White Paper

October 2006

DELL™

BLU-RAY DISC™ NEXT-GENERATION OPTICAL STORAGE: PROTECTING CONTENT ON THE BD-ROM

The Blu-ray Disc launch will occur in 2006 with broad support from the movie, consumer electronics, gaming, and computer industries. With the majority of the major motion picture content committed to the Blu-ray Disc format, Dell believes that it is well-positioned to succeed the CD and DVD as the next-generation optical disc standard.

Major movie studios such as Twentieth Century Fox, Walt Disney, Sony Pictures, Paramount Pictures, and Warner Brothers have stated that they are trusting their high-definition premium content to the BD-ROM disc, the Blu-ray Disc read-only version. For this reason, the BD-ROM content protection system must be world-class in its quality and robustness. This system must protect intellectual property against unauthorized copying and large-scale counterfeiting. At the same time, the system must allow customers the flexibility to manage and enjoy copies of legally purchased content.

The Blu-ray Disc Association and third-party technology partners have developed a unique BD-ROM content protection system to meet these requirements. The system takes a three-pronged approach to protecting content distributed on the BD-ROM disc:

- **Advanced Access Control System (AACS)** offers state-of-the-art core cryptographic protection.
- **ROM Mark** provides the physical-layer technology to store key cryptographic secrets.
- **BD+** offers title-unique and renewable protection.

Combined, these three components provide comprehensive security that meets the needs of movie studios and customers. This white paper reviews AACS, ROM Mark, and BD+ and explains how they complement each other to protect high-definition content distributed on BD-ROM discs.

How Do AACS, ROM Mark, and BD+ Interact to Protect Content?

The three technologies that make up BD-ROM content protection are complementary. Each works individually to provide unique benefits, but all three deliver the robust protection that sets BD-ROM apart.

AACS is the core cryptographic system that provides content encryption, specifies how to authenticate the optical disc and BD-ROM player as trusted entities, defines which output technologies are allowed to carry BD-ROM content, and enables new business and entertainment delivery models over the Internet. AACS, which is described in greater detail later in this paper, is used to authenticate the components of the BD-ROM playback environment, validate their secure status, derive the key for content decryption, and decrypt the content for playback.

ROM Mark is the physical technology by which important cryptographic elements or "secrets" are stored securely on the BD-ROM disc. Calling ROM Mark a *physical technology* refers to the way that the data is stored on the disc. AACS uses these cryptographic secrets to derive the keys required to decrypt the content on the BD-ROM disc.

Once the content has been decrypted for playback, BD+ provides an additional level of security that is unique to Blu-ray Disc technology. Using BD+, portions of the audio/video (A/V) stream may be scrambled in a way that is unique to a particular BD-ROM title. BD+ technology allows title-specific code to be extracted from the disc and loaded into a virtual machine, which performs security checks of the playback environment and descrambles the A/V stream. BD+ technology also includes the ability to renew content protection on BD-ROM players that may have been compromised by a hacker.

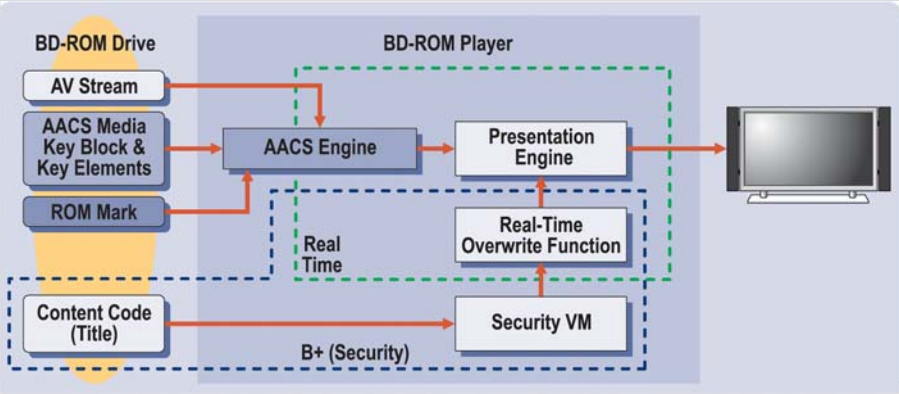


Figure 1. BD-ROM Content Protection Environment

This diagram depicts the main elements of the BD-ROM content protection environment. The AV stream, AACS key elements, and ROM Mark reside on the BD-ROM disc. AACS operations are handled in the BD-ROM player, which may be implemented as a DSP in a consumer electronics device or as a software player on the host PC. BD+ operates separately, adding an additional layer of title-specific and renewable protection.

As shown in Figure 1, each of the BD-ROM content protection technologies functions independently to provide unique benefits to the system. The following sections discuss AACS, ROM Mark, and BD+ in more detail.

AACS

Here we discuss AACS content encryption and decryption, bus authentication, and other important features.

Content Encryption/Decryption

Adequate protection starts with strong encryption. AACS employs the Advanced Encryption Standard (AES) with 128-bit keys. AES was adopted by the U.S. government in 2001 as an approved encryption standard and has become the *de facto* standard for most contemporary content protection systems.

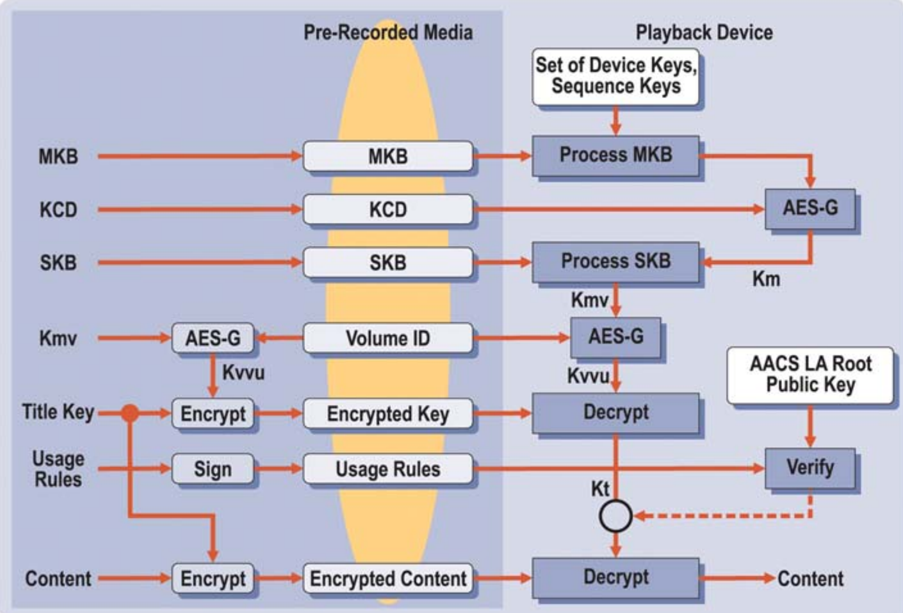
Under AACS, each BD-ROM player is issued a set of keys that are used in a multistep process to derive the Title Key required to decrypt content on a disc. The first step is to obtain a set of keys that are stored securely on the BD-ROM disc in an encrypted and packaged form called a Media Key Block (MKB). The MKB stores keys for each make and model of AACS-licensed BD-ROM player in a complex tree structure, thus providing the mechanism to prevent a compromised player from decrypting content. If a particular playback device is known to be compromised, the MKB can be composed so that the set of keys associated with the compromised player cannot be processed into valid keys. Each new BD-ROM movie title contains an updated MKB that reflects newly compromised players. Once a player is compromised, subsequent new BD-ROM movie titles cannot be played on that machine.

If the MKB is processed successfully, the resulting keys are combined with several other pieces of cryptographic data to derive the Title Key used to decrypt the content. All of the title-unique elements needed to derive the Title Key are stored on the disc, some encrypted, and some stored securely in the ROM Mark. See Figure 2 for a more detailed discussion of how the MKB is processed into the Title Key.

Bus Authentication

On a PC, content must also be protected as it passes over a data bus from the BD-ROM drive to the decryption and playback software running on the host PC. This is particularly important when using industry-standard bus interfaces such as Serial ATA (SATA), Parallel ATA, and USB with cables that may be accessible to hackers. AACS defines a bus authentication system that is designed to ensure a secure environment as data passes over a data bus.

The first step in securing any open interface is to authenticate the device on each end of the link—in this case, the BD-ROM drive on one end and the decryption and playback software on the other end. Authentication is the process of identifying each device and confirming that it is a "trusted" device. AACS authentication uses a complex challenge and response system that allows both devices to confidently identify each other.



The Media Key Block (MKB) is processed and combined with Key Conversion Data (KCD) stored in the ROM Mark to produce a "Media Key." The Media Key is processed, along with the Sequence Key Block (SKB), and then combined with the Volume ID stored in the ROM Mark. The resulting key is used to decrypt the Title Key stored on the disc. Once the disc usage rules are verified using the player's AACS Public Key, the Title Key is used to decrypt the content on the disc.

Source: *Advanced Access Content System (AACS) Pre-recorded Video Book,* www.aacsla.com.

Figure 2. Deriving the BD-ROM Title Key

AACS also defines a process to "revoke" the trusted-entity status of devices that have been compromised. Revocation lists are maintained by the optical drive and playback software, and they are updated each time a BD-ROM disc with a later version of the list is inserted into the drive for playback. The optical drive confirms that the playback software, which has already been identified and authenticated, is not on the revocation list. Similarly, the playback software confirms that the optical drive is not on the list. At this point, the interface is deemed secure.

Additional AACS Features

AACS has additional features that support online transactions, accommodate authorized copies, and protect against "analog theft."

Online Transaction Support

Because Blu-ray Disc technology supports Internet connectivity, content providers can augment a BD-ROM disc with additional online content. For instance, a movie disc can allow delivery of online content such as up-to-date movie trailers, games, and other extras. AACS supports such online "transactions" by cryptographically binding online content to a specific BD-ROM disc. This feature also allows content owners to offer innovative new services to customers. For example, movie studios can allow customers to transfer a movie to a portable device or make a legal copy. These features are not possible with today's DVDs.

Managed Copy

The Managed Copy feature is supported by the Blu-ray Disc copy-protection scheme. Although its details are not yet finalized, the Managed Copy feature promises to be a significant step forward in providing consumer flexibility by acknowledging the consumer desire to make copies of premium content. After confirming the presence of a commercial BD-ROM disc with AACS, the Managed Copy feature will enable consumer scenarios that may include making a backup copy of the disc, transferring the content to a portable video player, or adding the content to an electronic jukebox for playback throughout the home.

Analog Output Protection

Content owners, particularly movie studios, have long been concerned with protecting content that passes through legacy analog outputs such as S-Video, Composite video, or Component video. AACS provides four mechanisms to discourage unauthorized recording of content output over analog outputs, encouraging the use of protected digital outputs such as the High-Definition Multimedia Interface (HDMI) and the next-generation digital display interface, DisplayPort.

- **Audio Watermarks** — AACS also features the first standard consumer deployment of an "audio watermark." An audio watermark is an inaudible signal that carries data, which is placed in the audio stream. Although details are not yet finalized, there are two types of audio watermarks supported by AACS: "theatrical" and "consumer." The theatrical mark will be embedded in theatrical-released content. If an AACS-compliant BD-ROM player detects the theatrical mark, it is certain that the content was illegally recorded and copied to disc. In this case, there will be an appropriate enforcement action such as halting playback. The consumer mark will be embedded in content targeted for consumer BD-ROM players with AACS content protection. If the consumer mark is detected in content that is not protected by AACS or in an AACS-approved content protection system,[1] a similar enforcement action will be taken.
- **Analog Sunset** — The analog sunset refers to a defined date after which analog outputs are no longer approved for AACS-protected content. The AACS analog sunset will be enforced in two stages. Starting in 2010, analog output of AACS-protected content will be limited to interlaced standard definition formats only. In 2013, output of AACS-protected content on analog outputs will no longer be approved.
- **Image Constraint Token** — This mechanism allows studios to limit the resolution of content when played back over an analog output. If enabled, this token will limit resolution to 520,000 pixels per frame, which is 25 percent of the 1080p full high-definition resolution.
- **Digital-Only Token** — The Digital-Only Token instructs the player that video playback is not allowed over an analog output. Instead, playback is limited to protected digital interfaces such as HDMI and DisplayPort. This mechanism will allow movie studios to devise and offer new premium content offerings to customers while taking advantage of a higher level of protection. (In fact, the Digital-Only Token will only be allowed on new business models.) For instance, studios could release first-run movies to theaters and on BD-ROM disc concurrently.

AACS is a comprehensive, robust, and flexible content protection system that provides an excellent cryptographic base for BD-ROM discs.

ROM Mark

As mentioned earlier, ROM Mark is the physical-layer technology that securely holds certain cryptographic secrets on the optical disc. These secrets are essential to the successful decryption of content on the disc. Because it is a physical-layer technology, ROM Mark does not store data on the disc in a traditional manner. Instead, the technology employed to store data requires a licensed method in the optical drive to extract the data prior to playback.

The physical nature of ROM Mark is designed to prevent a bit-for-bit copy of the disc. By holding certain essential secrets in a method that is not simple bits stored on the disc, ROM Mark prevents unauthorized copying by direct disc-to-disc replication.

BD+

BD+ is an additional layer of security that complements, but operates separately from, AACS and ROM Mark. BD+ is designed to provide unique, title-specific content protection, which adds a layer of security beyond competing content management systems. BD+ also provides the ability to renew the BD-ROM content protection system.

At its core, BD+ is a virtual machine (VM), running within the BD-ROM playback engine. The VM runs title-specific code that is delivered to the system from the BD-ROM disc. The main job of the VM is to run a security check on the playback environment, extract the content-specific code from the disc, and run a "fix-up" function on the content stream.

Each BD+-licensed BD-ROM player is issued BD+ security keys and a certificate that is signed by a BD+

[1] Examples of current AACS-approved content protection systems are High-Bandwidth Digital Content Protection (HDCP) and Digital Transmission Content Protection (DTCP).

licensing authority. The security check performed by the VM matches the player's BD+ security keys with the player's certificate. This check insures that keys have not been compromised or stolen from another playback environment and inserted into the environment being checked.

Once the keys and certificates have been checked, the VM "discovers" the player's playback environment—or its "memory footprint." Each player manufacturer must provide the BD+ licensing authority with a memory footprint that can be used to identify their playback environment. Security checks use these memory footprints to positively identify the player and confirm the integrity of the content-protection environment. Playback can begin once these checks are complete and it is confirmed that the player does not appear on a list of compromised players.

As mentioned earlier, small sections of the A/V stream are scrambled during authoring. After content from a BD-ROM disc has been decrypted under the AACS process, the content must be descrambled by the BD+ VM before it can be rendered. The code used by the VM to descramble the stream is provided in a secure manner on the disc. At playback time, the playback engine extracts the content-specific code from the disc, as well as a "fix-up" table that identifies the scrambled sections of the A/V stream. The content-specific code is loaded into the VM, which uses the fix-up table in the process of decoding the scrambled sections of content. This process, shown in Figure 3, is called a Media Transform.

BD+ is designed to be deployed in three phases. The first phase is the Media Transform function described here. Phases 2 and 3 are countermeasures for compromised playback environments. If a player is known to be compromised, BD+ can be used to deploy code that can counteract the compromise. This capability is referred to as *renewability*. It is not necessary to revoke the compromised player; it can simply be updated to renew its content protection environment.

Phase 2 of BD+ deployment is called a *basic* countermeasure. Once a compromised player is identified and studied, it may be possible to develop content-specific code, with the cooperation of the player manufacturer, that subverts the hack. This content code is player-specific and can be deployed on the BD-ROM disc. If the compromised player is detected during the discovery process, the player-specific content code can be run in the VM to subvert the hack and allow the compromised player to play back the content. On all other playback platforms, the normal content-specific code described previously is run. Player-specific content code is also non-persistent.

Phase 3 countermeasures may be deployed when Phase 2 countermeasures are unsuccessful. Native code developed specifically for the compromised player environment can be developed and deployed via BD+. This native code runs as part of the player's native operating environment and is developed with the cooperation of the player manufacturer. If the compromised player environment is detected by BD+ at playback, and native code is available, it can be used to update the playback environment, rendering the hack ineffective.

The following characteristics of the BD+ system help to contribute to customer-friendly solutions:

- BD+ content-specific code is not persistent. When code execution halts, the code is discarded, which leaves little or no opportunity for a hacker to attack the system.

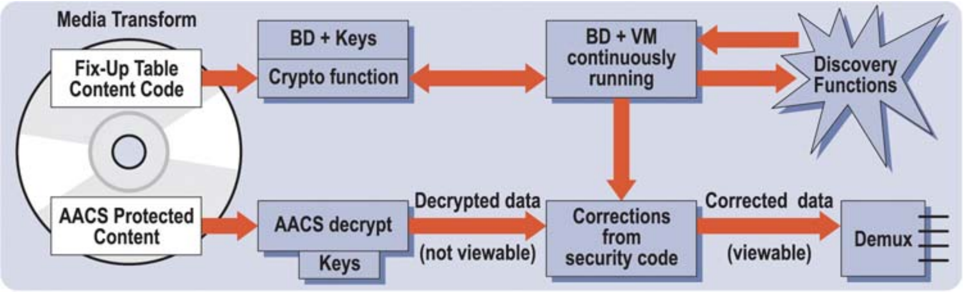


Figure 3. BD+ Media Transform Process

- BD+ content-specific code is cryptographically signed, insuring its integrity.
- BD+ content-specific code makes no persistent changes to a player. Instead, it leaves the player environment intact.
- During discovery of the playback environment, the process of matching the BD+ keys to the BD+-signed certificate cryptographically ties the environment together and makes false detection virtually nonexistent.
- Customer privacy was the top consideration during BD+ development. Only information about the playback environment is known to the BD+ system. No information about the customer is ever gathered or shared by BD+.

BD+ provides the BD-ROM playback environment an additional layer of title-specific security. It also provides the ability to re-secure compromised environments without having to revoke the player. These two unique functions propel BD-ROM content protection to levels of robustness and flexibility unmatched by previous and competitive content protection systems.

Conclusion

The BD-ROM content protection system takes a three-pronged approach to content protection, offering state-of-the-art core cryptographic protection in the form of AACS, a physical-layer technology for the storage of key cryptographic secrets in the form of ROM Mark, and title-unique renewable protection in the form of BD+. Each of these distinctive and cooperative technologies offer state-of-the-art security functions. Together, they provide the BD-ROM disc with a level of content protection not seen in previous and currently competing optical disc systems.

For More Information

- The source for the AACS content in this white paper is revision 0.91 of the specification, released February 17, 2006, and published on the AACS website at www.aacsla.com/specifications, and the interim adopter and interim content participant agreements at www.aacsla.com/support.
- Blu-ray Disc Association: www.blu-raydisc.com

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Trademarks used in this text: *Dell* and the *DELL* logo are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.