

# COPY PROTECTION STRATEGIES FOR THE DIGITAL HOME

Carmi Bogot  
NDS Technologies

## Abstract

*Digital entertainment content is the driving force in the “digital home” revolution. Availability of content drives demand for consumer electronics devices and for the ability to interconnect these devices using a home network. At the same time, the new availability of digital content on a wider range of connected devices makes content protection an ever-more pressing issue for content developers and rights owners.*

*Content protection is a highly emotive issue, which impacts all the players in the digital content distribution value chain. This paper defines both the technical and business terms critical to content protection in the digital home. It proposes the Secure Video Processor (SVP) — created by adding a small number of gates into an existing video processor chip design, creating a Secure Video Processor or SVP. The SVP Alliance is a group of interested parties committed to advancing the development of secure content distribution and the wide adoption of SVP technology. The paper also presents the business benefits that SVP brings to all the principal players in the content protection industry: operators, studios, chipset manufacturers, CE vendors and consumers.*

## INTRODUCTION

Digital entertainment content can take any of a number of formats — it can be broadcast TV content, digital music, or movies. The content can be delivered to the home in any of a number of ways — broadcast via terrestrial, satellite or cable

transmission, downloaded from the Internet via broadband or uploaded from a digital camera or other recording device.

What makes the digital home appealing is the high level of picture and sound quality and the ease with which consumers can access content on several devices, sharing and transferring high quality content throughout a home network. It is this same level of quality and flexibility which gives rise to worries about illegal reuse and redistribution of copyrighted content.

Today, it is technically possible for digital content to move freely between storage and access devices, and to reside in many locations from the time it is distributed until the time it is finally rendered and consumed by consumers. In fact it is so easy to move digital content, that systems that try and prohibit the movement of content are easily hacked.

Rights owners and content providers, as well as networks and platform operators, who generate revenues from reselling their content, do not care if an un-viewable / unusable copy of content is made. They are concerned with the uncontrolled viewing of content without proper content protection mechanisms in place.

The SVP Alliance proposes a solution which balances the consumers’ demand for fair and flexible use of content throughout their home network — their “domain” — with the rights owners’ need to protect their business interests. SVP does this by creating an end-to-end chain of control over content from distribution until rendering.

## Defining the Digital Home

A digital home features any combination of TV sets — analog and digital — DVD and MP3 players, DVRs, media centers, PCs, PDAs, cell phones and home video servers, all interconnected via a home network. The digital home consumer wants flexible access to high quality digital content, on demand, on any of these devices.

Digital TV content is playing an increasingly important role in the digital home. According to Strategy Analytics, there were around 100 million digital TV households worldwide at the end of 2003. By 2008, this number is projected to pass the 300 million mark.

The massive appeal of digital TV content creates an incentive for consumers to add another digital platform to their home — the digital set-top-box (STB). New STBs facilitate a two-way connection between the home and an external service. An increasing number of STBs also feature local storage (known as a PVR/DVR), allowing time-shifted viewing and archiving of digital entertainment. In addition, the existence of a digital STB stimulates consumers to use and look for convergence between the STB and other devices in the home, further driving the development of the home network.

Convergence, fair use, and flexible use are all terms used when talking about consumers' desire to access the same content easily on different electronics devices.

For example, most U.S. households include multiple TV sets. Owners of advanced DVRs and STBs with local storage express strong interest in having time-shifted viewing capabilities on every TV in their household. As a result, some

DVR vendors offer consumers the ability to stream recorded content from a central DVR to client devices over a home network.

Implementing home networks allows viewers greater convenience and flexibility since content can be consumed on multiple TV sets, DVRs, and DVD players within their homes as well as on portable devices such as PDAs.

## SECURE CONTENT IS THE KEY

Appealing, timely, and high quality digital content is the foundation of the digital home revolution. Without the content, consumers obviously don't have the incentive to purchase devices which enable them to use and enjoy digital content. But the availability of content depends on more than the simple existence of consumer demand for access to it — it depends on the willingness of content owners to provide content and the service providers to offer it as part of a secure pay TV service.

One of the most significant issues content providers face in the digital age is illegal use, distribution, and redistribution of content. Unprotected digital content can be copied, redistributed, and consumed at its original quality by anyone. Clearly, content owners and service providers whose business is based on selling content seek to prevent this by using content protection mechanisms. Without the means to control content rights in the digital home, content owners will limit their content offering for this environment. Furthermore, service operators are obligated to protect the rights of their content owners. Operators will hesitate to enable their digital STBs to interface with other devices in the home via high speed ports if they cannot control access to the content once it leaves the STB.

For these reasons, balancing the rights of the content providers with the needs and demands of consumers is critical to the future development of the digital home network. Flexible, low cost, user friendly, content protection mechanisms are required to satisfy the needs of consumers who should be able to enjoy greater access to and “fair use” of high-value content. Such mechanisms provide benefits to consumers as well, enabling dozens of new ways to purchase content, such as content rentals, video-on-demand, and other models made possible by content protection.

### A FLEXIBLE, LOW COST SOLUTION

The SVP-enabled chip ensures that content is under control from the beginning of distribution until it reaches its final destination and is rendered. The content is always encrypted, and the rights are defined in a separate, standard, tamper-resistant license.

Every device that consumes digital video must already have a digital video processing chip. SVP technology is embedded within this chip, turning the existing video processor into a “Secure Video Processor” chip. The SVP handles both the content and the license. The SVP is unconcerned with the physical distribution method and it is independent of the location or locations where content is stored and the networking or communications technology used to move content between locations.

Designing the SVP as a hardware-based solution enhances security while making it easier to standardize — and therefore easier to produce inexpensively in mass quantities. The SVP-enabled chip can be implemented in any digital device, including STBs, TVs, DVD players and recorders, DVRs, PDAs and other portable devices — without requiring special customization for each type or model of

device. Upgrading any existing video processing chip into an SVP is a simple process that typically increases the existing gate count by less than 2 percent.

### What does the SVP Protect?

The SVP is designed to protect any scrambled digital content, associated with a valid license. The content is typically SDTV or HDTV MPEG-2 / 4) and any form of digital audio. Content can be delivered to the home via any existing method in use today — cable, satellite, DSL, or terrestrial — and protected by any existing conditional access technology. The scrambling algorithms used on the content are market-dependent, and could be, for example, DVB-CSA, DES, 3xDES, AES, DVS-042, Multi-2 or CSS.

### Domain and Fair Use

To facilitate the fair use of content across multiple devices within a consumer’s home, SVP enables definition of two types of domains, within which content may be consumed. A domain is essentially a consumer household, made up of a number of interconnected consumer electronics devices. Domains may be externally managed or autonomous.

- An externally managed domain is managed using a gateway connected to an external network. An STB, connected to a service operator’s network and using the operator’s conditional access, would be considered an externally managed domain.
- An autonomous domain is a network of consumer electronics devices where one of the devices on the network manages the domain and the network.

Any device in the domain that wants to access controlled content must have an SVP enabled chip. Under the proposed SVP solution, it is possible to limit the number and type (STB, mobile device, TV, DVD player, etc.) of devices within a domain. In addition, SVP can control access rights and specify how consumers may use content. Use of content can include any combination of:

- Rendering (accessing the content)
- Rendering content plus permission to record and reuse the content for a short, defined time period, perhaps 90 minutes
- Permission to make and store recordings of the content
- Permission to copy the content and use it within the domain
- Permission to move the content, which entails creating a copy and deleting or disabling access to the original, and using the copy within the domain or outside the domain
- Exporting the content to a different content protection system. Such as transfer to 5C or HDCP control.

#### How SVP Protects Content

All content on an SVP-protected network is accompanied by a usage license. Content is never transferred between SVP devices in the domain “in the clear” — it is always scrambled either using the AES-based, SVP Native Scrambling Algorithm (NSA), or the original broadcast scrambling. In some cases both algorithms can be in use at the same time, resulting in super scrambling.

SVP provides a standard messaging format for defining content rights. Each movie should have one Content Segment License (CSL) and a set of Base Line ECM messages (BL-ECM). A new BL-ECM is required every time the control word (descrambling key) changes.

#### SVP FUNCTIONALITY

The SVP-enabled chip is capable of receiving clear or scrambled content, and can descramble and re-scramble the content using various ciphers including an SVP standard cipher NSA that uses 128-bit control words. The SVP can also receive and transmit standard format licenses, consisting of a CSL and any number of BL-ECMs. All processing of content, whether in scrambled and compressed format or descrambled and decompressed format, and all of the processing of the license occurs in hardware within the confines of a single SVP-enabled chip.

Each SVP is associated with a public certificate that uniquely identifies the SVP, and the properties of the device in which it resides — device type, whether it supports watermark detection capability, which decryption algorithms it supports, which video formats, and other properties.

At any given time, an SVP is linked to a specific authorized domain. The maximum number of devices within the domain is limited by the certificate. SVP-equipped devices within a domain will mutually authenticate each other and establish a secure channel prior to exchanging content.

## SVP and Conditional Access

An SVP can work alongside and in conjunction with a service provider's conditional access system:

1. Content arrives at the STB under conditional access system control.
2. Content is then transferred to the SVP so it can be used by other standard devices within the domain.
3. To transfer or share control, the conditional access system must be able to generate a *standard* content license, including a standard Content Segment License (CSL)<sup>1</sup> and a standard Base Line Entitlement Control Message (BL-ECM)<sup>2</sup>, for the content.

Three conditional access systems are available in the STB — embedded, smart card, CableCARD. Each can act as a gateway between the conditional access system and the SVP system. In addition, the conditional access system should be used by the network operator to perform actions such as setting up authorized domains, issuing and renewing certificates, and passing SVP certificate revocation lists.

## BUSINESS BENEFITS OF SVP

The digital entertainment industry comprises a range of players whose interests often seem to conflict. Content protection is an often-contentious issue which affects each of the principal players — network operators, content providers, chipset vendors, CE vendors, and consumers — differently. SVP offers a unique win-win situation where every player can realize

benefits from the adoption of SVP as a standard approach for digital content protection.

## Network Operators

The growth of pay TV businesses demonstrates an increasing willingness of viewers to purchase the rights to view compelling content. However, along with that willingness is an expectation of being able to use that content in increasingly varied and personalized ways. Many, or most, viewer households include multiple TV sets, as well as a DVD, a VOD service, a DVR, and, increasingly, a home network that connects several home entertainment devices.

These viewers want to be able to access their pay TV subscription on all the TV sets in the house, they want to make backup copies on DVD-R media, store content on removable USB keys, and use it anywhere that they are.

Network operators know that their continued success depends on their ability to provide viewers with top content *and* flexible accessibility. At the same time, the operators won't be able to obtain that content if they cannot demonstrate to content providers and rights owners their ability to protect the content and control access to it. They need a solution that offers viewers the fair use they demand, while protecting content and expanding the operator's business models.

Current solutions require a second or third STB for every location that content is used. This is not only an unattractive solution from the consumer's viewpoint, cluttering up the house with numerous boxes and cables; it is expensive for the service operator. In most cases the service operator

---

<sup>1</sup> The attributes and usage rights for content are defined in a standard tamper-resistant message.

<sup>2</sup> BL-ECM messages are used to securely transmit decryption keys.

pays for the development of the STB and supplies the boxes to subscribers at minimal or no cost. Furthermore, subscription fees for secondary devices are usually priced at very low rates. The result is that secondary STBs generate cost, not profit. Even if the operator implements a solution with a single high-end STB which communicates with numerous secondary, relatively inexpensive STBs, the operator still faces an enormous expense in developing, deploying, and maintaining large numbers of STBs.

Viewers would pay for off-the-shelf consumer electronic devices to access content within the home, as long as these devices were and not linked to a specific service operator.

SVP solves these problems. SVP allows any network operator to deliver content in a secure fashion to any SVP-enabled third-party device. With SVP-enabled chips included in each consumer electronics device on a viewer's home network, the operator can extend access control throughout the home network and even to all devices — including portable devices — and realize dozens of new business models and program packaging options. This is accomplished at virtually no cost to the operator, since proprietary and conditional access components are required only in one “gateway” STB, not in all of the networked devices. Thus operators can enable access to stored content or video-on-demand (VOD) content on all TVs within a viewer household while deploying / subsidizing only one STB per viewer household.

On-demand content can be sent directly from the network to any device using SVP content protection. Broadcast and On-demand content can also be sent via an operator controlled SVP enabled STB enabling redistribution to other SVP-

equipped TV sets, PDAs, DVDs, etc. in the home or domain. This enables new business models based on secure home network distribution to multiple viewing devices. Operators can offer extended content rental packages, for example, charging extra for the rights to view across the home network or on multiple TVs. Pay-per-view and Video-on-demand content is now truly available on demand to consumers, when and where they want to see it. Operators can determine which additional devices may be used to access content and for how long — and charge accordingly for these access rights. The operators also control copying and storage rights, providing even more opportunities for licensing fees. They can charge a certain amount to permit saving content for a limited time period with on-demand viewing, including the ability to pause, rewind, and fast-forward the content — and charge more for permission to make a permanent copy. The SVP license is even flexible enough to enable operators to charge for rights to view content in an additional domain or to “transfer” rights — canceling the viewing permissions in the original domain when a copy is made to be viewed elsewhere.

Furthermore, SVP protection extends even to content which is archived onto D-VHS or DVD devices. The content license defines the access criteria as determined by the network operator. Operators can then enable viewers to record and keep content indefinitely, confident that the content can only be viewed within that viewer's domain, not recopied and redistributed freely to friends and neighbors.

### Content Providers

Content providers have a clear interest in protecting their content and determining who may access it and when. They need to

protect content from piracy and other unauthorized use and redistribution, and to enforce business models.

Until now, only a few models have been available for protecting content. One method of controlling access to content has been using limited packaging and distribution options, such as a CD for audio content or DVD for video content. These do not provide reliable content protection, and offer no flexibility in packaging and marketing.

Another method of content protection, particularly for video content, is to work with network operators who use conditional access to protect content rights. This solution is being challenged by the proliferation of home networks — and is not satisfactorily meeting consumer demands for fair use access to content on these networks.

Historically, discussions of content protection have focused on protecting interfaces / pipes and not on protecting content. For example using 5C for 1394, using DFAST for CIM, and using HDCP for DVI. These are all interface protection mechanisms that attempt to protect the transfer of content over specific media but do not provide an end-to-end method for controlling rights to content. In addition, new forms of digital copying and storage that are becoming easily available to consumers make it easier for consumers to evade restrictions on content.

SVP offers reliable protection for content, wherever that content resides and however it is accessed. It can offer content providers the confidence to permit better viewing windows for new movie releases, opening up new business opportunities both for the content providers and the network operators who distribute the content.

## Consumer Electronics Manufacturers

Manufacturers of consumer electronics devices might initially be inclined to argue that content protection is not their concern. However, it is clear that the ramifications of unlimited illegal distribution of digital entertainment media will ultimately affect their industry, as solutions are either legislated or imposed by content providers.

Proactive implementation of content protection using SVP creates a situation where all players in the digital home entertainment arena benefit. SVP enables CE manufacturers and chipset vendors to offer a standardized, low-cost content protection solution which does not significantly increase their manufacturing costs. The security is placed in chips that are already an integral part of the CE device. The SVP solution offers CE vendors new business opportunities as well. SVP facilitates home networking while preventing unauthorized use and redistribution of content. If a content protection solution is in place, content providers will be more likely to enable the use of high value content across these networks. The availability of high value content will, in turn, drive the demand for newer and more networked devices, enabling CE manufacturers to create a wide range of SVP-compliant devices which can be used to consume content in increasingly sophisticated home entertainment systems.

For example, a new device and delivery mechanism can be created by simply combining a broadband connection, SVP and any existing viewing device like a DVD player. This would enable the device to receive video-on-demand directly from content owners — increasing the value of the device and providing room for additional revenue.

Thus, SVP presents the opportunity for CE manufacturers to participate in pay TV distribution on home networks. Without a standardized content protection solution, pay TV operators could only permit their own proprietary devices to be used to decrypt their programming. However, the ability to use SVP certificates and licenses to enforce the pay TV operator's entitlements means that CE manufacturers can now enter this lucrative market with non-proprietary "horizontal" retail devices. This provides consumers with increased choice, while spurring development of and creating new markets for CE devices.

### Consumers

It often seems to consumers that the entertainment industry is putting a lot of effort into making it difficult for them to access content. If a viewer has paid for access to content, why shouldn't that viewer be able to decide whether to view it in the living room *or* the bedroom? Consumers are increasingly willing to pay for access to top value content, but in return, expect to be able to access that content when they want to, and on a variety of consumer electronics devices.

SVP presents a way out of the confusion, with a solution that protects the rights of content owners while making it *easier* for consumers to access content in more ways and in more locations.

As a standard chip component which enforces the rules set by the pay TV operator who sells the content, SVP can be used in any type of consumer electronics device. The license defines where content may be

consumed — what types of devices, even which specific devices — and for how long. This ensures that rights owners get paid for their content while enabling viewers greater freedom of access and use than any solution previously implemented. Once consumers have purchased the right to access content, they can use it on any device in their home network, even in a second home, or on portable wireless devices. The SVP is designed to be inherently flexible, giving content providers and distributors more options for packaging and marketing content, further expanding consumer choice

### A SOLUTION FOR EVERYONE

The issue of content protection is not going away; in fact as the digital home becomes more commonplace, content protection is becoming an ever-more complex problem. As proposed, SVP offers a win-win opportunity for all the players in the digital entertainment food chain.

The SVP solution addresses the issue of end-to-end content protection in a wide range of devices, yet does not require a large financial investment. It creates new business opportunities for CE manufacturers, content owners and content distributors, while making it possible for consumers to access high quality digital entertainment on any of their home network devices. Adoption of SVP is a crucial step on the road to realizing the full potential of the digital entertainment revolution.

For further details, visit the SVP website at [www.svp-cp.org](http://www.svp-cp.org), or email us at [info@svp-cp.org](mailto:info@svp-cp.org).