



Frequently Asked Questions

Q: What are CPRM and CPPM?

A: Content Protection for Recordable Media (CPRM) and Content Protection for Pre-recorded Media (CPPM) are technologies designed to balance the need of content providers to protect their intellectual property while allowing consumers to use digital media to access, store and display movies, games and other entertainment content.

Q: What are the differences between CPRM and CPPM?

A: CPRM protects commercial entertainment content copied on to portable data storage technologies such as SD cards, CompactFlash™, recordable DVD media and the IBM Microdrive™ in the CompactFlash physical form factor. CPPM, on the other hand, protects commercial entertainment content copied onto pre-recorded media, including DVD-Audio, an emerging physical audio format.

Q: Why are these content protection technologies needed?

A: The move from analog to digital media increases the risk for unauthorized reproduction. That's because digital content, unlike analog content, can be reproduced almost infinitely in mass quantities with minimal reduction in quality. Widespread availability of digital copying devices and the Internet has increased rampant, unauthorized distribution of copyright-protected content. CPRM and CPPM technologies were developed to enable consumers to enjoy premium content on a wide range of devices. CPRM and CPPM enable consumers to make authorized copies of commercial entertainment content where the content copyright holder has decided to protect it from unauthorized copying.

Q: What are the advantages of CPRM/ CPPM?

A: The primary advantage of CPRM/ CPPM is enabling protected interchange of stored content among different devices, such as between portable players manufactured by different companies. For more information, [click here](#) .

Q: How do CPRM and CPPM work?

A: These technologies adds a Media Identifier and Media Key Block (MKKB) to the media. A standardized command interface, such as in the ATA specification, would permit any CPRM-enabled host device or application to robustly read the Media Identifier and MKB to enable playback. The rest of the command interface for CPRM-

enable devices is the same as other devices: data are read or written using existing commands. Encryption and decryption are performed by the host device or application.

Q: When will CPRM and CPPM be available?

A: CPRM specifications and licenses are available now for all supported media.

Q: How can we license CPRM/PPM?

A: These technologies are licensed by the 4C Entity, an industry group formed by IBM, Intel, Matsushita and Toshiba. For more information, [click here](#).

Q: What is the 4C Entity?

A: 4C Entity is the licensing body for technology developed by the 4C Entity founders. The body also leads the development, adoption and promotion of interoperable standards for sharing premium content. 4C Entity has licensed and coordinated with numerous industry-leading content providers, service providers, application developers, and hardware manufacturers to offer the best digital media solutions. By using these standards, device manufacturers offer consumers a mix of brands that best meet their needs, while reducing long development time and resources.

Q: Which products use CPRM/PPM?

CPRM and PPM technologies can be used in a wide range of consumer electronics, including but not limited to:

- PDAs for storing all kinds of data
- Mobile phones for storing images, sound clips and other media files
- Portable media players

Q: Who supports CPRM?

A: 4C Entity has coordinated with numerous industry-leading content providers, service providers, solutions providers, application developers, and hardware manufacturers to offer the best digital media solutions. More than 250 companies have licensed the technology. CPRM is also an approved output for many other content protection technologies.

Q: Will CPRM/PPM affect file systems and defrag programs?

A: No. The media key block does not have to be at a fixed location. It is outside of the addressable sectors, so it is transparent to operating systems and disk defragmentation. In this respect, it is like the hardware error logs that are already written on the media.

Q: Doesn't CPRM/PPM prevent backup?

A: This technology handles/treats DVD and SD card media differently. No, the technology does not prevent backup for DVD. In this case, CPRM is transparent to non-protected files, so data can be backed up and restored normally. Protected files are also just files, so backup copies (playable only when restored to the original media) can be made. However, for SD cards, the situation is different. Files--including access keys to protected content--are stored in a special area called the Protected Area. Backup copies of

files in the Protected Area are not allowed because the key data needs to be securely erased when the content is digitally moved to another media or device.

Q: What is CPSA?

A: Content Protection System Architecture (CPSA) is a comprehensive, standards-based architecture. It was created by the 4C Entity to define an overall framework for various content protection technologies including:

- CPRM for protecting content stored on recordable media such as DVD or Flash
- CPPM for protecting pre-recorded DVD-Audio content
- CSS for protecting pre-recorded DVD-Video content
- DTCP for protecting content during digital transmission over 1394, USB, and IP
- HDCP for protecting content moving across high-bandwidth interfaces to digital displays
- Conditional Access for protected distribution of premium content via cable or satellite
- 4C/Verance Watermark for embedding and reading watermark content management information (CMI) in audio content