

DVD+RW
The perfect match for every system



V-CPS

Video Content Protection System



PHILIPS

What is VCPS*?



VCPS is an innovative technology for encrypting video recordings on DVD+R and DVD+RW discs.

Designed to protect recordings of digital broadcast according to the Broadcast Flag rules adopted by the United States Federal Communications Commission (FCC), VCPS also enables direct digital recording of 'copy-once' content from satellite and cable sources. VCPS was jointly developed by Philips and HP.

Where can you find out more about VCPS?

More information about VCPS, including the specifications and the license agreement, is available from Philips at:

<http://www.licensing.philips.com/vcps/>

For any questions regarding VCPS contact us at:

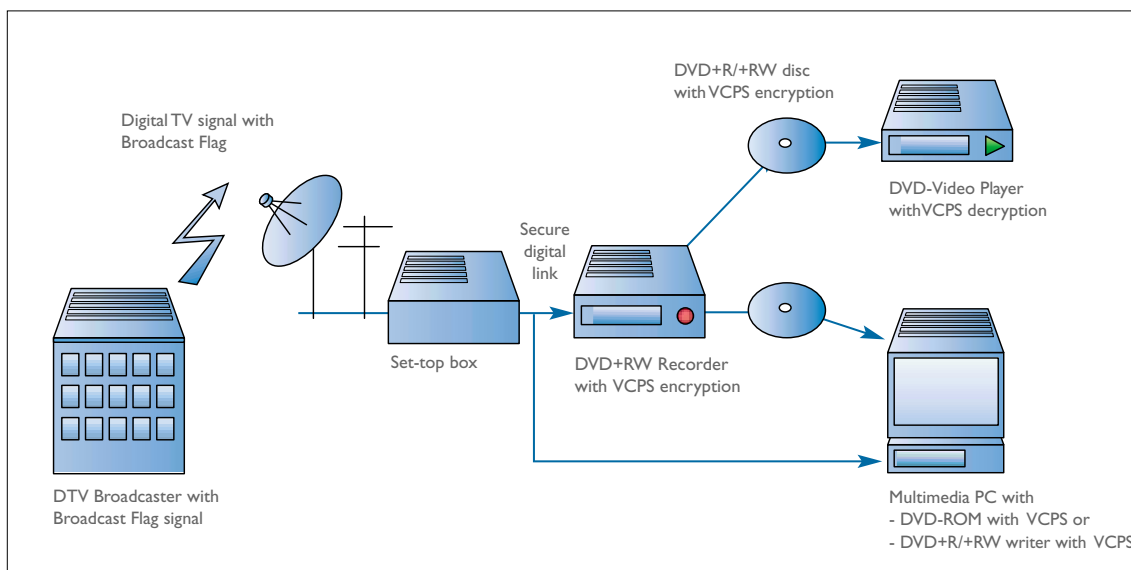
vcps@philips.com



*VCPS was previously known as Vidi.

What is the Broadcast Flag?

The Broadcast Flag is a digital code that can be embedded into an ATSC digital broadcasting stream in the USA. The Broadcast Flag does not affect the consumers' possibilities for making digital copies; the Broadcast Flag only seeks to prevent mass distribution over the Internet. In practice that means that the recorded video must be encrypted, and that the encrypted recordings will play only on equipment that does not make the content available to the Internet.



Why do you need VCPS?

On 4 November 2003, the United States FCC published its decision on the Broadcast Flag, meaning that after 1 July 2005, digital video recorders in the United States will have to encrypt recorded TV broadcasts that carry the flag. In Japan, a similar regulation already requires the encrypted recording of digital TV broadcast signals.

The implementation of VCPS in DVD+R/RW equipment and discs is not mandatory, but equipment and discs without VCPS capability will be unable to record or playback digital TV broadcast in the USA that is protected with the Broadcast Flag.

Why choose VCPS?

- No change in the disc manufacturing process.
- No increase in the manufacturing costs of blank DVD+R/RW discs.
- IC manufacturers can supply VCPS-capable IC without restrictions.
- Implementers of VCPS-capable software do not have to pay a per-installation royalty.
- No annual fees for implementers of the VCPS technology. Implementers only pay for the actual use of keys and key blocks.



How do you add VCPS capability to your product?

Adding VCPS capability to DVD+R/+RW equipment and discs is straightforward. Manufacturers of blank DVD+R and DVD+RW media simply need to place VCPS-related information in the ADIP (Address-in-Pregroove) of their discs, which can be done without investing in new manufacturing equipment and without increasing manufacturing cost. Manufacturers of optical drives can add VCPS capability in firmware. Manufacturers of DVD+RW recorders and DVD players need to add an implementation of the publicly available AES cipher in their MPEG decoder ICs. *Table 1* shows an overview of required product upgrades.

Necessary product upgrades to enable VCPS compatibility

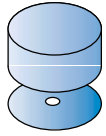
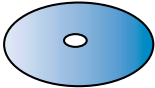
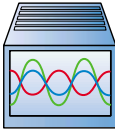
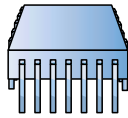


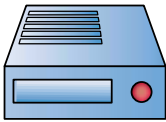
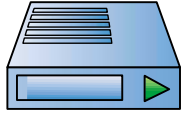
<p>DVD+R/+RW master and stamper</p>	<p>DVD+R disc DVD+RW disc DVD+R DL disc</p>	<p>DVD+R /+RW formatter and test equipment</p>	<p>DVD+R /+RW chipsets</p>
			
<p>Include a VCPS Disc Key Block in the information that is recorded in the ADIP of the master.</p>	<p>Manufacture disc with a VCPS-enabled stamper.</p>	<p>Include Hardware Device Keys and Disc Key Blocks for testing purposes.</p>	<p>Add AES cipher in MPEG2 decoder ICs.</p>
<p>DVD+R /+RW PC writer</p>	<p>DVD+R /+RW PC application</p>	<p>DVD+R /+RW video recorder</p>	<p>DVD-Video/ROM player</p>
			
<p>Store a VCPS Hardware Device Key in flash memory.</p>	<p>Include a VCPS Device Key and Application Key Block in software application.</p>	<p>Add a VCPS Hardware Device Key, a VCPS-capable drive and a VCPS-capable MPEG2 encoder/decoder IC.</p>	<p>Add a VCPS Hardware Device Key, a VCPS-capable drive and a VCPS-capable MPEG2 decoder IC.</p>

Table 1



VCPS - Technology and Architecture

Encrypting MPEG2 streams

VCPS protects a video recording by encrypting the MPEG2 streams on DVD+R, DVD+RW and DVD+R DL discs.

The main techniques are:

- A 128-bit AES cipher encrypts the disc sectors that contain MPEG2 video.
- VCPS-capable blank DVD+R/+RW discs contain a Disk Key Block coded in the track wobble (ADIP). The Disk Key Block contains a hidden key that can only be found by an authorized player with the help of the Device Key. A non-authorized player cannot find it.
- VCPS-capable recording equipment and playback equipment need a Device Key embedded in the product. The Device Key is a group of 40 keys used to extract the Disk Key.
- VCPS-capable recording- and playback equipment use their Device Key to calculate the encryption key of the MPEG2 stream from the Disk Key Block.

The disc

The Disk Key Block that is coded in the track wobble (ADIP) of VCPS-capable recordable discs is written together with the address information on the stampers that are used in replicating blank recordable discs. Disc manufacturers do not have to invest in new manufacturing equipment, and there is no change in the manufacturing process. This means the manufacturing cost of a VCPS-capable blank disc is the same as for a non-VCPS disc.

Implementing VCPS on players and recorders

A VCPS-capable DVD recorder or DVD player uses its Device Key to calculate the encryption/decryption key for the MPEG2 video (see figure 1).

Each sector that contains MPEG2 video is encrypted, except for the first 128 bytes. These 128 bytes contain header information that is useful for navigating the disc.

Implementing VCPS on PCs

Encryption and decryption in PC implementations is performed in the same way as in a stand-alone DVD-recorder. Each software application requires a Device Key to calculate the encryption key (see figure 2). Encryption and decryption of the video is carried out by the software. The only difference is that PC software and the PC drive are required to perform an authentication protocol in which the optical drive proves that it is a genuine optical drive and not a software emulation of an optical drive. The optical drive also needs a Device Key to perform this authentication, and the software applications need a so-called Application Key Block in addition to its Device Keys.

A disc can contain both encrypted and non-encrypted video

A VCPS-capable disc can also record unprotected video. It is also possible to mix unprotected and protected recordings on the same disc. The unprotected video recordings will play in all DVD players, while the protected recordings obviously need VCPS-capable playback equipment.

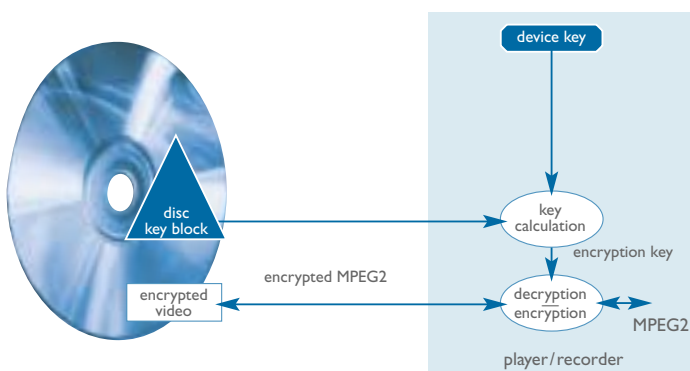


Figure 1. Device Key on player or recorder

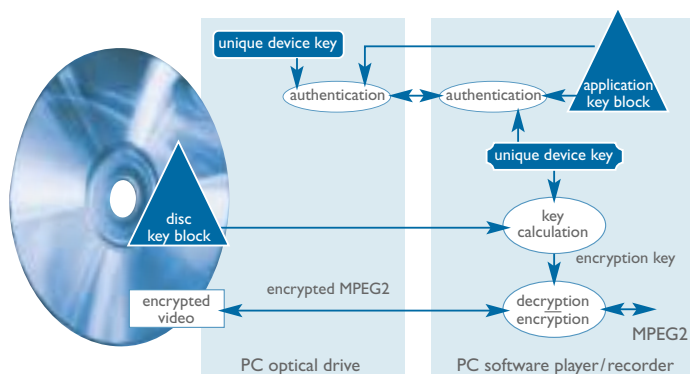


Figure 2. Device Key on PC player / recorder and optical drive



Where can you find out more about VCPS?

More information about VCPS, including the specifications and the license agreement, is available from Philips at:

<http://www.licensing.philips.com/vcps/>

or contact us at:

vcps@philips.com

More information about the Broadcast Flag and the anti-piracy policy of the Federal Communications Commission (FCC) is available at:

http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-240759A1.pdf

How to implement VCPS

	Step 1	Step 2	Step 3
	Obtain the specifications from Philips	Sign VCPS Content Protection Agreement ⁴	Pre-Production Events
DVD Recorder, Player & PC Drive Manufacturers	<p>The VCPS specification is available for everyone, even without signing a license.</p> <p>The VCPS specifications contain Device Keys and Key Blocks for development and testing purposes¹</p>	Sign VCPS agreement as Hardware Implementer.	Purchase Hardware Device Keys from Philips (order form is included with the VCPS agreement).
IC Manufacturers		Sign VCPS agreement as Component Implementer.	
PC Software Implementers		Sign VCPS agreement as Software Implementer.	Purchase Software Device Keys and Application Key Blocks from Philips (order form is included with the VCPS agreement).
DVD+R & DVD+RW Disc Replicators		Sign VCPS agreement as Replicator.	Purchase stampers from a VCPS-licensed Manufacturer of stampers.
Master and Stamper Manufacturers		Sign VCPS agreement as Master manufacturer.	Obtain a VCPS-capable formatter from your usual supplier or direct from Philips.
Test Equipment and Formatter Manufacturers		Sign VCPS agreement as Master Manufacturer & Hardware Implementer.	Depending on the type of product that you create, you may need to purchase Hardware Device Keys and Disc Key Blocks from Philips (order form is included with the VCPS agreement).
Multi Media PC Manufacturers		NA	

Table 2



Step 4	Step 5
Production Events	Costs Involved ²
Insert a different Hardware Device Key in each individual product when assembling the product.	Cost euro 0.05 per manufactured product.
	VCPS-capable ICs can be sold and distributed without restrictions, also to non-licensed set-makers. ³
A single Software Device Key can be used in an unlimited number of installations.	One set of Software Device Keys and Application Key Blocks costs Euro 750 and can be used for an unlimited number of installations.
Report the number of VCPS-capable discs manufactured, using the Key Fee Reporting Form included with the VCPS agreement.	Replicators pay euro 0.01/ manufactured disc for the right to embed the Disc Key Block in the discs.
A different Disc Key Block must be used for each master with VCPS-capability. An unlimited number of stampers may be created from a single master. VCPS-capable stampers may be sold only to VCPS-licensed replicators.	A set of 100 Disc Key Blocks costs euro 750.
Include a VCPS-capable PC drive and VCPS-capable application software in the PC.	No need to take a VCPS license or pay any VCPS-related fees on the sales of VCPS-capable PCs.

1. In Q4 2004, Philips also will be able to supply you with test discs, both blank DVD recordable discs and recorded discs.

2. Q2 2004 price.

3. IC manufacturers do not pay any VCPS related fees on VCPS-capable ICs.

4. This agreement is available at: <http://www.licensing.philips.com/vcps/>



PHILIPS

