

**Submission of  
New Digital Outputs and Content Protection Technologies**

**September 17, 2004**  
Rev. 1.4

© Cable Television Laboratories, Inc., 2004. All Rights Reserved  
858 Coal Creek Circle  
Louisville, CO 80027-9750  
[www.cablelabs.com](http://www.cablelabs.com)

# Table of Contents

<b>1</b>	<b>BACKGROUND</b>	<b>3</b>
<b>2</b>	<b>PROCESS AND PROCEDURE</b>	<b>3</b>
<b>3</b>	<b>ELEMENTS OF SUBMISSION</b>	<b>4</b>
3.1	LICENSE TERMS	4
3.2	SECURITY OVERVIEW	4
3.3	VIDEO TRANSPORT	5
3.4	CONTENT PROTECTION PROFILES	5
3.5	KEY EXCHANGE ALGORITHMS	5
3.6	SECURITY INTERFACES	5
3.7	SECURITY PROCESSING	5
3.8	CERTIFICATE MANAGEMENT	5
3.9	REVOCAION/RENEWABILITY OF KEY	6
3.10	POINTS OF ATTACK/POTENTIAL WEAKNESSES	6
3.11	COMMERCIAL USE	6
3.12	CONTACT INFORMATION	6
<b>4</b>	<b>REVIEW CRITERIA</b>	<b>6</b>
4.1	VIDEO TRANSPORT	6
4.2	SECURITY INTERFACES	7
4.3	POINTS OF ATTACK AND SYSTEM WEAKNESSES	7
4.4	EFFECTIVENESS OF PROPOSED TECHNOLOGY	7
4.5	SECURITY PROCESSING	7
4.6	REVOCAION AND RENEWABILITY OF KEYS	7
4.7	NEW ALGORITHMS	7
4.8	DFAST/JTS/CABLECARD CONSISTENCY	7
4.9	LICENSING TERMS	8
4.10	OVERALL IMPACT ON THE CABLE NETWORK	8
<b>5</b>	<b>CONTACT INFORMATION</b>	<b>8</b>

## 1 Background

Under the Compliance Rules of the DFAST Technology License Agreement (“DFAST License Agreement”), various digital outputs and content protection technologies are allowed on Unidirectional Digital Cable Products (UDCPs), e.g., 1394/DTCP, DVI/HDCP, HDMI/HDCP, etc. Additionally, CableLabs may approve new digital outputs or content protection technologies.<sup>1</sup>

Each digital output and content protection technology review is performed in the context of a distribution network that must protect high-value content that is encrypted at the source and which must be protected throughout the network. Unlike broadcast flag technologies that serve a more limited purpose, content protection technology in UDCPs is required to maintain the integrity of a conditional access distribution network, and must not, among other things, “technically disrupt, impede or impair the delivery of services to a cable customer.”

This document outlines the general process, procedures, elements of a submission, and the review criteria used by CableLabs in analyzing such submissions for new digital outputs or content protection technologies for UDCPs. Approval of any digital output, copy protection, or encryption technologies under this program is not deemed to be approval for any use other than UDCPs, including without limitation bi-directional digital cable products, or products intended for broadcast flag approval.

CableLabs reserves the right to modify the criteria for submissions outlined herein (including, but not limited to changing the fees for output/recording approval), and the criteria under which CableLabs will review such submissions.

## 2 Process and Procedure

Any party desiring to obtain approval of a protected digital output, content protection, digital rights management, or secure recording and storage technology may submit such proposal to CableLabs at the address provided in Section 5. Complete submissions must include all information necessary to evaluate the submission in detail, and the associated submission fee posted at <http://www.cablelabs.com/udcp/downloads/2004pricing.pdf>.

Some of the minimal essential elements are included herein. Detailed documentation, generally in the form of a specification, should be provided by the proponent in order for CableLabs to perform a complete review. Where appropriate, reasonable non-disclosure restrictions may be accommodated (e.g., covering third party security reviews exposing weaknesses or vulnerable points of the proposed system). Failure to provide complete information may result in disapproval of the proposed technology, and/or delay in a response from CableLabs.

CableLabs will evaluate all submissions in a reasonable, objective, and non-discriminatory manner. Decisions will be made on the effectiveness of the proposed technology, the license terms governing the secure implementation of the technology, and other objective criteria as described herein.

If approved, the new digital output, content protection, secure recording, or DRM technology will be added to the Compliance Rules (Exhibit B) of the DFAST Technology License Agreement in the appropriate section(s), along with any accompanying restrictions or additional information on the use of the output or technology (e.g., Robustness or Compliance Rules). Approval of any particular technology under this program does not automatically result in changes to the Joint Test Suite (“JTS”) that must be used by all manufacturers to verify compliance of individual UDCP models prior to marketing such models as “Digital Cable Ready.”

After a technology is approved by CableLabs for use in UDCPs, any material or substantial changes to the technology must be submitted to CableLabs for re-approval. Material or substantial changes include, but are not limited to: 1) mapping to a new transport or media; 2) changes in the encoding or treatment of content; 3) changes

---

<sup>1</sup> See DFAST Technology License Agreement, Exhibit B (Compliance Rules) Section 2.4.4. The FCC Second Report and Order (FCC 03-225) provides that CableLabs shall make such initial determinations, subject to FCC review.

that may have a material and adverse affect on the integrity or security of the technology; 4) changes in the cryptographic method used (except where the algorithm is unchanged and only the key length is expanded); 5) changes in the scope of redistribution; and 6) any fundamental change in the nature of the technology.

### **3 Elements of Submission**

The technologies covered under this evaluation program include protected digital interfaces, secure recording and content storage and playback, and digital rights management. The specific security measures used by these technologies may vary. Additionally, different output technologies may employ transport mechanisms and protocols that require certain limitations or implementation restrictions. This section identifies several crucial elements that should be common to all submissions, but is not an exhaustive list that precludes other types of information that may be necessary for fully evaluating a particular technology. Submissions must not omit or misrepresent material specifications, facts, or other details necessary for CableLabs to conduct a thorough and accurate review of the technology. CableLabs may request additional information or clarification as reasonably necessary to fully assess the proposal. Until such information or clarification is provided, the submission will not be considered complete.

Submissions may incorporate mixed elements of protected digital interfaces, secure recording and content storage, and digital rights management technologies. In this situation, one complete submission may be sufficient for conducting the review, and only one submission fee will be charged.

#### ***3.1 License Terms***

License terms, if any, should be included with the submission. Preferably the complete, executable, license should be included. Essential terms should minimally include:

- royalty (or royalty-free)
- commitments to offer on a reasonable and non-discriminatory (RAND) basis
- Robustness Rules and implementer guidelines or checklists (see note below)
- Compliance Rules (see note below)
- Enforcement provisions (conformance or certification testing, implementation auditing, etc.)
- Approval procedures for downstream technologies and recording methods
- Change provisions (to the technology or the license terms), including change process participants
- IPR indemnity or other IPR arrangements (e.g., a patent pool)
- Warranty Provisions
- Term
- A list of known essential patents
- Authority and limitation, criteria, process, and participants required for revocation of devices or outputs.
- Compliance with applicable encoding rules.

#### Note on Robustness and Compliance Rules:

A UDCP containing any digital output or content protection technology must comply with the Robustness and Compliance Rules in the DFAST Technology license. The DFAST robustness and compliance rules are controlling for the overall UDCP product. As a result, the robustness and compliance rules in any manufacturer's technology license must not be contradictory to such rules in the DFAST license. Any proposed language to add the digital output or recording technology to the allowed outputs/ recording technologies listed in the Compliance Rules of the DFAST license should also be submitted.

#### ***3.2 Security Overview***

The security specification and documentation should include an introduction and security overview that includes:

1. An overview of the security architecture, its components (e.g., Packaging Server, License Server, Client, etc.), their functions, and key interfaces; connectivity requirements for output/security.
2. A detailed block diagram of the security architecture identifying the key components and interfaces necessary to implement the solution from end-to-end, including receiver and other media elements (PCs, storage, display, etc).

3. This overview should also clearly identify video transport options where there are alternatives in implementation. For example, video transport cipher algorithms (AES, 3-DES, etc.), and key exchange algorithms, (Diffie-Hellman, RSA, etc).

### ***3.3 Video Transport***

The security specification should include details regarding the video transport method and the specifics of how the Copy Control Information (CCI) presented by the CableCARD across the CableCARD-Host Interface is translated into the proposed environment/profile. The specification should also detail how the video transport is associated with any content protection profiles and the methods for authenticating and protecting the content protection profiles.

In addition, specifications or other technical descriptions must be provided to fully explain how the proposed digital output supports one or more video transport protocols capable of delivering all defined<sup>2</sup> audio-video services associated with a UDCP without disrupting, impeding or impairing the delivery of such services to the final display device. Such services also include, but are not limited to delivery, decoding, or display of analog and digital closed caption data, content advisory ratings, and emergency alert system messages. CableLabs will review only the transport mechanisms and protocols that are included in the submission. Technology approvals will be made on a transport-by-transport, or media-by-media basis. Submitters may re-submit previously approved technologies for approval on a different transport, and CableLabs will use reasonable commercial efforts to expedite approval of the proposed new transport, providing that the submitter provides a complete and thorough explanation of all legal and technical modifications that result from the new transport. Approval of a particular technology should not be considered a “blanket approval” for that technology on any transport.

### ***3.4 Content Protection Profiles***

The security specification should include details regarding the format and use of any digitally signed content protection profiles used in the system. The security specification should also define the structure and options that are employed in this system and all messaging and signaling needed for implementation.

### ***3.5 Key Exchange Algorithms***

The security specification should include details regarding the authentication of receiving devices, storage devices, and any devices connected thereto. The security specification should also include authentication methods of the License server, packaging server and the client. All of the session keys exchanged and the cryptographic protocols used should be well defined for a complete review. Non-encryption alternatives may also be employed, but should be explained thoroughly.

### ***3.6 Security Interfaces***

The specification should include details that completely define the security interfaces of the overall system and the creation and protection of symmetric and asymmetric keys. Detailed definitions of the security components implemented in hardware and software need to be defined so that these security interfaces can be reviewed.

### ***3.7 Security Processing***

The specification should include details that demonstrate how the keys and secrets are protected from reading and writing during the cryptographic calculations, and how the CCI, image constraint and other parameters are protected throughout the system.

### ***3.8 Certificate Management***

The specification should include details that completely define the certificate usage, methods for protecting RSA private keys, revocation methods and how certificates relate to content and the packaging/license servers. Details on

---

<sup>2</sup> See for example, ANSI/SCTE-40 2004; Section 8.1

installation, signing, chaining to the root, as well as the overall structure, validation of security, and protection against cloning of certificates should be included.

### ***3.9 Revocation/Renewability of Key***

The specification should include details on how system key revocation is accomplished, and how key renewability is accomplished.

### ***3.10 Points of Attack/Potential Weaknesses***

The specification should include reviews or threat analyses that may be available to review the possible weaknesses/threats and the trade-off versus the applied costs. Independent security reviews should also be provided. As appropriate, non-disclosure restrictions can be put in place to cover the review.

### ***3.11 Commercial Use***

The submission should include any known commercial use of the proposed output or technology, as well as any known affects on performance of devices, and interoperability issues. Submitter should provide a list of adopters (implementers) and supporters (owners, content developers, etc.), and identify any commercial relationships between the technology submitter and any content owners.

### ***3.12 Contact Information***

The submission should include the names and contact information for the security specialist and other individuals who may be contacted with questions concerning the submission.

## **4 Review Criteria**

CableLabs will evaluate all proposals in a reasonable, objective, and non-discriminatory manner. Depending on the specific output or technology submitted, criteria for evaluation will include the following:

### ***4.1 Video Transport***

- Are the methods defined for translating and delivering CCI from the CableCARD across the CableCARD-Host Interface into the proposed device environment or profile?
- A: Compressed Digital Outputs:
- Is the original digital compression system utilized on the interface, or is the signal re-compressed?
  - If recompressed, what system, profile, resolution and data rates are required?
  - If the original compression is preserved, is the full transport multiplex sent over the interface, or is the interface limited to single program streams sent after demux?
  - If the output carries the full transport stream, how does the system information (e.g., OOB data) get transported?
  - What methods are used to ensure uninterrupted flow of programming across this interface, regardless of other traffic that might be present on the interface (QOS)?
  - What is the minimum guaranteed data throughput provided on the interface?
  - What methods are used to enable delivery, decoding, or display of analog and digital closed caption data, content advisory ratings, and in-band emergency alert system messages?
  - How are analog programming services preserved seamlessly on this interface?
  - How does the interface deliver MMI screens over this interface?
- B: Uncompressed Digital Outputs:
- What is the minimum guaranteed data throughput provided on the interface?
  - How are analog programming services preserved seamlessly on this interface?
  - What methods are used to enable delivery, decoding, or display of analog and digital closed caption data, content advisory ratings, and in-band emergency alert system messages?
  - How does the interface deliver MMI screens over this interface?

## ***4.2 Security Interfaces***

- How is the security used on the video transport and how is the transport associated with content protection profiles and the methods for authenticating and protecting the content protection profiles?
- What are the key generation, key protection and key exchange methods used?
- Are there obvious areas where content is in the clear?

## ***4.3 Points of Attack and System Weaknesses***

- Can technology be circumvented somewhere?
- Where are the lowest barriers to be attacked?
- Where will the hacker attack and what resources are required?
- What are possible weaknesses/threats and what is the trade-off of security versus the applied costs?

## ***4.4 Effectiveness of proposed technology***

- Does the proposed technology adequately protect content passing through the digital output or being securely recorded or stored for later playback?
- What is the scope of content redistribution? Does the digital output or DRM technology effectively protect content from unauthorized redistribution through localization control or other geographic or user restrictions?

## ***4.5 Security Processing***

- Are the keys and secrets protected from reading and writing during the cryptographic calculations?
- Are CCI, image constraint, and other controls protected throughout the system design?

## ***4.6 Revocation and Renewability of keys***

- Does the product provide a system key revocation solution?
- Does the product provide a system key renewability solution?
- What criteria and processes are used for revocation and renewability? Who are the participants in the process?
- What is the minimum and maximum size of the system renewability message (SRM), and what format is it delivered in?
- How is the SRM generally delivered? What operational and infrastructure impacts would the revocation/renewability solution have on a cable network (including capital equipment or network upgrades that may be required)? What must a cable operator or other content distributor do to adopt the proposed revocation and renewability solutions?

## ***4.7 New Algorithms***

- What is the relative strength of the algorithm?
- What is the relative strength of authentication with respect to other technologies?

## ***4.8 DFAST/JTS/CableCARD Consistency***

- Does the proposed output/technology interfere with a UDCP device's meeting its DFAST or testing obligations? Is analog source switching or high definition pass-through required for the proposed digital output, and if so, what is the resulting impact to the JTS?
- Does the proposed output/technology interfere with OpenCable devices and interfaces?
- Does the proposed output/technology raise interoperability issues with other CableCARD devices and interfaces?
- Is the proposed interface interoperable with products from other manufacturers, or is it a proprietary or otherwise exclusive solution?
- Is the interoperability defined by industry standards (which ones) or license, or both?
- What specific changes would be required in the JTS? (Submitter should propose new PICS items and ATP modifications associated with the proposed technology.)

#### ***4.9 Licensing Terms***

- If licensable to third parties, does the license include the Robustness Rules, Compliance Rules, Conformance testing, Change provisions (to the technology or the license terms), IPR indemnity or other IPR arrangements (e.g., a patent pool), Warranty Provisions, Term, and other standard terms?
- Do the Robustness and Compliance Rules adequately cover any software being licensed with the technology?
- Does the license identify and grant appropriate rights for known relevant patents?
- How are downstream outputs and recording technologies approved by the licensor? What process is used to help ensure interoperability between technologies from different proponents?
- Is the technology offered royalty-free, or does it include commitments to offer reasonable and non-discriminatory (“RAND”) license terms? If software is part of the technology solution, does the license provide adequate software developer tools or other reasonable support for implementers?
- How do the Robustness rules fit with other licensing requirements?
- Are licensing terms compatible with and complimentary to the Encoding Rules applicable to Digital Cable Ready products?
- What license fees are required annually and on each device?
- Are the terms of use reasonable and fair?
- What is the scope of content usage rights for any proposed DRM technology?
- If not licensable to third parties, how does proponent assure the above?

#### ***4.10 Overall Impact on the Cable Network***

- What operational and infrastructure impacts would the proposed technology have on a cable network (including capital investment or network upgrades that may be required)?
- What must a cable operator or other content distributor do to adopt the proposed technology solution?

After receipt of a complete submission, CableLabs will document the reasons for approval, or disapproval, of the submission within the applicable timeframe.

### **5 Contact Information**

Should you have further questions regarding this document, please contact:

CableLabs  
858 Coal Creek Circle  
Louisville, CO 80027-9750  
Attn: Project Director, Business Relations, APS Department  
303 661-9100