T10 Encryption Key Management Study Group

Inputs on Security Requirements

Gideon Avida
Enterprise Requirements

• Enterprises have requirements for secure key management
  – Driven by regulators & auditors (FIPS 140-2 best practice)
  – Industry security standards (ex. VISA PCI)
  – Will continue to get more stringent in 2006

• Secure key mgmt is required for both tape and disk
  – “Tapes falling off the truck” not the only issue
  – Solutions must be robust to insider threats (FBI: 50-80%)

• Current T10 proposal must be expanded to address these requirements
Example: VISA Security Requirements

Visa U.S.A. Cardholder Information Security Program (CISP)
Frequently Asked Questions

CISP Program Overview

1. To whom does CISP apply?
CISP is directed to all entities that store, process, or transmit Visa cardholder data.

3.5 Protect encryption keys against both disclosure and misuse.
   3.5.1 Restrict access to keys to the fewest number of custodians necessary
   3.5.2 Store keys securely in the fewest possible locations and forms.

3.6 Fully document and implement all key management processes and procedures, including:
   3.6.1 Generation of strong keys
   3.6.2 Secure key distribution
   3.6.3 Secure key storage
   3.6.4 Periodic key changes
   3.6.5 Destruction of old keys
   3.6.6 Split knowledge and dual control of keys (so that it requires 2 or 3 people, each knowing only their part of the key, to reconstruct the whole key).
   3.6.7 Prevention of unauthorized substitution of keys
   3.6.8 Replacement of known or suspected compromised keys
Recommendations

• Need additional formats for secure key transport and storage
• Support for “smart” target devices that provide both encryption and key functions
  – “Generate key”
  – “Load key by reference”