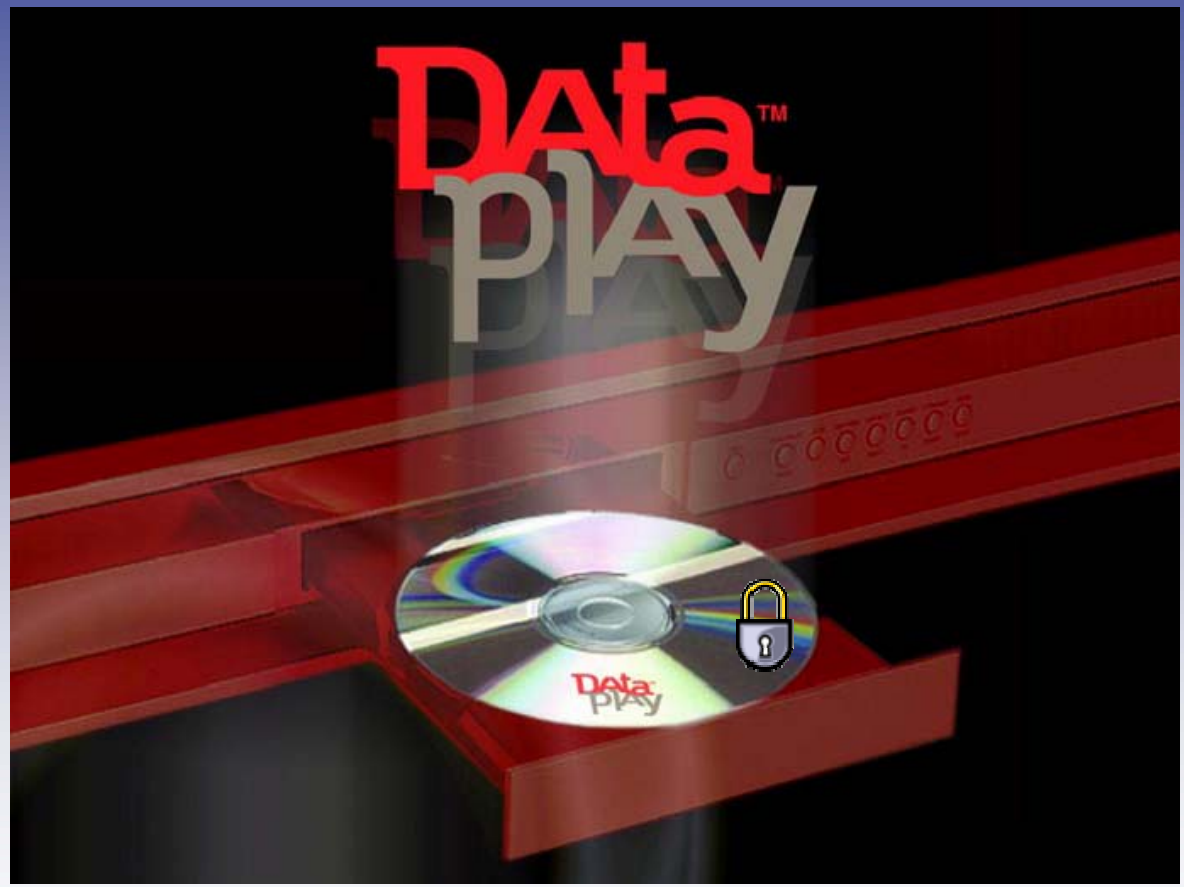
Data Protection Summit

TRUSTED COMPUTING GROUP™



Trusted Optical Disc

March 2008

DAta™ pIAy

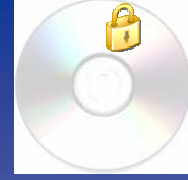
Data Protection Summit

Agenda

- TCG - Trusted Optical Disc™ mission
- Overview - 2 minute drill
- Target Features/Platforms/Markets
- Optical SSC Details

Data Protection Summit

Trusted Optical Disc Mission



- ✓ Encrypt data on standard optical discs;
- ✓ Provide access control to support organizational security policies with strong, n-factor authentication and Full Disc Encryption;
- ✓ Employ the Trusted Computing Group as a forum for critical security review, system architecture and interoperability;

- "Georgia on the mind of three million after CD loss"

  Sensitive personal information on 2.9 million Georgia residents is at risk after a company lost a CD that contained the details.

  http://www.theregister.co.uk/2007/04/11/georgia_data_loss/

- "Brown apologizes for records lost"

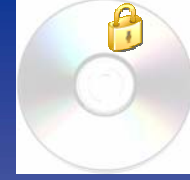
  Prime Minister Gordon Brown has said he "profoundly regrets" the loss of 25 million child benefit records. The Revenue and Customs data on the two missing discs includes names, dates of birth, bank and address details.

  http://news.bbc.co.uk/2/hi/uk_news/politics/7104945.stm

DAta PIAY

Data Protection Summit

Legislative Requirements



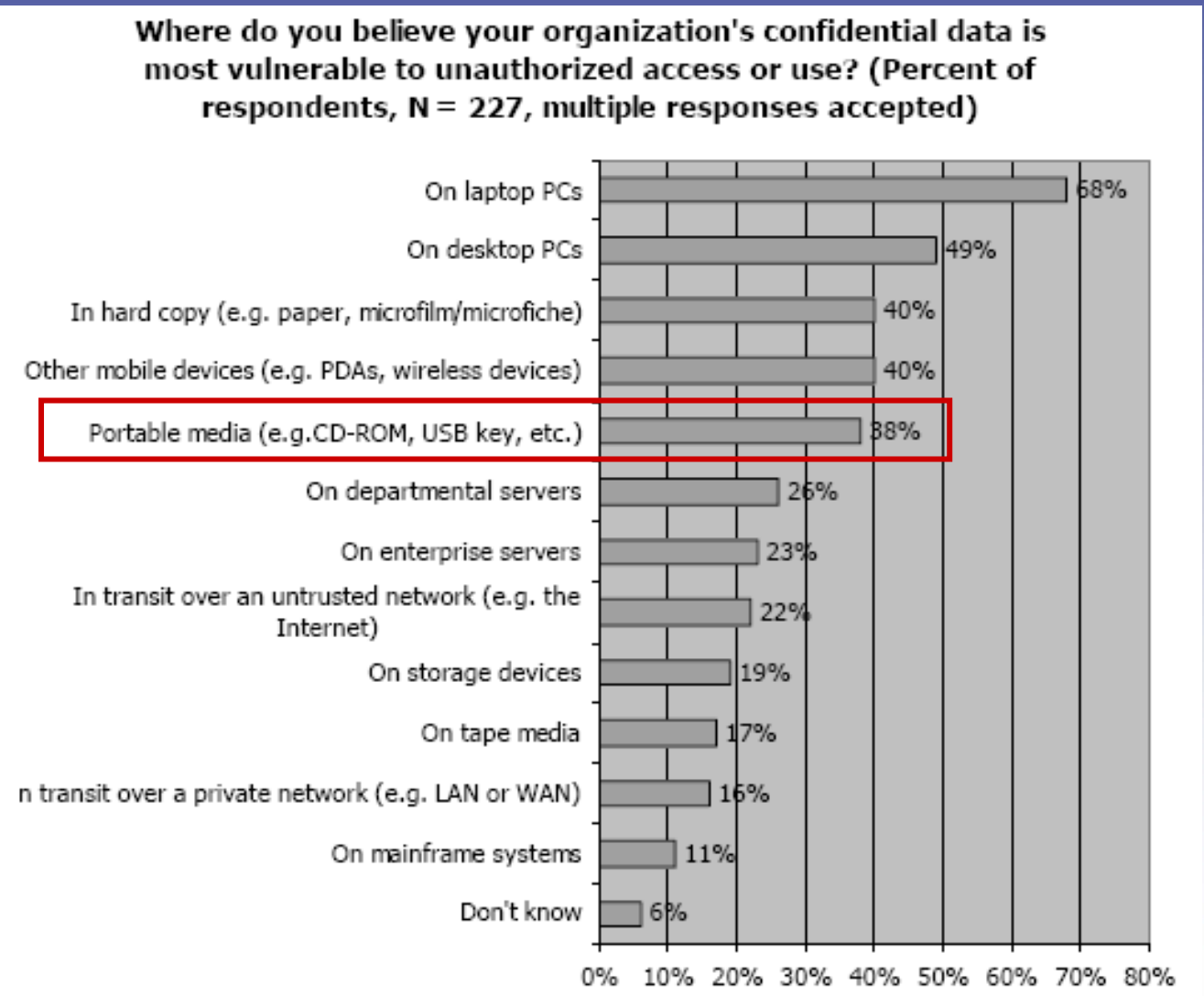
US Government Regulation concerned with Data Security

- Presidential Mandate requiring US government agencies to encrypt mobile data
  - http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf
  - "Encryption. Encrypt, using only NIST certified cryptographic modules, all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary or a senior-level individual he/she may designate in writing;"
  - "Control Remote Access. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;"
- Health Information Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley Act (SBA)
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Gramm-Leach-Bliley Act (GLBA)
- SEC Rule 17a

DAta PIAy

Data Protection Summit

Data Security Concerns

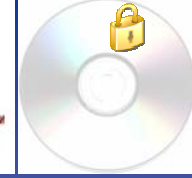


Source: TCG

Data Protection Summit

Trusted Optical Disc Overview

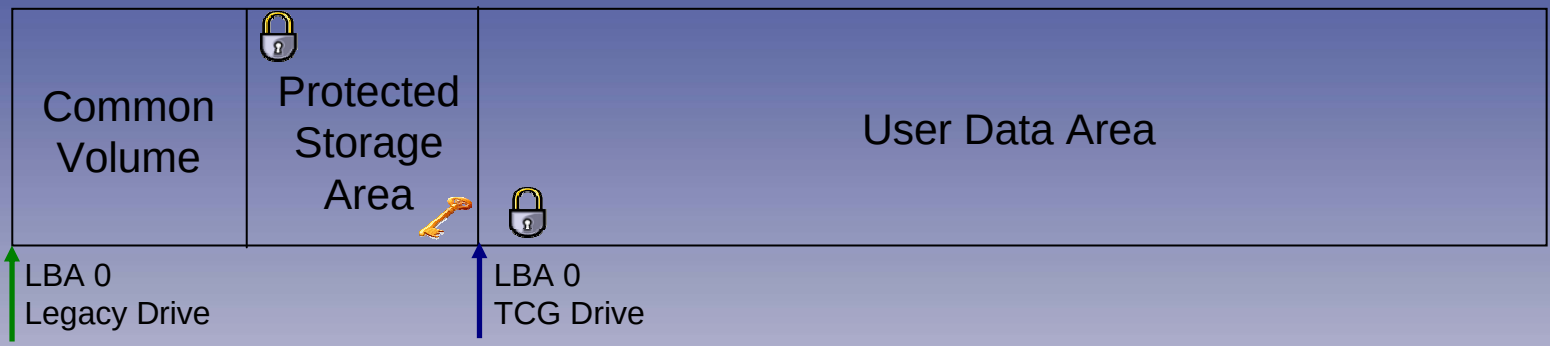
TRUSTED COMPUTING GROUP™



- ✓ **Trusted Optical Disc provides 2 key features:**
  - ✓ **(1) Access control**
    - ✓ Support organizational security policies with strong, n-factor authentication
  - ✓ **(2) Full Disc Encryption (FDE)**
    - ✓ AES Data Encryption
- ✓ **Trusted Optical Disc is compatible with all existing Optical Disc Formats**
  - ✓ Supports all writable disc types
    CD-R, RW, DVD +/-R/RW, HD-DVD –R/RW, Blu-ray R/RE
  - ✓ NO change required to physical format

DAta™ pIAy

TCG Optical Disc Structure



- **TCG is an application layer above standard disc formats**
- **Compliant with all consumer optical disc standards**
- Address space is partitioned into Three areas:
  - Common Volume is to provide “predictable behavior” when TCG disc inserted into Legacy Drive
  - Protected Storage Area is where TCG Tables are stored
  - User Data Area is where Encrypted User Data is written

Data Protection Summit

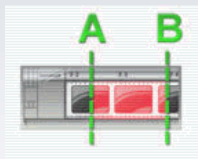
TCG is not Copy Protection

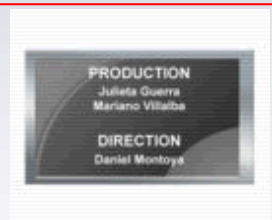
TCG	AACS
Prevent unauthorized access	Prevent unauthorized copying
Once authorized, copy is OK	Authentication is part of revocation
Data decrypted at device	Data decrypted in host player
Limited number of users, each disc may have a unique collection of users	Billions of pre-positioned 'users'

Life Cycle of a Movie

Capture → Production → Distribution → time

TCG | AACS

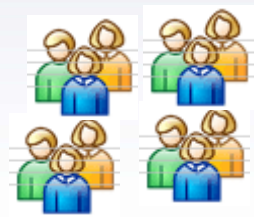







Small number of users need to copy, edit, and replicate

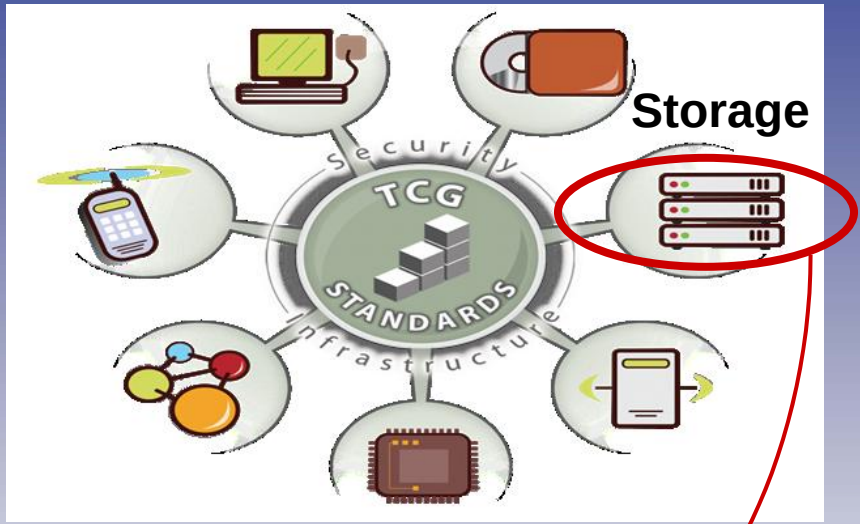


… 000,000,000's of users; copy is restricted

DataPlay

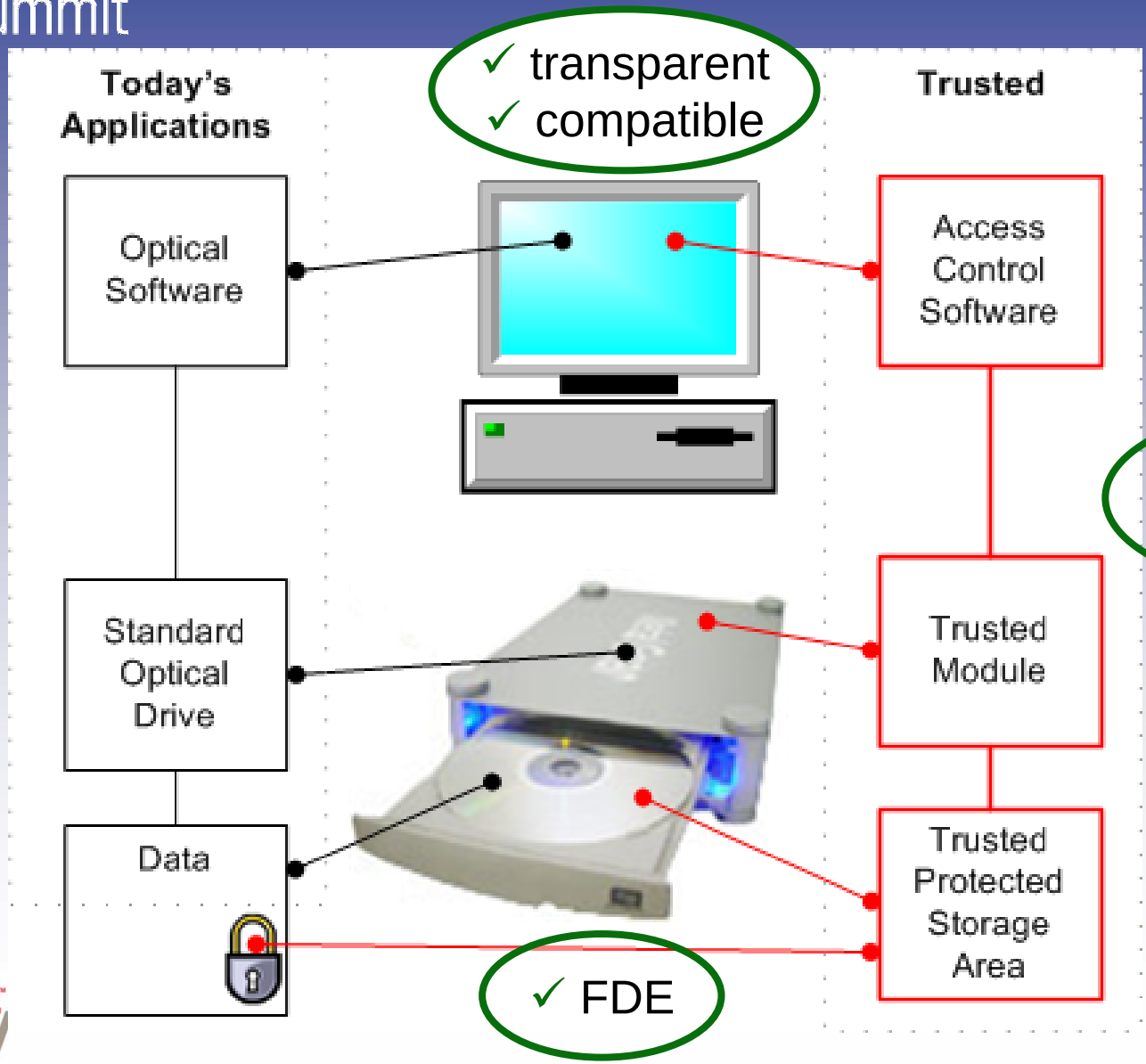
Data Protection Summit

TCG Storage Work Group



- Storage Architecture Core Specification
- HDD Security Subsystem Classes
- Optical Security Subsystem Class (OSSC)

Optical SSC Goal



Separate control channel

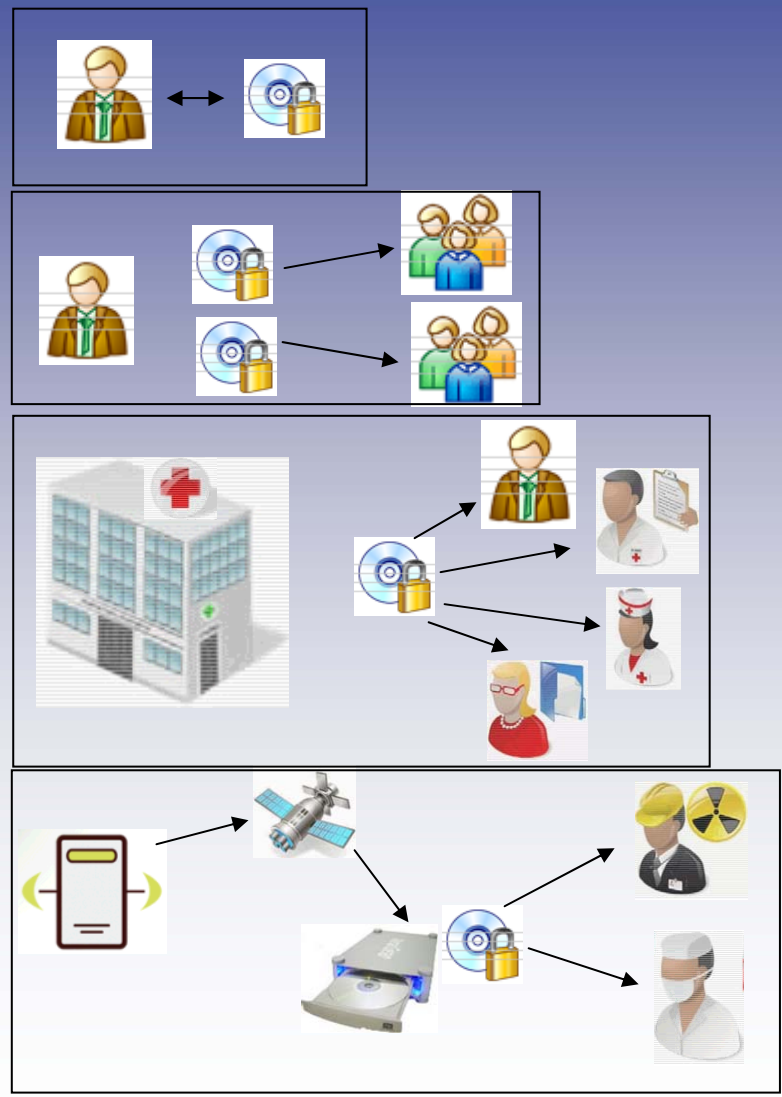
✓ ease of use
✓ unobtrusive



Data Protection Summit

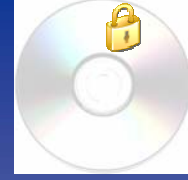
Optical Use Cases

- Simple, personal password protection for ‘sneaker net’
- Plural passwords for ‘slow mail’ distribution
- Role based access control for electronic health records
- Secure network endpoint for disaster response



Data Protection Summit

Target Features, Platforms & Markets



- Optical SSC Features
  - Strong user authentication, exactly one user at a time can connect; n-factors may be used to authenticate each user
  - Enable data path encryption in optical drive (FDE)
  - Optical drive can operate as an endpoint of a secure tunnel
  - Hardware support of organizational security policies
- Platforms
  - Any platform that uses an optical drive
  - TCG connection application is small and simple
  - Familiar optical software behaves as expected
- Markets
  - Government: Presidential mandate and NSA guideline
  - Enterprise: archival, distribution
  - Electronic health records: personal, archival and disaster response

DAta PIAY

Trusted Peripheral (TPer) Internals

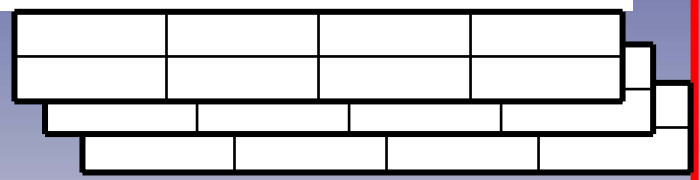
Data Protection Summit

TPer

Methods

- Set
- Get

Tables are storage elements organized as columns and rows



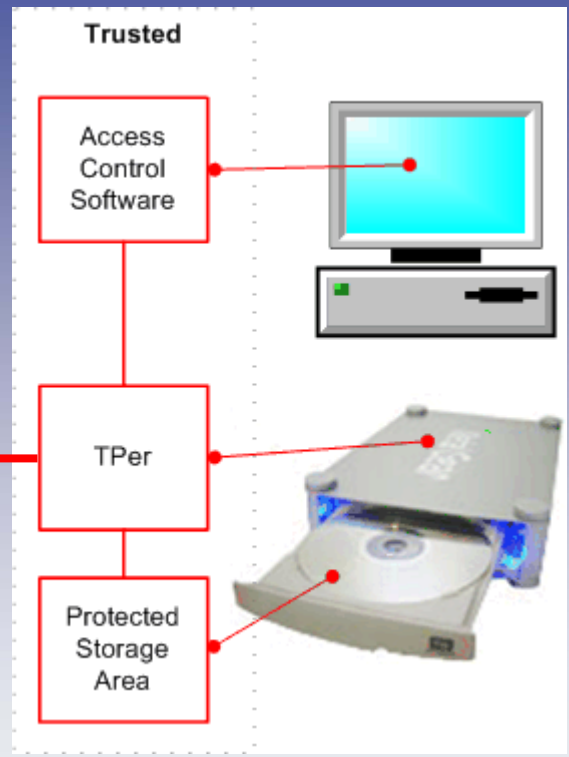
T10

SPC

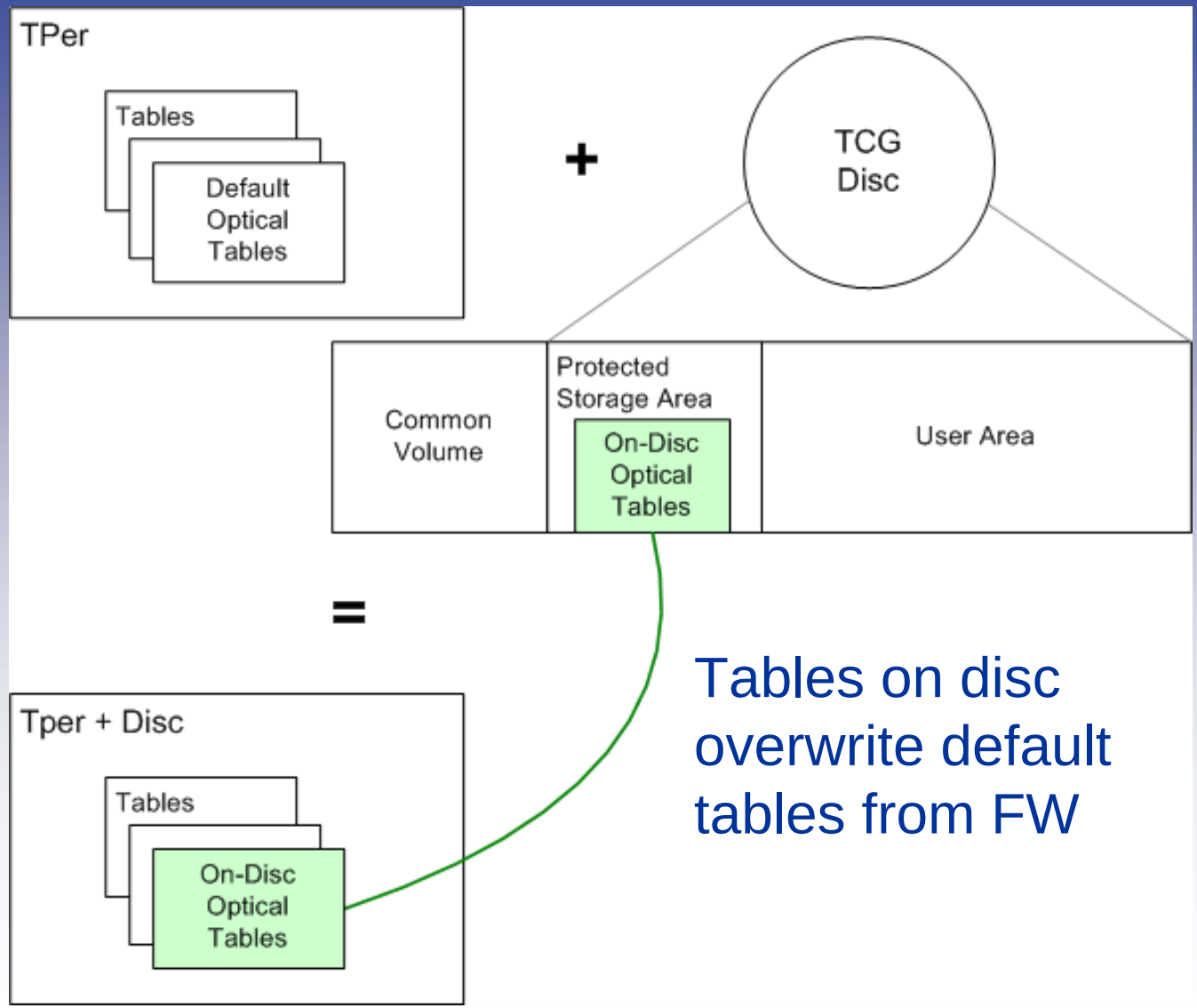
- Security In
- Security Out

MMC

- TCG feature
- TCG behavior

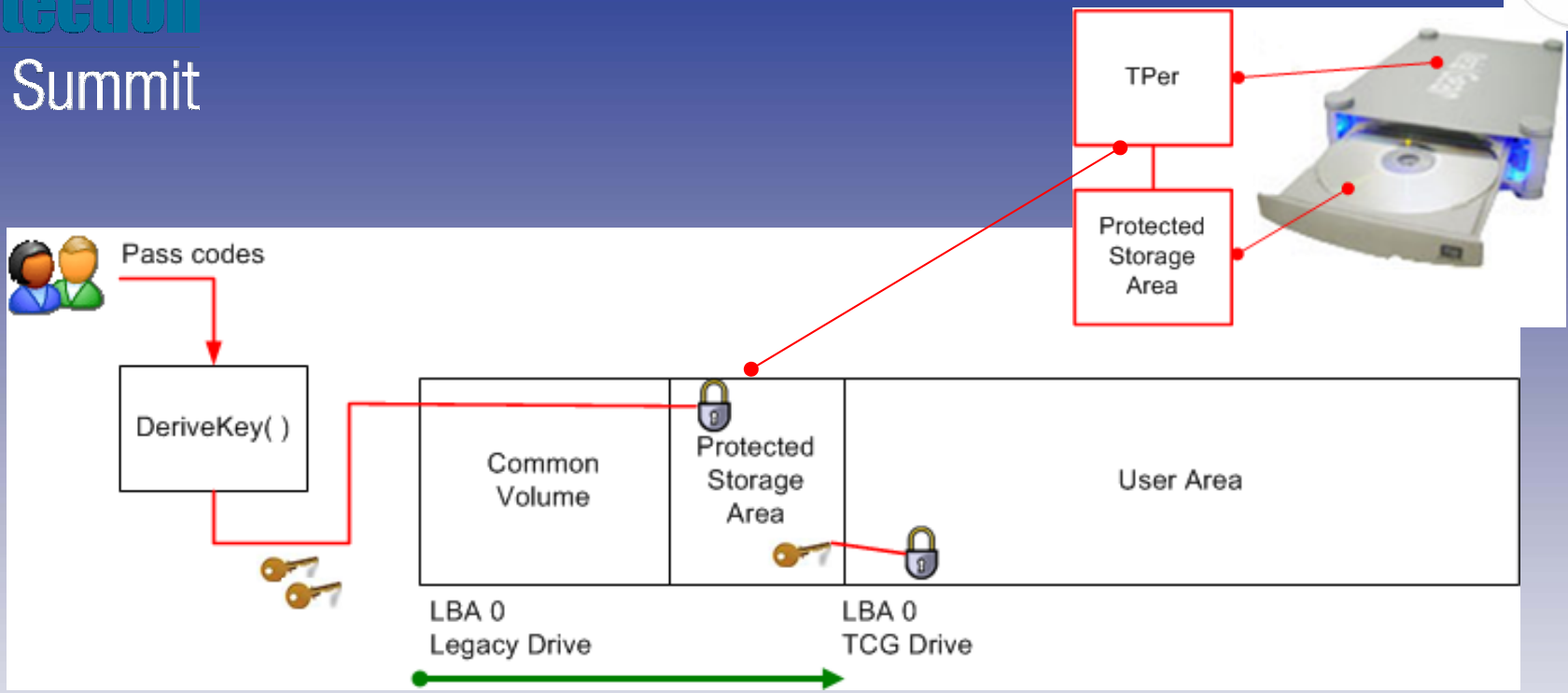


TPer Disc Behavior



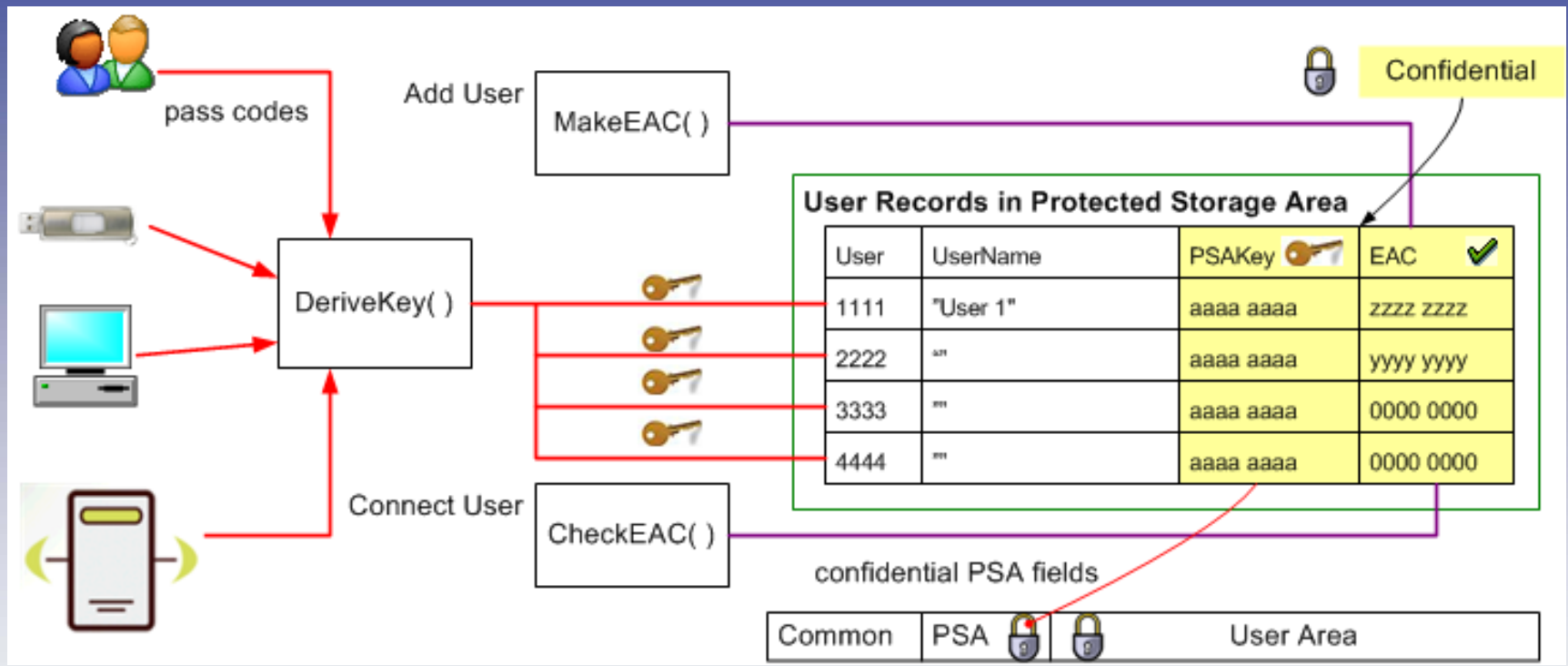
Tables on disc overwrite default tables from FW

TCG Optical Disc Structure



- Address space is partitioned into three areas
- TCG is an application layer above standard disc formats
- Compliant with consumer optical disc standards
- DeriveKey() – a cryptographic hash function that takes a pass code as input and produces an encryption key

User Authentication

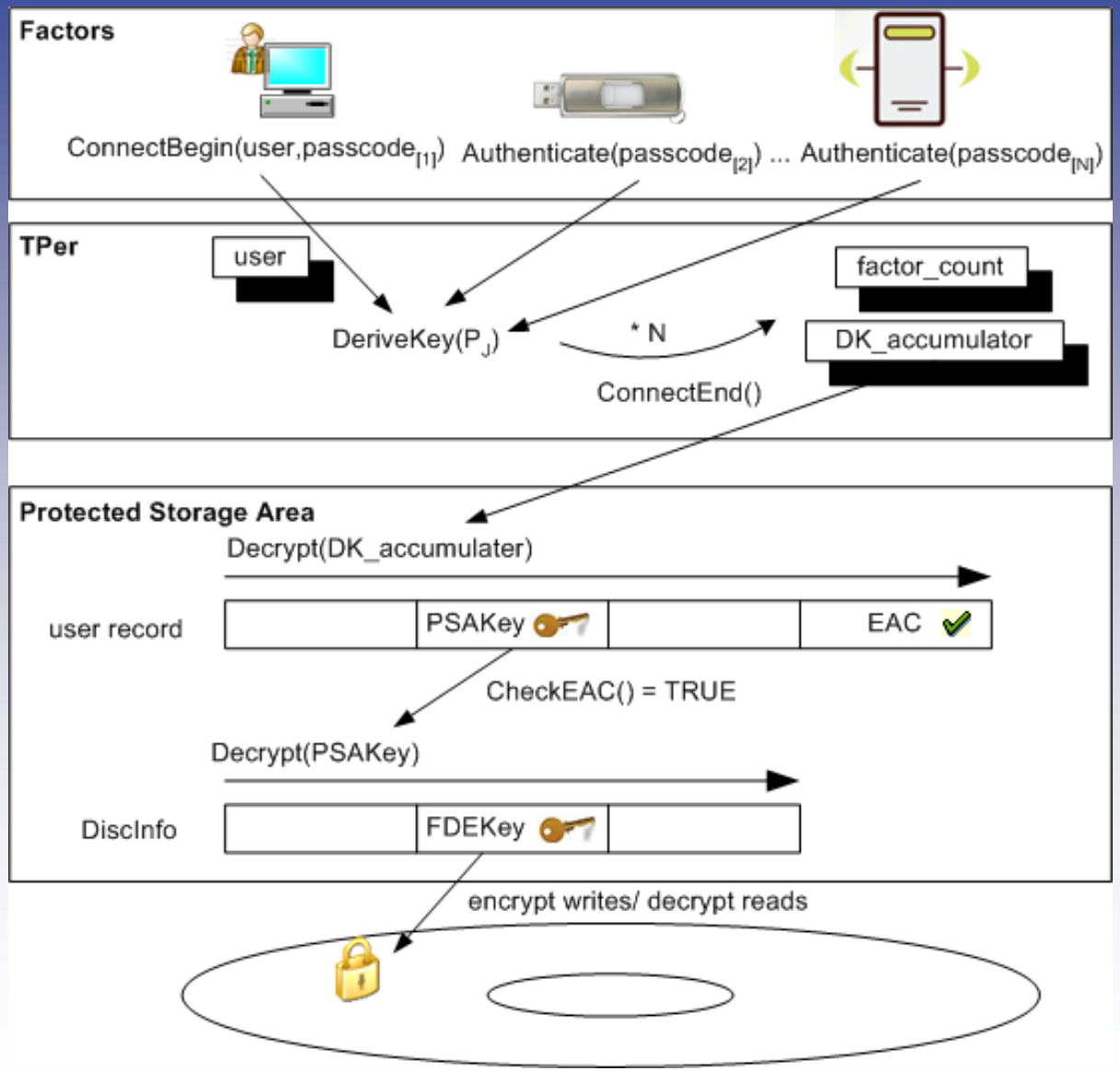


- MakeEAC() and CheckEAC() are cryptographic functions that validate pass codes.

- Multiple user records may exist, each having a different derived key that is used to encrypt the same protected area key, thereby allowing different users access to the medium even though they have different, individualized pass codes.

Data Protection Summit

N-Factor Authentication

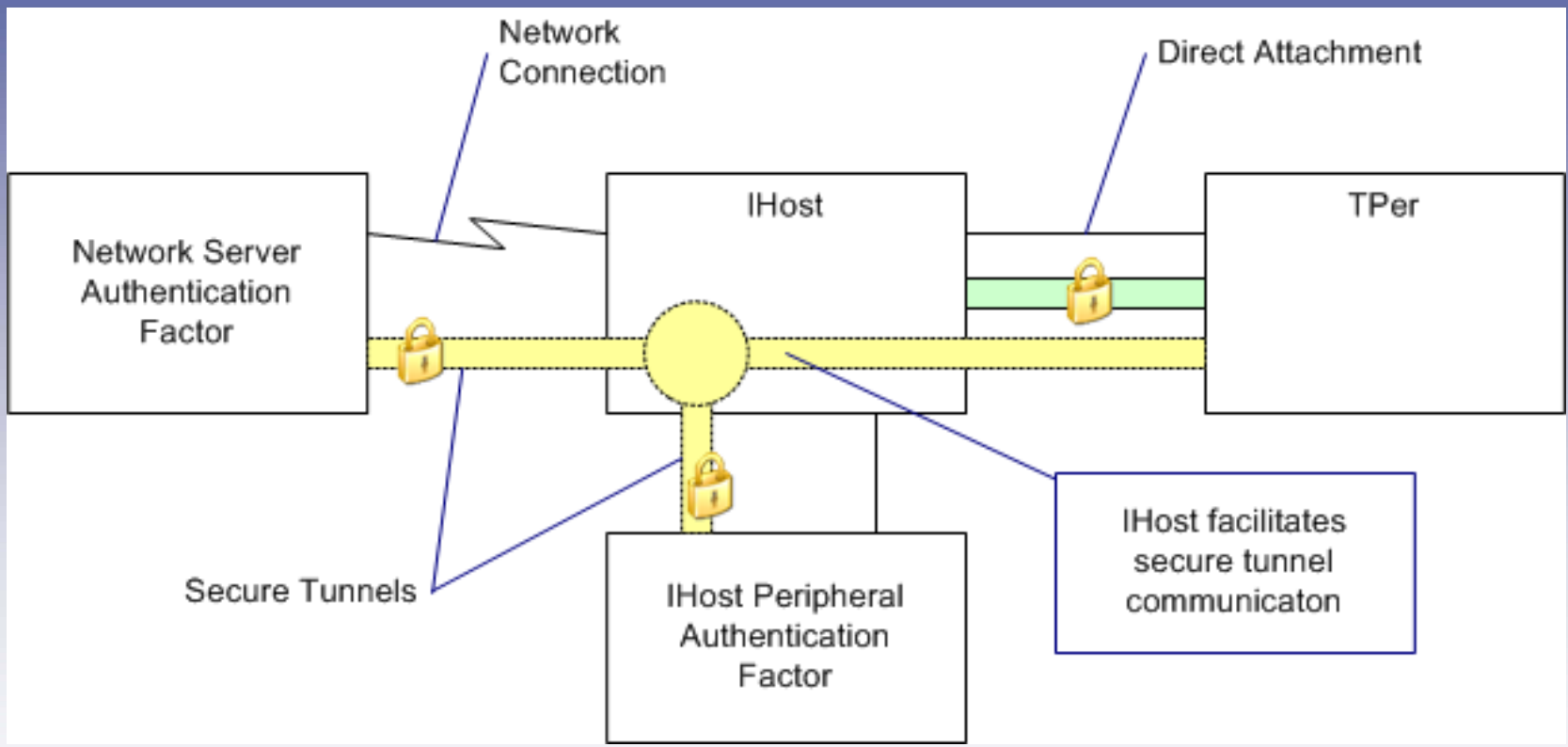


DataPlay

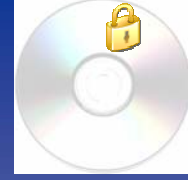
Data Protection Summit

N-Factor Tunnels:

Logical Communication Paths



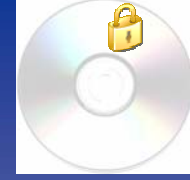
Trusted Optical Disc Authority



Trusted Optical Disc Authority serves a similar role as AACS and DVD CCA

- Certificate authority for:
  - Drives
  - Application software
  - Server software and security tokens
- Enforcement against circumvention software and devices
- Licensor of cryptographic parameters (algorithms are public)
- Licensor of device and software reference designs
- Licensor of patents, trademarks, and logos
- Registrar of applications that require OSSC metadata fields
- Compliance authority

Reference Design

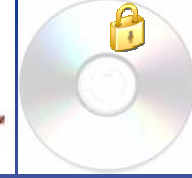


- Drive Firmware Development Kit:
  - Firmware Source Code for Optical SSC implementation
- Development Tool for Optical SSC debug and test
  - Includes Source Code
- Windows Software Client for:
  - User connection
  - Add/Delete Users
  - Administrative management (initialize discs, etc.)
  - Includes Source Code
- Redistributable binary for Windows client/drive communications (Microsoft approved)

Data Protection Summit

Thank You

TRUSTED COMPUTING GROUP™



- Demand for trusted storage is here today!

- For further information contact:
  - Bill Almon: balmon@dataplay.com
  - Dave Blankenbeckler: dblankenbeckler@dataplay.com
  - Bill McFerrin: bmcferrin@dataplay.com

DAta PLAY