EX PARTE OR LATE FILED

VERNER · LIIPFERT
BERNHARD · McPHERSON AND HAND
CHARTERED

901 - 15TH STREET, N.W.
WASHINGTON, D.C. 20005-2301
(202) 371-6000
FAX: (202) 371-6279

Writer's Direct Dial:
202-371-6206

RECEIVED
MAR 4 1999
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

March 4, 1999

BY HAND DELIVERY

Ms. Magalie Roman Salas
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: Ex Parte Communication in CS Docket No. 98-120

Dear Ms. Salas:

On March 3, 1999, Lawrence R. Sidman and Sara W. Morris of Verner, Liipfert, Bernhard, McPherson & Hand; and David Arland of Thomson Consumer Electronics met with Rick Chessen, Senior Legal Advisor to Commissioner Tristani, concerning issues involved in the aforementioned proceeding. The discussion tracked Thomson's written comments and reply comments filed in this proceeding, as well as topics addressed in the attached documents, which were distributed at the meeting.

In accordance with Section 1.1206 of the Commission's Rules, 47 C.F.R. § 1.1206, an original and one copy of this letter, including attachments, are being filed with your office. Please direct any questions concerning this matter to the undersigned.

Respectfully submitted,

Lawrence R. Sidman

Lawrence R. Sidman

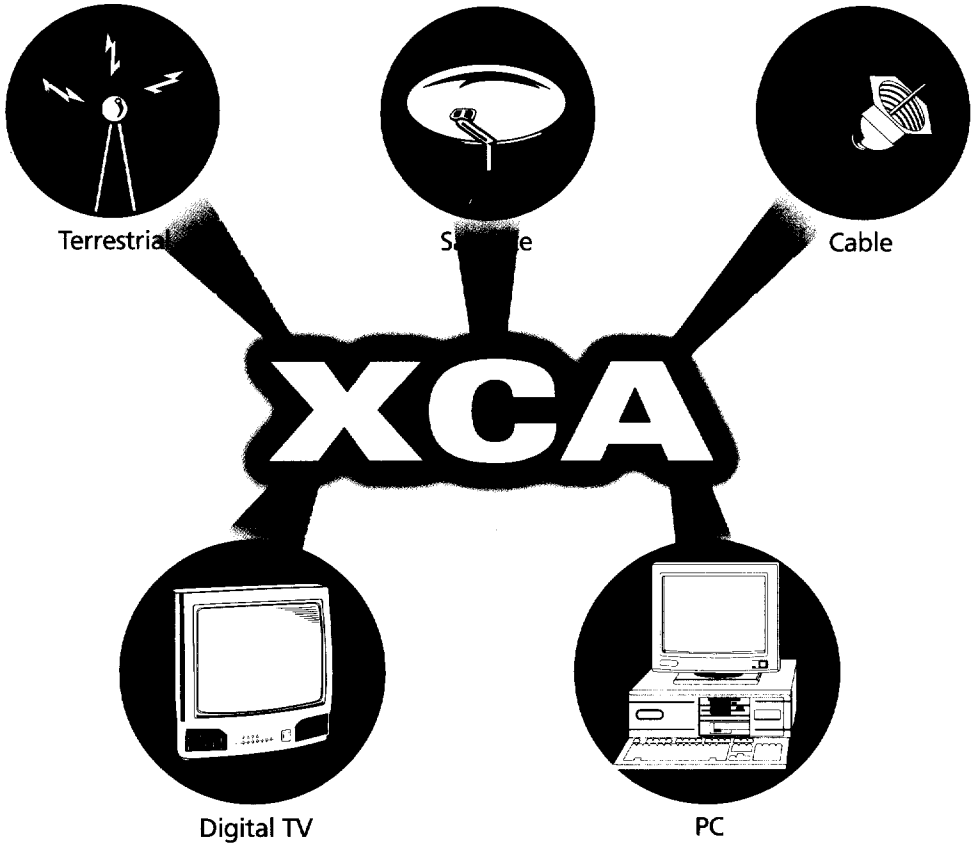
Enclosures
cc (without enclosures): Rick Chessen

0

No. of Copies rec'd
List ABCDE

XCA

A Global Copy Protection System For Digital Home Networks



C O N T E N T S

What is this brochure about?

What is a digital home network?

What is a digital interface?

Why is copy protection needed?

What are the two problems in digital home networks that a copy protection system must address?

What are the fundamental encryption-based approaches for copy protection systems?

Which approach is used by XCA?

What is NRSS?

How are secrets managed in XCA?

How is XCA implemented in CE devices?

What about renewability?

THOMSON CONSUMER ELECTRONICS, INC.

zenith

WHAT IS THIS BROCHURE ABOUT?

In this brochure, Thomson Consumer Electronics and Zenith Electronics present XCA, a global copy protection system for digital home networks. This system:

- protects content both in transmission and in storage
- is applicable to all (one-way and two-way) digital interfaces
- is renewable in a practical and cost-effective manner
- does not use embedded secrets in CE devices
- does not impose device revocation to maintain content security
- provides new business opportunities for content providers by allowing full control over copies

XCA, which stands for "Extended Conditional Access," is separate from, and complimentary to, available conditional access systems.

WHAT IS A DIGITAL HOME NETWORK?

A digital home network is a cluster of digital audio/visual (A/V) devices including set-top boxes, TVs, VCRs, DVD players and general-purpose computing devices such as personal computers.

WHAT IS A DIGITAL INTERFACE?

It is a means by which interaction or communication is achieved between digital A/V devices. Two digital interfaces are now available as Electronic Industries Alliance (EIA) standards for device interconnection. These are:

1) ***EIA-775:*** This standard defines a specification for a baseband digital interface to a DTV. It is based on the IEEE 1394 Standard for High Performance Serial Bus.

2) ***EIA-762 and EIA-761:*** This standard defines minimum specifications for a one-way data path utilizing an 8 VSB or a 16 VSB remodulator in compliance with ATSC Standard A/53 Annex D.

WHY IS COPY PROTECTION NEEDED?

Original copyrighted content is delivered to the digital home network from a number of sources. It may be transmitted via satellite, terrestrial or cable systems or recorded on a digital tape or a DVD. Transmitted or recorded on media, the content may be identified as **"never-copy," "copy-once"** and **"free-copy."** These three states are represented using the Copy Generation Management System (CGMS) bits. The A/V devices in the cluster should obey "playback control," "record control" and "one-generation control" rules as summarized in the following table. To prevent unauthorized copying by non-compliant devices, content needs to be protected by cryptographic means.

	Play	Do not record
	Play	Record and change the CGMS bits to "no-more-copies" in the new copy
	Play	Do not record
	Play	Record

WHAT ARE THE TWO PROBLEMS IN DIGITAL HOME NETWORKS THAT A COPY PROTECTION SYSTEM MUST ADDRESS?

Digital copyrighted content (e.g., a movie) needs to be protected in transmission from one A/V device to another and in storage on magnetic or optical medium (e.g., digital tape or DVD).

WHAT ARE THE FUNDAMENTAL ENCRYPTION-BASED APPROACHES FOR COPY PROTECTION SYSTEMS?

Two fundamental approaches are possible:

1) In the first approach, content can protected by rescrambling across each link, and, if it needs to be stored at its final destination, scrambled under a local key. This approach requires physically secure components in all A/V devices for keeping secrets. For any given link, the source device and the sink device authenticate each other and establish a shared key for scrambling and descrambling.

   Device revocation is an optional feature to shut-off the devices in violation of the copy protection system. Revocation lists are distributed to home networks and can be updated from compliant devices with newer lists, prerecorded content media and compliant devices that can communicate with external sources (e.g., the Internet, cable or satellite systems).

2) In the second approach, content can be kept scrambled until it is displayed for the consumer to watch. Descrambling is performed by an authorized removable security device, such as a smartcard, attached to the display unit. Copy protection systems based on this approach are applicable to both IEEE 1394 and RF Remodulator interfaces, as well as any other digital interface that may be used in the future.

WHICH APPROACH IS USED BY XCA?

Under XCA, the second approach is used. Content is scrambled once at the source (broadcaster/cable/satellite headend), and is descrambled by display devices only. The content remains protected during its entire life cycle.

XCA maps the three basic controls, i.e., "playback control," "record control" and "generational control" into "viewing control." It allows recording of scrambled content, but prohibits viewing if the content is not legitimate. An "illegitimate" content is one that is not an original or a first-generation copy.

Renewable security devices, based on the National Renewable Security Standard (NRSS), are critical elements of this system. They will be used to control access to the content.

WHAT IS NRSS?

The NRSS is a voluntary national standard for renewable security. Recently developed, it provides an architecture to allow the conditional access functionality to be detached from consumer electronics devices such as digital television receivers and digital VCRs.

The NRSS provides two physical designs: Part A defines a removable and renewable security element form factor as an extension of the ISO-7816 standard for smartcards. Part B defines a removable and renewable security element based on the PCMCIA form factor.

The main differences between the two lie in the range of functional capabilities. The interface defined by Part A is limited to 8 electrical contacts and provides serial communication. The interface defined by Part B has 68 electrical contacts for parallel communication. In comparison, Part A devices are smaller in size and less expensive, whereas Part B devices can be more robust and extensible.

However, the attributes common to both parts allow either device type to provide security for applications involving terrestrial, cable and satellite TV services, electronic commerce and telephony.

HOW ARE SECRETS MANAGED IN XCA?

XCA does not involve any management of secrets by the CE manufacturers nor does it require drastic changes in traditional manufacturing processes and practices. As the copyrighted content is scrambled only once, no secrets or cryptographic processes (encryption, authentication, hashing and digital signature generation) are needed in CE devices. The only function included in the system is a one-way function, the definition of which is public information.

In most applications, content is encoded in the MPEG-2 Transport Stream format. Its protection involves two steps:

Content scrambling: Different parts of the content are scrambled with a symmetric algorithm under different keys. For robustness, the key is changed every few seconds.

Key protection: The scrambling keys (i.e., the control words) are derived in a number of ways. They can be generated randomly or derived from Entitlement Control Messages (ECMs). Randomly generated keys are protected using a public-key algorithm or any other method.

Scrambling and key protection take place at the source (i.e., cable/satellite/ terrestrial headend or publishing house). MPEG-2 defines Entitlement Control Messages (ECMs) for carrying the scrambling keys (control words) together with A/V content.

In XCA, the ECMs are extended to contain the CGMS bits and copy protection information as well as control words. Every time copyrighted content (e.g., a movie) is recorded, the extended ECMs (XECMs) are modified through a one-way, irreversible transformation to distinguish copies from the original. These ideas comprise the distinctive features of the XCA architecture, providing a unique way of implementing record control, playback control and one-generational control.

Before viewing is allowed, the smartcard checks how many times the XECMs are modified and responds in accordance with the CGMS bits and the policies of the CA system.

HOW IS XCA IMPLEMENTED IN CE DEVICES?

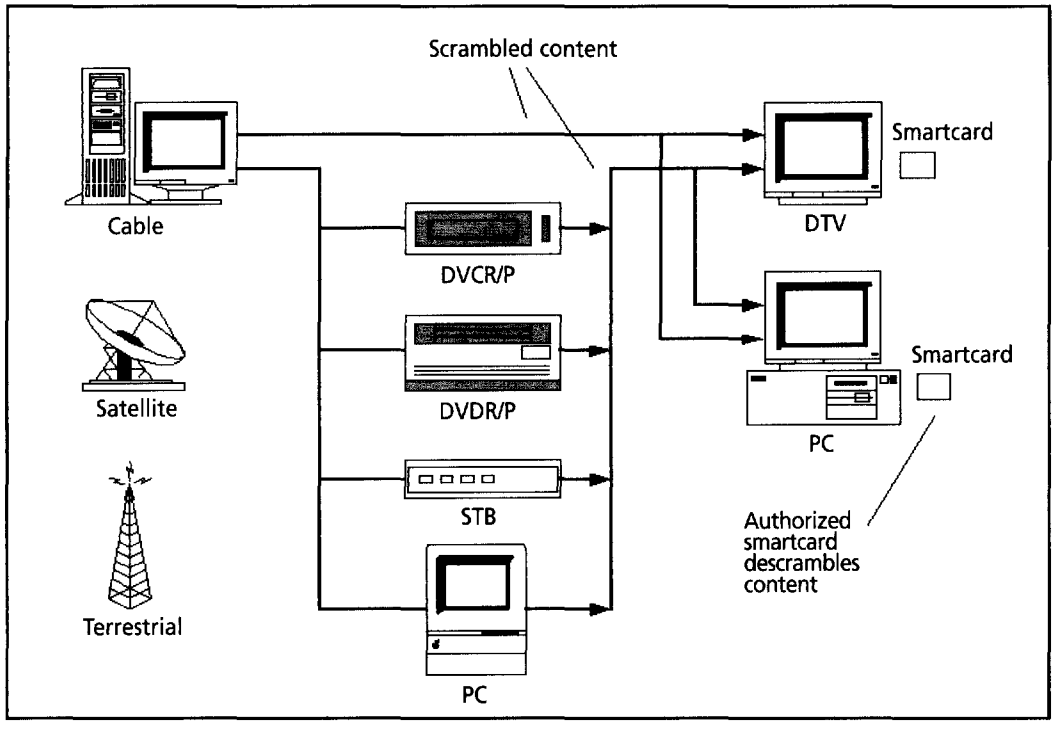
The impact of the system on CE devices is minimal. A summary of the functionality and operation of set-top boxes, display, recording and playback devices is given below. The below figure shows the flow of protected stream from the source to the display unit.

Display Devices

- The display device is the final destination of the digital content for viewing. The DTV is one of the most common display units in home networks.
- The display device receives the scrambled A/V stream from a source (broadcast/cable headend, satellite, cable STB, satellite STB or playback device) and transmits it directly to the smartcard.
- The type of the smartcard depends on the original source of the content. Several different smartcards (cable, satellite, terrestrial, publishing house, etc.) may be in use.
- The card checks if the content is legitimate and behaves in accordance with the rules of the CA system. For example, if it receives a broadcast PPV movie, an OSD prompts the consumer to initiate a purchase offer before the movie starts. If the movie is purchased, a record is stored in the card. The card then recovers the scrambling keys and descrambles the stream. The information about the event (price, start time, length, etc.) contained in the XECMs is used to generate the purchase offer.
- If the display device has an output port, it outputs the same stream it receives. If the input stream is scrambled, for example, descrambled output is not allowed.

Set-Top Boxes

Two scenarios need to be considered for STBs:



The digital set-top-box receives cable or satellite signals. The STB functionality is embedded in the display unit (i.e., the DTV) that receives signals directly from the headend.

In either case, the device functionality depends on the type of the signal.

Cable STB

- Today, the Cable STB is a component of a private CA system run by the cable operator. It receives signals from the cable headend and descrambles the content protected with the private CA system.
- In the near future, the cable operators will remove security from navigation, and STBs will be sold at retail.

- In either model, XCA eliminates the need for descrambling in STBs. Tuning, demodulation and OSD insertion are the functions performed by the STB before the scrambled content is sent to an A/V device.
- The STB performs an additional function depending on the interface type (RF Remod or 1394).
- ***DTV as the receiving A/V device:*** The DTV smartcard has (i) the corresponding decrypting key for recovering the descrambling keys, and (ii) the private descrambling engine.
- ***DVCR or DVDR as the receiving A/V device:*** Creates a copy as described.

Satellite STB
The functionality of the satellite STB is as described for the cable STB.

DTV with Cable STB Functionality
- The DTV receives signals from the cable headend.
- The cable smartcard has (i) the decrypting key for recovering the descrambling keys, and (ii) the private descrambling engine.

DTV with DBS STB Functionality
- The DTV receives signals from the satellite.
- The DBS smartcard has (i) the decrypting key for recovering the descrambling keys, and (ii) the private descrambling engine.

STB As a Network Access Device
In an optional architecture, the STB may descramble content coming from the headend and rescramble it in accordance with XCA.

Recording Devices
- Among the A/V devices, the recorder is the only device that has copy protection functionality.
- If a movie is to be recorded, the recorder detects and modifies the XECMs.
- If the content is not scrambled, it is copied as is.
- In general, every time a scrambled movie is copied, its XECMs are modified once more. This allows the smartcard in the display device to determine how many times the original movie has been copied.
- Optionally, instead of being embedded in the recording device, the XECM modification functionality can be assigned to a smartcard. In this case, the recorder needs to have a smartcard reader.

Playback Devices
- Every playback device (e.g., a DVC or DVD player) sends the scrambled content together with the XECMs to the display or recording device.
- Another output may be CSS-protected content.

Pre-recorded A/V Data Formats not Compliant with XCA
- The market will offer pre-recorded content with other data representations. One example is the DVD Program Stream format for A/V content. The contents of a DVD Movie Disc are protected with the proprietary Content Scramble System (CSS) scheme.
- Presently, the DVD players send the descrambled and decompressed content to the display unit in-the-clear. This output is analog because the first generation DVD players do not have a digital output. As the consumer buys a DVD with unlimited viewing rights, there are no conditions for watching a DVD movie.
- When a CSS-protected content needs to be copied, the DVD player outputs it without descrambling. After performing CSS-descrambling, the DVD recorder converts the content from Program Stream format to Transport Stream format and scrambles it using a common scrambling algorithm (e.g., DES). The DES keys are encrypted with the public key carried with the content. For viewing of this copy, an appropriate smartcard is required.

General-Purpose Computing Devices
- The personal computer (PC) is one of the most common general-purpose computing devices.
- It can be used as a display, playback or recording device.

WHAT ABOUT RENEWABILITY?

The XCA system is renewable as the descrambling is performed by a removable security device, e.g., a smartcard. The end-customer knows that the smartcard controls access to premium content, and would therefore contact the smartcard provider for renewal.

As all copy protection systems can undoubtedly be compromised in time, this type of renewability is much preferred and convenient when compared with alternatives involving embedded secrets.

For more information about XCA, please contact Dave Arland of Thomson Consumer Electronics, (317) 587-4450, ArlandD@tce.com or contact John Taylor of Zenith Electronics Corporation, (847) 391-8181, jtaylor@zenith.com

Copyright 1998, Thomson Consumer Electronics, and Zenith Electronics Corporation

CONSUMER INTERESTS AND CONSUMER CONTROL MUST GOVERN THE QUEST FOR CABLE-DTV COMPATIBILITY

Thomson Is Committed to Resolving DTV-Cable Compability Issues In a Manner That Best Serves Consumers. DTV-cable interoperability is a top priority for Thomson. Through recognized standards-setting bodies and in cooperation with the cable industry, Thomson continues to work vigorously to *guarantee* that, at every stage of the transition, America's 70 million cable subscribers are no less capable of exploiting all of the functionality Thomson's feature-rich DTV products will put in their hands -- and choosing freely among all available DTV services and features -- than those receiving DTV services off-air. Such a guarantee is *essential* to ensuring, as the Commission must, that consumers, not cable companies or any other single interest, retain ultimate control over how they will participate in the DTV revolution. Until important DTV-cable compatibility issues (including copy protection, as discussed below) are resolved, this guarantee to consumers can only be realized if every cable operator provides an ATSC-compliant (*i.e.*, 8 VSB) output of broadcasters' DTV signals. Thomson is encouraged by the recent announcements of two cable MSOs that they plan to provide such an output (albeit on a limited basis) and urges the Commission to extend that obligation to all cable systems until an alternative approach is available to consumers.

Achieving DTV-Cable Compatibility Will Require Time. Thomson Cautions the Commission To Adopt a Transitional Approach That is Both Realistic and Geared Toward Solutions That Are Optimally Consumer-Friendly. As the Commission confronts the issues surrounding how best to ensure optimal compatibility between cable systems and digital television services, it should not create unrealistic expectations, particularly early in the transition, lest it thrust consumers into an environment in which the search for the best solution *for consumers* becomes lost in the search for any quick solution. To that end, Thomson urges the Commission to adopt a transitional approach to cable compatibility which ensures, both in the short- and long-term, that no consumer subscribing to cable is denied either the ability to receive all available DTV signals in their intended quality and entirety, or the ability to enjoy all the receiver-based features which consumer electronics manufacturers such as Thomson will build into their receivers. Specifically, as the attached chart portrays, Thomson foresees a migration path that begins, in 1998, with an 8 VSB output by all cable operators, evolves to include a component video and/or 1394 interface (once complete), and concludes with the availability of cable-ready DTV receivers.

It Is Essential That Control Over The DTV Services and Features That Are Available to Consumers Rests Squarely With the Consumer, Not His or Her Cable Operator. Consumers must be confident, when purchasing any DTV product, that they will be able to enjoy the full functionality of that product, as well as all broadcaster-delivered DTV services, regardless of whether they receive DTV signals via cable or off-air. At its core, the debate over cable compatibility centers on the issue of control. It is Thomson's firm belief that a successful transition demands that that control not reside with anyone other than the *consumer*. Cable operators must not be allowed to degrade or diminish any DTV data intended for receipt by the consumer, nor deny consumers access to a competitive array of features and functions (including electronic program guides). Specifically, the Commission should:

- Require cable operators to retransmit DTV broadcast signals to their subscribers without material degradation (*i.e.*, downconverting an HDTV signal to any lower resolution digital video format must be expressly forbidden);

- Require cable operators to deliver to their subscribers all data transmitted by broadcasters in the entirety of their 6 MHz DTV channel, including the maintenance of program-related information within the PSIP (*i.e.*, any alteration or deletion of USER data or broadcaster-transmitted navigational information and program-related information services must be expressly forbidden).

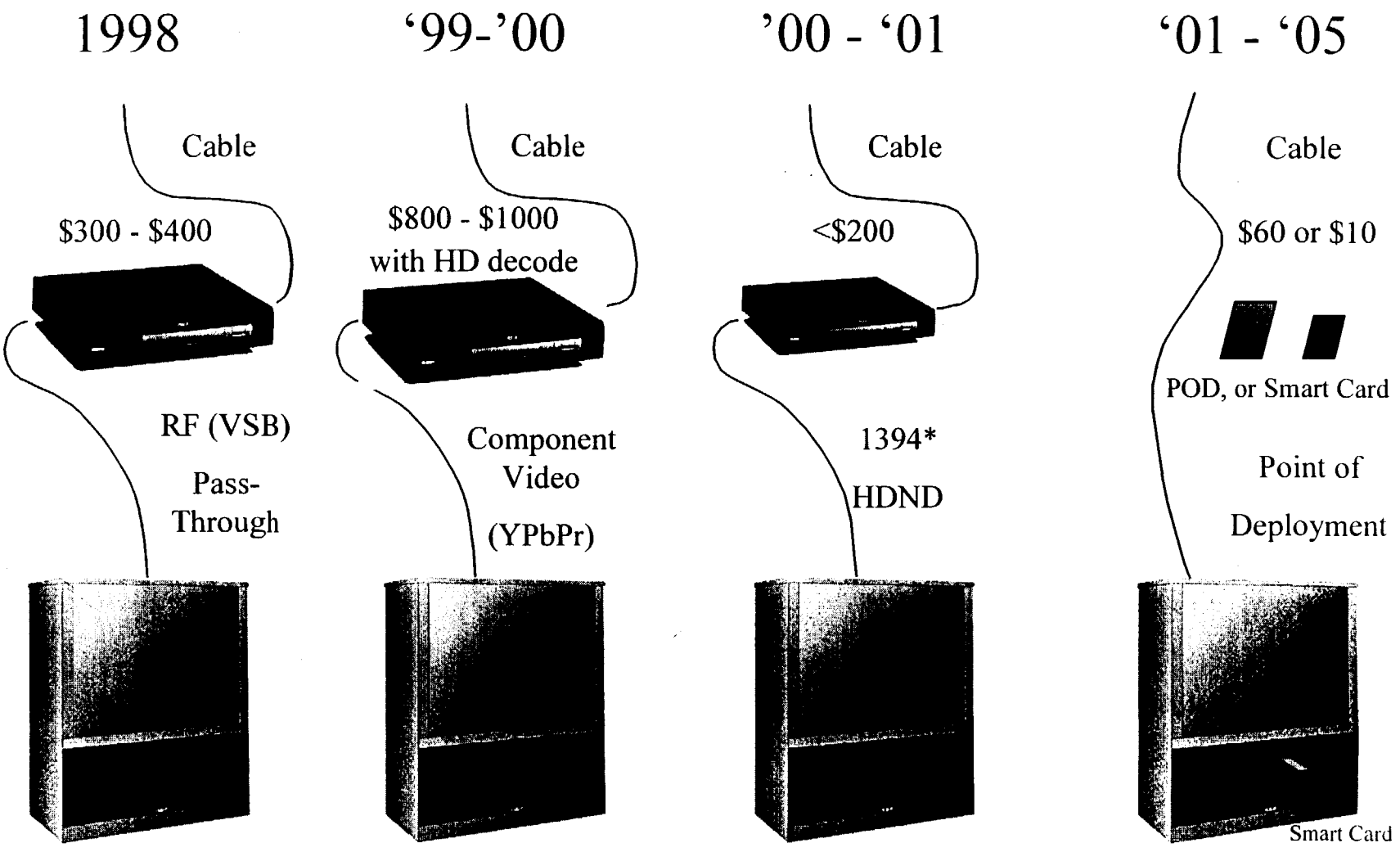
The IEEE 1394 Interface Standard Requires Agreement on a Copy Protection Standard, and, Even Then, Is Not the Optimum Solution for Consumers. Thomson strongly cautions the Commission not to view the IEEE 1394 interface as a "panacea" to cable compatibility with DTV. For an ever-growing number of reasons, such an approach is far from perfect. Moreover, given the lack of agreement on critical copy protection issues, the 1394 interface likely will be eclipsed by other technically superior and consumer-friendly solutions -- ultimately the availability of "cable-ready" DTV receivers. Thomson therefore urges the Commission to avoid viewing the 1394 interface as anything more than an interim solution to cable compatibility.

These broader concerns aside, Thomson has other serious reservations about the recently announced adoption of standards for the 1394 standard, particularly its proposed use of the so-called "5C" copy protection standard. The 5C approach falls far short of technical and consumer-acceptability on several counts: (1) its inability to prevent multiple generations of copies of digital data (i.e., it protects data only in transmission, but not in storage); (2) its reliance on embedded security chips (which, once (inevitably) compromised, could only be renewed by recalling and retrofitting *every device in which it resides*); and (3) perhaps most pernicious to the interests of consumers, its proposed "device revocation" would have the effect of completely or partially disabling a consumer's DTV receiver (or other device) immediately upon its receipt of data thought to be violative of the copy protection scheme. The unprecedented assumption of authority to deactivate the personal property of our customers -- particularly given the possibility of false reporting -- and the angry consumer backlash that would follow the revocation of any device -- makes the 5C approach highly undesireable.

As discussed in the attached summary, Thomson and Zenith have developed a global copy protection solution, called XCA ("Extended Conditional Access") that, unlike 5C, protects content in both storage *and* transmission (thus defeating attempts to create multiple generations of copies); employs the more practical "smart-card"-based approach to security, thus preventing the need for a consumer to haul his or her DTV device back to the retailer should the system be compromised (or "hacked"); and eliminates the undesireable "device revocation" scheme to ensure content security. Moreover, XCA is applicable to both one <u>and</u> two-way digital interfaces (including the RF interface and the 1394 firewire) and will be licensed freely and without discrimination. Thomson and Zenith believe the XCA copy protection system addresses the concerns of the cable, consumer electronics, motion picture and computer industries, and protects the interests of its consumers.

Thomson Will Offer Consumers a Wide Array of Feature-Rich DTV Products At Various Prices And Envisions Substantially Lower Prices As Early As The End of 1999. Consistent with the introduction of any new consumer electronics product -- which typically begins with the most elaborate and expensive products and then moves to products designed for more of a mass market, Thomson will introduce a wide range of multi-functional DTV products, including rear projection and direct view HDTVs, in a variety of screen sizes, as well as digital-to-analog set-top converters. All of Thomson's DTV products will be capable of receiving and displaying: (1) all analog broadcast and cable delivered signals; (2) all terrestrial digital television signals (including all 18 ATSC formats); standard digital satellite (DBS) services; and high definition digital satellite services from DBS services DIRECTV and USSB. Thomson's line of HDTV receivers will enable consumers to make the early leap to digital television in a manner that offers consumers maximum DTV functionality at a very competitive price which, when adjusted for inflation, is comparable to the cost of the pioneering black and white and color TV receivers.

Interface Migration Path



Incorporating Cable Functionality into DTVs

Extended Conditional Access (XCA)

A Comparison to 5C in Layman's Terms

Presented by
Thomson Consumer Electronics
Zenith Electronics Corporation

An Executive Summary

Introduction

The major hurdle that remains in the ratification of the 1394 interface spec is a method of copy protection that meets the requirements of the CE, PC, Cable and Entertainment industries. Five major companies, the 5C, have introduced a system to protect digital information in transmission, which, admittedly, is not intended to address the complex issue of protecting digital content in storage: on DVD-RAM, digital tape, or on the hard drives of PCs and servers. Thomson and Zenith have developed a global copy protection solution, called XCA, that protects content in both storage and transmission. Furthermore, it is superior in its application to both one-way and two-way interfaces, and its practical approach to system renewability, which will be necessary when encryption schemes are inevitably compromised. These companies seek support to influence the standards-setting process in order to realize the copy protection method that is the most beneficial, renewable and easiest to implement.

A New Paradigm

In considering copy protection methods, there are two fundamental approaches. You can either protect the content by rescrambling across each link, or keep the content scrambled until it is displayed. Under XCA, content is only encrypted once at the head end or by the content creators, and is only decrypted by display devices. This should be attractive to the content owners, because they are assured that all content becomes encrypted properly, prior to distribution. (Similarly, the content could be encrypted by distributors, such as media publishers and cable and satellite head end operators.) The content remains encrypted using either public or proprietary cipher methods, during its entire life cycle. Two-way device authentication is not required, because only those displays with a smart card slot and an authorized, current decoder card will be able to display the high value content.

XCA, which stands for Extended Conditional Access, is a copy protection system that is separate from, and complimentary to, any available conditional access systems. As long as the CA systems are based upon the widely used MPEG-2 standard, they may be changed, or updated periodically on cable or satellite systems with no effect on the XCA system.

By contrast, 5C, does not protect content in storage. It is encrypted and decrypted each time it crosses a 1394 interface, and may be stored in the clear. The problem here is that it becomes much easier for perpetrators to access and replicate the stored content. The worst scenario involves replicating content on computer mass storage devices, and then distributing the copies over the Internet, or downloading these copies onto digital tape. The 5C companies are reported to be working on a fix for this, but it is a well-known cryptographic fact that extending 5C to cover storage protection is not possible.

Renewability – No Embedded Secrets

The robustness of any security scheme should always be assumed to be vulnerable. Given sufficient time, and subsequent developments in technology and methodology, the compromise of any encryption scheme is inevitable. Therefore, the practical renewal of the global encryption method should be of paramount importance to any company that has based its primary business on consumer devices and/or interactions.

Because no industry is subject to mandatory recognition and processing of watermark technology to protect content through legislation, encryption seems to be the only alternative. In any encryption scheme, secrets to encode and decode are mandatory. The primary issue becomes where to store these secrets? 5C proposes that the secrets be embedded on a chip inside each device that has a 1394 interface, including cable and satellite decoders, VCRs, DVD players, PCs and digital TVs. These secrets would include a unique identification, or certificate for each device, and a set of fixed "keys" used for encoding and decoding.

Thomson and Zenith oppose the notion of embedded secrets for two important reasons. First, we would always be subject to an uncertain supply of chips and device certificates to place into our devices, and may not have immediate access to any latest revision levels. This creates a commercial disadvantage for non-5C companies in time to market, and product cost (licensing fees). The second, more important, reason to oppose embedded secrets is that it is not economically practical to renew the encryption system, once it is compromised. The only way to renew the system would be to recall every cable and satellite decoder, VCR, DVD player, PC and digital TV with a 1394 interface, and reprogram new certificates and keys into their EEPROM chips. The profit margins on these devices would have to double in order to pay for the "insurance" against such a liability.

We believe that any system will eventually have to be renewed quickly, and affordably. Using the XCA solution, the only devices that would need to be renewed would be the "smartcards" (either NRSS A or B could be used) on display units, namely TVs and PCs. Rather than a recall, new smartcards could be issued within a few weeks in a mass mailing to all registered users by the CE manufacturers, in cooperation with the content distributors or CA providers. Additionally, retailers may want to be involved in smart card distribution to those display (PC) owners who aren't service subscribers. Not only would the cost per unit be much less than a physical recall, but also there would be much fewer devices to renew.

Revocation

As Consumer Electronics manufacturers, whose profitability and brand image depends on satisfied consumers, Thomson and Zenith are fundamentally opposed to the notion of device revocation proposed under the 5C method. Their solution sets up a licensing authority that will have the power to revoke individual devices that are reported to be violating the CP scheme. These reported devices' identities are added to a "revocation list", which is published as a header to all new content releases, and broadcast via cable and satellite. Any legitimate device is then obligated to compare the identity of any other device on the 1394 network to this list before transmitting data, and if it encounters a known violator, simply refuse to transmit the content to that device. Since these devices will no longer be capable of decrypting content across the 1394 interface, they are essentially rendered worthless.

Needless to say, this will be quite upsetting to someone who has invested thousands of dollars in a new HDTV. Once revoked, they will start making angry phone calls to their retailer, the CE manufacturer, their cable company, and then their lawyers. The resulting backlash from consumer groups might result in boycotts, class action suits, and federal regulation. It would be particularly difficult to justify the continued use of such as system due to its susceptibility to false reporting and the lack of any judicial "due process" by which consumers' property is rendered useless.

Regarding the systems' susceptibility, revocation relies on a few assumptions that may not be true. The first is that violating devices <u>will</u> be reported. This may not be true because reporting will only take place

via a networked return path, such as a cable network. Even not-so-clever pirates will realize that they have to make their illegal copies "off network". The second assumption is that honest users will somehow be fairly warned that they are violating terms of an implicit contract, and that if they continue, their device will be destroyed. This may not be true, especially since many users do not read manuals, or for that matter read English at all. Further, some may try making copies without the use of a monitor, and without visual feedback, have no means of knowing they are violating any terms. The most critical assumption is that only the violating devices will be reported. Recent copy protection systems that have been deployed with embedded secrets have proven to be broken or circumvented rather easily. The validity of the above assumptions is therefore questionable.

We can think of several instances in which the identities of honest devices may get reported to the licensing authority. Beyond industrial sabotage (which shouldn't be ruled out), there are two critical scenarios which must be guarded against.

- First, an honest consumer could become the victim of sophisticated hacker, who clones the certificates of valid devices. This could be done by a dishonest repairman, or assembly worker, or possibly by a sufficiently programmed computer which finds a way to randomly generate copies of certificates, and continues to request access to content with them until one is found that works. After time, that device's certificate will be revoked (along with that of the honest consumer) and the hacker will move onto the next available certificate.
- Second, an honest consumer could become the victim of an honest mistake. With mischievous and naïve children around many households, it is conceivable that children will make copies or somehow violate the 5C terms, either with or without knowledge or malice. As a result, their innocent parents will lose the rights to view content, and may have no knowledge of their child's activity.

We are quite concerned about the unprecedented assumption of authority to deactivate the personal property of our customers. We believe that all consumer electronics firms should vigorously oppose the notion of revocation. Who will accept the responsibility and liability associated with this?

With the XCA approach, the CA provider and/or content provider are directly responsible for the copy protection system. If there is an alleged pirate device, they can disable that specific smart card through its removal from the user. This is an important distinction, as it places the company making money from the pay-per-view or CA system directly responsible for the operation and maintenance of the system. This will ensure the system is always kept up-to-date and the consumer will always know who to approach to get the situation fixed, as the smartcards will only be distributed from the CA provider or content provider.

Effect on CE devices

As mentioned above in the discussion about renewal, the 5C solution would require all devices with a 1394 interface to have embedded secrets. This would add approximately ($3.00??) to the manufacturing cost of every cable and satellite decoder, VCR, DVD player, PC and digital TV with a 1394 interface, due to incremental chips required, as well as licensing and administration fees. With these secrets being embedded in each device, the inevitable cost of a recall to renew the system could add as much as ($30 ??) per unit in accrued liability. Even if the secrets were not embedded, and the system was re-architected with smart cards in every device, this would still add approximately ($12 ??) per device for the reader and for the card.

Alternatively, XCA would only have an impact on the production of digital content at the source and on those CE devices designed to display such content. Since not all PCs may need to ship with 1394 interfaces, to receive multimedia content on local networks, XCA may have no impact on most PCs. However, those "multimedia PCs" which will be sold to homes will need a Smart Card reader (probably just a free PCMCIA/NRSS B slot) and some software to decode data. There will be no impact on PC monitors, since images will then be transferred to from the PCs via the RGB analog interface. All digital TVs will require a Smart Card reader, to decrypt protected content. The card could be either the decoder card shipped with the TV, or in the future, could incorporate conditional access (CA) functionality from a

cable or satellite operator, in a POD implementation. So, while the cost impact to add smart card readers to DTVs and some PCs may also be approximately ($12 ??) per device, the overall system cost on all components and on system maintenance would be much less than in the 5C system.

Importance of One-Way Interfaces

Each CP solution will have a significant amount of overhead to license, administer and potentially renew each system. Therefore, one of the most important considerations in selecting a system should be its utility in as many applications as possible. The XCA solution is applicable to not only the 1394, but also one-way interfaces, such as the Rf Remodulator, EIA-761, and can be extended to other interfaces as well, and incorporated into a Point of Deployment (POD) module.

The Rf Remod interface is especially important to include because it is the least expensive method to move digital video to a display device. In cases where the display will not need to send signals back to the source devices, an Rf Remod interface is adequate and will enable more affordable displays. CE manufacturers are all very interesting in using this interface (and reducing manufacturing costs) whenever possible, but it is much less valuable without copy protection.

Conclusion

Digital copy protection for home networks is a very complex problem that affects consumers' relationships with the providers of equipment, service and content, and their rights to use them. The problem is too large and difficult to approach in a piece-meal fashion, one system at a time, which will result in weak, expensive, and complex solutions. The ideal solution must be global, provide robust security for both transmission and storage, support all digital interfaces, and not violate consumers rights to use their equipment. In spite of the pressure felt by the CE and Cable industries, sufficient time must be allocated to develop a complete solution

XCA is a more complete and secure solution than that proposed by the 5C companies. It protects content in both storage and in transmission. It is applicable to both one and two-way digital interfaces, and can be extended to Point of Deployment (POD) architectures. XCA is renewable in a practical and cost-effective manner and does not impose a device revocation scheme to ensure content security. XCA will only add cost to display devices and will be licensed freely and without discrimination. Thomson and Zenith seek the understanding and support of the Cable, Consumer Electronics, Motion Picture and Computer industries to promote the copy protection solution that makes the most sense.

NEW DIGITAL COPY PROTECTION PROPOSAL WOULD SECURE AUTHORIZED COPIES

One-time digital home recording protects both consumer's rights and recorded content

WASHINGTON, D.C., November 13, 1998 - A new technology to protect against unauthorized copying of television programs and movies in the digital age will soon be reviewed by the industry working group charged with examining copy protection approaches for digital interfaces.

Thomson Consumer Electronics and Zenith Electronics Corporation are jointly proposing a digital copy protection method dubbed "XCA" for Extended Conditional Access. XCA allows for copy protection of home recordings on both one-way and two-way interfaces and uses a renewable security system. XCA is easily and inexpensively implemented for all digital interfaces (such as the EIA-762 RF Remodulator Standard and the IEEE 1394 Interface) that will be used between digital television sets and other digital devices, including digital VCRs, DVD players, and cable TV equipment in the near future.

"Other copy protection proposals provide no mechanism to prevent multiple generations of copies. Any copies of a program made by a consumer might be easily duplicated by others - including video pirates," explained Ed Milbourn, product manager for Digital Television at Thomson Consumer Electronics. "The XCA method will allow copies only of encrypted data, with decryption occurring just in the display device. In the architecture, only original content or first generation copies would be displayed," he said.

Tom Sorensen, Zenith vice president, Digital Business Development, said "We believe that those who produce movies and TV shows should be concerned that some copy protection schemes do nothing to prevent recording the data in-the-clear. Extended Conditional Access is an elegant, simple solution that addresses this issue head-on."

The XCA method avoids complex two-way key exchange schemes and allows for simple one-way copy protection across any digital interface. The join Thomson/Zenith proposal also eliminates the need for embedded software secrets in consumers' television sets or recording machines that could someday be "hacked."

Another major problem with the other proposals is that they are interface-specific. Manufacturers would be required to support different copy protection solutions if they choose to implement different digital interfaces. This is likely not acceptable to the consumer electronics industry as it introduces unnecessary complexity to digital product design and manufacturing, resulting in a cost increase, Milbourn explained.

Thomson and Zenith - among the largest TV marketers in the U.S. and accounting for about one-third of all TV sales - plan to submit their XCA proposal to an engineering working group of the Consumer Electronics Manufacturers Association (CEMA), a committee formed to evaluate the impact of different architectures for protecting copyrighted digital content on consumer electronics devices.

"Digital copy protection is important for consumer recording devices and also for the successful rollout of digital television throughout the United States," Zenith's Sorenson said. "Digital transmissions can be recorded and duplicated without degradation - a key improvement over analog recording. This necessitates an effective and flexible means of preventing the creation of multiple generations of perfect copies of digital entertainment content.

With XCA, manufacturers would not be required to build overly complex software into consumer devices. Some copy protection schemes proposed by other companies would allow a cable company or movie studio to single-handedly disable a television or VCR through the cable TV connection. This process, while attractive to some in the video content business, would mean a sweeping change in how consumer products are used. Consumers would be forced to determine what led to the deactivation, and how best to restore the product's usefulness.

"The beauty of the XCA proposal is its simplicity. It's easily renewable with a simple 'smart card,' much like current digital satellite receiving systems. And our method would keep pirates at bay in the digital environment," Thomson's Milbourn said.

About Thomson

The nation's largest manufacturer and marketer of home entertainment products, Thomson markets under the RCA, PROSCAN, and GE brand names. Thomson makes and sells TV sets, VCRs, digital satellite receiving systems, camcorders, digital video disc players, and wide range of consumer audio and communications products. Thomson is based in Indianapolis, where the company's technical center employs more than 700 engineers and technicians for audio/video product research and