SMPTE STUDY GROUP DC28.4
CONDITIONAL ACCESS & ENCRYPTION

Chuck Harrison  <chuck_harrison@iname.com>    Co-Chair
Bill McMannis    <bmcmannis@gqti.com>          Co-Chair
Phil Lelyveld    <phil.lelyveld@disney.com>     Secretary

Contact co-chair to participate

Monthly meetings at AMPTP, next one is Nov. 7
Biweekly conference call
DC28.4 E-mail reflector

19 Oct 00
INTRODUCTION & SCOPE

Title: - DC28.4 Study Group on Conditional Access & Encryption

Reality: - Content Protection (encryption/decryption)
- Conditional Access
- Key Management
- Watermarking & Fingerprinting
- Audit Trail
- And a bit more
• Studios – individually and through MPAA
• Theatre Owners
• Distribution
• Equipment manufacturers
• Security experts
REQUIREMENTS EXPRESSED TO US

Content Owners
• End-to-end security
• Renewability, upgradeability
• Traceability for anti-piracy enforcement
• Precise control of authorized use (per rental agreements)
• Worldwide compatibility
• Single inventory

Exhibitors
• Reliability & Maintainability
• Ease of use
• Flexibility in scheduling
• Multivendor interoperability
• Field reconfigurability

Everyone
• Affordable
• Early rollout

19 Oct 00
SECURITY “BAG OF TRICKS”

- Encryption algorithms for content
  AES (Rijndael), 3DES, others
- Authentication techniques
  - for people, communications, and equipment
  - may use public key certificates
- Key management
  Exchange or generate keys, secure from eavesdroppers
- Systems may be on-line or off-line
  - online: private networks, modem, internet
  - offline: smartcards, crypto tokens, disks, etc.
SOME WORK ITEMS

• Audit system for usage tracking
  • ensures every showing is logged
  • completely separate from boxoffice systems
• Standard way to specify “authorized use” conditions
• Watermarking (forensic)
  • trace distribution path and time/place of piracy
  • DCinema performance goals are very demanding
• Security within the theatre
  • must defend against possible “hackers” in booth
  • no exposed plaintext
  • tamper response: equipment “self defense”
  • maintainability without introducing security holes

19 Oct 00
DC28.4 SUMMARY

• It can be done, but needs careful execution.
  - Full-performance watermarking may be delayed.
• We have developed a fairly complete set of requirements.
  - Refinements will continue.
• Some proven cryptographic tools are available.
• We need additional input from Digital Cinema equipment designers and security experts in order to continue.
• Working Group should convene early 2001. We want participation from all sectors of the business.
STUDY GROUP DC28.4  
CONDITIONAL ACCESS

This Presentation Can Be Found In The Conditional Access/Presentations Folder
ftp://smpte.vwh.net/pub/dc28/