



## **Complete CSS Testing on DVD-Video Discs**

By Doug Carson, Founder and Chairman of DCA & Bob Dobbin, CTO DaTARIUS Group

The purpose of this paper is to consider some of the ramifications of the presence of CSS encryption on the proper testing of DVD-Video discs. Several potential pitfalls concerning CSS are discussed, as well as some ideas on how to detect and avoid them.

CSS, which is an abbreviation for Content Scramble System, is a proprietary copy protection system which can be used to protect the video content of DVD-Video discs. When utilizing CSS, sectors of video data on the disc can be encrypted using digital keys during the mastering process. If appropriate keys are not used to decrypt the video data during the playback process, that video data will be unintelligible. In other words, the improperly decoded sectors can not be viewed.

As CSS is intended to prevent the unauthorized playback of video content, almost any error in the CSS encoding process will render authorized playback impossible. Complete testing of the CSS encoding, therefore, must be performed to ensure that the protected content will play where intended.

There are five aspects of implementing CSS on DVD where errors can cause playback failure. Proper testing must be performed to ensure that each of these potential pitfalls is avoided.

### Pitfall 1 - Flags.

Only some sectors of each movie are encrypted according to specific CSS rules. Not only must the proper CSS keys be used, but they must be applied to those sectors intended, and not the others. There are two components to each CSS protected sector: the CSS encrypted contents and a set of CSS flags, which indicates to a playback device that CSS has been applied to the particular sector. Therefore,

- Each and every DVD sector must be tested to ensure that the CSS flags are applied to sectors that contain encrypted content, and are not applied to sectors which do not.
- Each sector that has the flags properly set to indicate encrypted content must be tested to ensure that the CSS encryption has been properly applied.

### Pitfall 2 - Title Sets.

Generally, DVD-Video discs contain more than one "Title Set" of files. Each "Title" contains a complete segment of video content. For example, one disc can contain one Title which is the movie as formatted for standard screen, and another Title which is the movie formatted for wide screen. Discs can also contain additional Titles which include bonus content, director cuts, special features etc. Each Title Set is encrypted with its own unique CSS "Title Key". The Glass Mastering Encoder, which performs the actual CSS encryption, must encode the protected sectors using the proper Title Key for that sector's Title Set. These Title Keys are presented to the Mastering Encoder at mastering time. The Mastering Encoder must select the proper Title Key with which to

encrypt each Title's sectors, and also store a version of each title key in the correct locations on the DVD disc for the player to utilize in decryption. Therefore,

- Each DVD sector must be CSS tested within the context of its Title Set.
- Each encrypted sector must be tested to ensure the presence of the proper Title Key.

#### Pitfall 3 - Dual Layer.

The Title Keys which are stored within the encrypted sectors are themselves encrypted, requiring decryption with a "Disc Key" to be usable. There is one such Disc Key per disc. In addition to the data required in Pitfall 2, above, the Mastering Encoder must use the proper Disc Key when encrypting the Title Keys. The Disc Key is also stored on the disc by the Mastering encoder.

A problem arises in the case of replication of DVD-9-OTP (Dual Layer) discs, which is currently the most prevalent format for DVD-Video. Quite often the two layers of these discs are mastered separately, either on different laser recorders or on the same laser recorder at different times. Due to the fact that the CSS encryption keys are provided to the Mastering Encoder separately from the content source image, it is possible to encrypt Layer 1 with a different Key Set (Disc Key and Title Keys) than that with which Layer 0 was encrypted. The player retrieves and uses the Disc Key from Layer 0 only. Therefore in this case, the player will decrypt the CSS data on Layer 1 using the wrong Disc Key, rendering the Layer 1 video data invalid. Layer 0 will play back correctly, but Layer 1 will not. Therefore,

- The Title Keys on all sectors of both layer 0 and 1 must be tested.
- The Title Keys on both layers must be tested to be derived from the same Layer 0 Disc Key.

#### Pitfall 4 - Player Type.

DVD movie console players use different CSS flags than do PC-based DVD players. DVD discs which contain properly CSS encrypted sectors, but only have the properly set console flags will play properly on consoles, but fail to play properly in PC-based devices. The reverse is also true when the PC flag is properly set and the console flag is not. Therefore,

- The console and PC player CSS flags must be tested to ensure that they are properly set on each CSS sector, and also on each non-CSS sector.

#### Pitfall 5 - No Self-Authentication.

CSS encrypted sectors are not "self-authenticating" after decryption. In other words, there is no mechanism by which to determine whether a sector has been properly encrypted and decrypted. If the sector was encrypted improperly the result is the same as if it were decrypted improperly, that result being unviewable video. The sector address, error detection and correction values are perfectly OK on these corrupt CSS sectors, therefore these discs will test perfectly well in DVD testers and will "play" in

DVD movie players. The player is not aware that there is a problem, but the data presented to the video decoder is corrupt. Therefore,

- Each and every sector retrieved from the DVD-Video disc, after CSS decryption, must be compared to the original source sector before encryption to ensure proper encoding.

To be completely certain that CSS has been properly applied to a DVD-Video disc, replicators must test that each of the above pitfalls has been successfully avoided. The natural places to accomplish these tests are during the Electrical Testing of replicas and stampers. Currently, most Electrical Testing performed on replicated DVD-Video Discs do not adequately address the above pitfalls. For example, Pitfall 3, above, is addressed by checking that the same Title Keys are present on both layers at the layer change, but this method has assumptions gaps leading to false positives, and is certainly not complete.

The only way to completely ensure that a disc has been properly encrypted with CSS protection is to implement all the pitfall checks mentioned above.

#### *DCA Corporate Information*

*DCA, Inc. (Doug Carson & Associates) is the industry's leading provider of world class signal processing technology. Since 1988, CD and DVD manufacturers worldwide have relied on DCA's pre-mastering, mastering and verification products for optical discs, including copy protected discs. DCA's products include MIS (Mastering Interface System) V8 – supporting both CLV and CAV mastering, DDP Archiver and OptiSend – for electronic transfer of optical disc content. DCA has also been responsible for the signal processing of many special formats for the optical disc industry, including the Xbox game console from Microsoft. For more information on the company and its products, visit [www.dcainc.com](http://www.dcainc.com)*

#### *DaTARIUS Corporate Information*

*DaTARIUS is a world-leading supplier of test equipment, not just proving but also improving optical media quality through comprehensive products and services embracing process optimization. Our Analyzers and Evaluators support all formats: pre-recorded, recordable, and rewritable, and our revolutionary DaTABANK technology is fully Blu-ray disc (BD) and HD-DVD enabled. Complementing these testers: optimization, including our MF DisCo temperature regulator; and inspection, with print label, disc orientation and ident code validation. We also offer extensive training through our service and test centres worldwide. For the past 18 years DaTARIUS has been at the forefront of optical media technology with our commitment to the future of the industry and our customers.*

*For more information on the company and its products, visit [www.DaTARIUS.com](http://www.DaTARIUS.com)*

Copyright 2004, DaTARIUS and DCA, Inc. All rights reserved. MIS, DDP Archiver and OptiSend are trademarks of DCA, Inc. Xbox and Microsoft are trademarks of Microsoft Corp. All other trademarks or registered trademarks are the property of their respective owners.

