

James H. Barker
Direct Dial: 202-637-2231
james.barker@lw.com

555 Eleventh Street, N.W., Suite 1000
Washington, D.C. 20004-1304
Tel: (202) 637-2200 Fax: (202) 637-2201
www.lw.com

LATHAM & WATKINS LLP

June 18, 2007

VIA COURIER

Federal Communications Commission
Media Bureau
P.O. Box 358205
Pittsburgh, PA 15251-2505

FIRM / AFFILIATE OFFICES

Barcelona	New Jersey
Brussels	New York
Chicago	Northern Virginia
Frankfurt	Orange County
Hamburg	Paris
Hong Kong	San Diego
London	San Francisco
Los Angeles	Shanghai
Madrid	Silicon Valley
Milan	Singapore
Moscow	Tokyo
Munich	Washington, D.C.

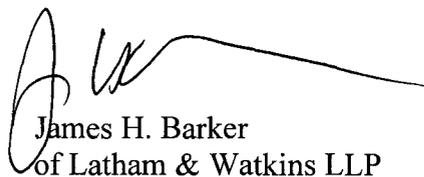
Re: In the Matter of Northeast Oklahoma IPTV Providers Petition for Clarification or, in the Alternative, Waiver of Sections 76.1204(a) and (b) of the Commission's Rules

Dear Sir or Madam

On behalf of Northeast Oklahoma IPTV Providers, we submit an original and four (4) copies of the above-referenced Petition for Clarification or Waiver. Also enclosed is a completed FCC Form 159 and a check in the amount \$1,250 to cover the required filing fee. We have filed a copy of this Meditation electronically in CS Docket 97-80.

Please contact me if you have any questions regarding this matter.

Sincerely,



James H. Barker
of Latham & Watkins LLP

Attachments

**Before the
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554**

In the Matter of)	
)	CS Docket No. 97-80
Northeast Oklahoma IPTV Providers)	CSR -
Petition for Clarification or,)	
in the Alternative, Waiver of)	
Sections 76.1204(a) and (b))	
of the Commission's Rules)	
)	

PETITION FOR CLARIFICATION OR WAIVER

James H. Barker
Cameron Smith*
of Latham & Watkins LLP
555 Eleventh Street, NW, Suite 1000
Washington, DC 20004
(202) 637-2200
Counsel for Northeast Oklahoma IPTV Providers

June 18, 2007

*Admitted in New York. Not licensed to practice law in the District of Columbia; all work supervised by a member of the D.C. Bar

**Before the
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554**

In the Matter of)	
)	
Northeast Oklahoma IPTV Providers)	CS Docket No. 97-80
Petition for Clarification or,)	CSR - _____
in the Alternative, Waiver of)	
Sections 76.1204(a) and (b))	
of the Commission’s Rules)	

PETITION FOR CLARIFICATION OR WAIVER

I. INTRODUCTION

Pursuant to Section 629(c) of the Communications Act of 1934, as amended¹ (the “Act”), and Sections 1.3, 76.7, and 76.1207 of the Commission’s Rules,² the Northeast Oklahoma IPTV Providers,³ respectfully request that the Commission clarify they are in compliance with, or, in the alternative, grant a limited waiver of the separate security and “commonly used interface” requirements set forth in 47 C.F.R. §§ 76.1204(a) and (b).

Oklahoma IPTV Providers are rural local exchange carriers using Internet Protocol Television (“IPTV”) technology to enter the Multichannel Video Programming Distributor (“MVPD”) market. Three years ago, Oklahoma IPTV Providers introduced their IPTV service, and currently have approximately 1,100 IPTV subscribers. Petitioners’ customers receive video

¹ 47 U.S.C. § 549(c).

² 47 C.F.R. §§ 1.3, 76.7, and 76.1207.

³ The Northeast Oklahoma IPTV Providers include as members the Cimarron Telephone Company, Pottawatomie Telephone Company, Cross Telephone Company, Cim-Tel Cable, and Cross Cable LLC (hereinafter “Oklahoma IPTV Providers” or “Petitioners”). Cim-Tel Cable and Cross Cable LLC provide distribution and related functions while the telephone company entities provide billing, customer support, and other retail functions.

over a broadband connection delivered to the home over fiber-to-the-home or hybrid fiber-copper loops. Oklahoma IPTV Providers' subscribers are located in northeast Oklahoma and the majority of these subscribers migrated from traditional incumbent cable service or from a direct broadcast satellite service. Petitioners' IPTV service relies on Verimatrix to provide encryption technology for content protection and Myrio as its middleware provider.

The Oklahoma IPTV Providers believe they are in compliance with Section 76.1204(a) and (b)'s separate security and commonly-used interface requirements because their downloadable security solution is separate from the navigation functions in their set-top boxes, and their conditional access interface is commonly used by multiple consumer electronics ("CE") vendors. The Oklahoma IPTV Providers support the request for clarification of common interface criteria for IPTV devices suggested by NTCA and OPASTCO in their recent Petition for Clarification or Waiver.⁴

However, if the Commission has not issued such a clarification by July 1, 2007, Oklahoma IPTV Providers respectfully request a limited waiver (to the extent one may be required) until such time as the FCC clarifies the criteria for satisfying the common interface requirement of Section 76.1204(b) and vendors have a reasonable opportunity to comply, or until such time as a national standards organization can develop an open interface standard. A waiver would be appropriate in these circumstances because it would allow Oklahoma IPTV Providers — new MVPD entrants relying on emerging technology — to maintain continuity of service to their very small number of subscribers in rural communities in northeast Oklahoma.

⁴ *NTCA-OPASTCO Petition for Clarification or Waiver of 47 C.F.R. §§ 76.1204(a) and (b)*, CS Dkt. No. 97-80 (filed May 4, 2007) (hereinafter "NTCA-OPASTCO Petition").

II. OKLAHOMA IPTV PROVIDERS' DOWNLOADABLE, SEPARATE SECURITY TECHNOLOGY RENDERS THEIR DEVICES COMPLIANT WITH § 76.1204

When Section 76.1204 of the Commission's rules was adopted in 1998, the majority of MVPD providers delivered programming via traditional coaxial cable technology. Innovative technologies such as IPTV have emerged since that time. As the pending NTCA-OPASTCO Petition explains, downloadable security is a universal feature of IPTV.⁵ Thus, by their very design, IPTV systems like the ones deployed by Petitioners comply with Section 76.1204(a) because they rely on downloadable, separate conditional access functions.⁶ Therefore, Petitioners respectfully submit that they are in compliance with Section 76.1204(a) because they rely on a downloadable and non-integrated conditional access technology.

The Commission has issued a general acknowledgement that downloadable security technology that provides for common reliance on an open standard satisfies the Commission's rules.⁷ The NTCA-OPASTCO Petition asks the Commission to clarify that IPTV devices that rely on a separate, downloadable conditional access function are in compliance with Section 76.1204(a). Granting such a clarification would be consistent with the Commission's Public Notice regarding the use of Beyond Broadband Technology's solution, where it stated that downloadable security solutions comply with the Commission's Rules.⁸ In order to remove any uncertainty about the application of this ruling to IPTV devices, Oklahoma IPTV Providers

⁵ *NTCA-OPASTCO Petition*, at 4.

⁶ *IPTV Operators Group Petition for Waiver of 47 C.F.R. § 76.1204(b)*, CS Dkt. No. 97-80 (filed June 1, 2007) (hereinafter "IPTV Operators Group Petition").

⁷ *Commercial Availability of Navigation Devices*, CS Docket 97-80, Second Report and Order, 20 FCC Rcd 6794, ¶ 35 (2005) ("*Second Report and Order*").

⁸ *See Commission Reiterates That Downloadable Security Technology Satisfies The Commission's Rules on Set-Top Boxes And Notes Beyond Broadband Technology's Development Of Downloadable Security Solutions*, CS Docket No. 97-80, Public Notice, 22 FCC Rcd 244 (January 10, 2007).

support the NTCA-OPASTCO Petition’s request for explicit clarification that IPTV providers that make use of a downloadable security access function are in compliance with Section 76.1204(a). And in considering the instant Petition, the Commission should reaffirm that principle as applied to Oklahoma IPTV Providers.

III. PETITIONERS’ CONDITIONAL ACCESS EQUIPMENT EMPLOYS A COMMONLY USED INTERFACE AND IS COMPLIANT WITH § 76.1204(B)

Section 76.1204(b) provides that “[c]onditional access function equipment . . . shall be designed to connect to and function with other navigation devices available through the use of a commonly used interface or an interface that conforms to appropriate technical standards promulgated by a national standards organization.”⁹ This provision, which was adopted with traditional cable technology in mind, does not address how devices that rely on emerging technologies — for which national standards remain under development — can comply with its terms. The Commission has “declined to specify any particular standard . . .” for Section 76.1204(b)’s interface requirement, and a national standard for an IPTV conditional access interface has yet to emerge.¹⁰ Nor has the Commission clearly defined the term “commonly used interface,” leaving Petitioners uncertain as to whether their vendors’ solutions will be deemed compliant.

NTCA and OPASTCO have proposed a clarification under which an interface would be deemed “commonly used” if it (a) connects to and functions with the navigation devices of more than one consumer electronics vendor, or (b) is publicly offered via licensing to CE vendors. Petitioners strongly support this clarification and believe it complies with the letter and spirit of Section 76.1204(b). The purpose of Section 629 of the Act is to enhance competition for

⁹ 47 C.F.R. § 76.1204(b).

¹⁰ *Second Report and Order*, 20 FCC Rcd 6794, 6809 n.136.

navigation devices by preventing cable operators from integrating proprietary security mechanisms with the basic navigation device. In an attached statement, Petitioners' middleware provider, Myrio, which enables the conditional access interface between the consumer's set-top box and the video programming distributor's content, makes clear that its technology functions with the navigation devices of more than one consumer electronics manufacturer, *and* that it publicly offers licensing to CE vendors via an open interface.¹¹ Myrio can interface with devices made by at least nine different set-top box manufacturers, including Motorola, Samsung, and Scientific Atlanta, and it can operate with the conditional access and encryption technologies of at least eight different vendors, including Verimatrix and Widevine.¹² Petitioners' interface solution therefore exceeds the standard that NTCA-OPASTCO have suggested the Commission should adopt by satisfying each of the two disjunctive requirements.

Petitioners respectfully submit that the other relevant characteristics of their IPTV device, including its use of Verimatrix for encryption functions, also comply with Section 76.1204(b). Verimatrix operates on a range of client devices manufactured by over 30 different set-top box vendors, and it is compatible with at least 13 different middleware vendors. More detailed specifications about the middleware and set-top box vendors with which Verimatrix can interface are attached at Exhibit C and information on the Verimatrix product is attached at Exhibit D. Petitioners' encryption solution relies on technology that is broadly compatible across middleware, conditional access, and set-top box vendors.

In short, Petitioners' security and conditional access interface rely on technology available for public license on standards that enable broad interoperability and are commonly

¹¹ See Exhibit A.

¹² See Exhibits B (providing information about the set-top box and conditional access function vendors with which Myrio can interface).

used. The Oklahoma IPTV Providers therefore submit that they are in compliance with Section 76.1204(b) because they rely on commonly used interface technology, and respectfully request that the Commission so acknowledge.

IV. IF THE COMMISSION DOES NOT PROVIDE THE REQUESTED CLARIFICATION BEFORE JULY 1, 2007, PETITIONERS REQUEST A WAIVER OF § 76.1204(B)'S OPEN INTERFACE REQUIREMENT FOR A LIMITED TIME

If the Commission has not issued a clarification of the common interface criteria for IPTV devices by July 1, 2007, Petitioners respectfully request a limited waiver of Section 76.1204(b)'s open interface requirement until such time as the Commission clarifies the criteria for compliance with the common interface requirement of Section 76.1204(b) and vendors are able to comply, or until such time as vendors are able to develop an interface based on an industry standard developed by a recognized national standards organization. Petitioners support the standard for clarification suggested by NTCA and OPASTCO in their recent Petition.¹³ Absent clarification, a waiver would be necessary so that uncertainty regarding compliance with the Commission's rules does not impede the development of new video services or the expansion of fiber networks in the rural communities that Petitioners serve.

The instant request meets the waiver standard contained in Section 629(c) of the Act and Section 76.1207 of the Commission's rules. Section 629(c) provides that waivers should be granted "to assist the development or introduction of a new or improved multichannel video programming or other services offered over multichannel video programming systems, technology, or products."¹⁴ Section 76.1207 states that the Commission "may waive a

¹³ *NTCA-OPASTCO Petition*, at 2.

¹⁴ 47 U.S.C. § 549(c).

regulation” regarding the competitive availability of navigation devices (including waiver of Section 76.1204) upon the same showing that would be required under Section 629(c).¹⁵

IPTV is precisely the kind of emerging technology most appropriate for waiver under the Section 629(c) standard, and the Oklahoma IPTV Providers are just the kind of new entrants, relying on an emerging technology and providing service to small rural communities, that are most deserving of a waiver. New technologies like IPTV are often the product of an organic process of creativity and innovation. A national standard is often the subsequent sign of, and not a precedent for, an innovative technology’s success. Failure to grant a waiver in this case would punish new entrants and manufacturers of new technologies. Requiring creators of new technologies to wait for standards to be developed by a national standards organization before they can begin to develop and market their products would frustrate the normal process of market-driven innovation.

Petitioners’ request also satisfies the general waiver standards of Sections 1.3 and 76.7 of the Commission’s Rules. Under Section 1.3 of the Rules, a waiver is appropriate where the “particular facts make strict compliance inconsistent with the public interest.”¹⁶ IPTV technology already delivers fully digital video programming. Its continued and increased deployment, particularly in the rural communities that the Oklahoma IPTV Providers serve, will provide customers with broader options to support the transition to all-digital programming by February 17, 2009. In addition, IPTV revenues better enable Petitioners to bear the costs of continued network expansion in the rural markets they serve. Without clarification or waiver from the Commission, the inability to deploy IPTV set-top boxes after July 1, 2007 would inhibit the Oklahoma IPTV Providers’ further expansion of fiber-based networks in rural communities

¹⁵ 47 C.F.R. § 76.1207.

¹⁶ *Northeast Cellular Tel. Co. v. FCC*, 897 F.2d 1164, 1166 (D.C. Cir. 1990).

in northeast Oklahoma. Maintaining continuity of service for existing subscribers and Petitioners' ability to play a positive role in transitioning rural customers to an all-digital solution present good cause for waiver of Section 76.1204(b)'s open interface requirement under the Commission's general waiver standards.

Finally, while IPTV demonstrates great promise, IPTV providers make up only a tiny portion of total MVPD market share.¹⁷ Petitioners, for example, have only approximately 1,100 IPTV subscribers. Grant of a waiver under the circumstances described herein would exert no material effect on the market for navigation devices.

In sum, the public interest will be served by the grant of the limited waiver requested herein. It will (i) help maintain continuity of service, (ii) enable increased consumer choice and competition for video service in support of the digital transition, (iii) have no effect on a competitive market for navigation devices, and (iv) allow for the greater development of high-speed networks in rural communities.

V. CONCLUSION

Petitioners respectfully request that this Petition be granted for the reasons set forth herein.

Respectfully submitted,

/s/ James H. Barker

James H. Barker

Cameron Smith*

of Latham & Watkins LLP

555 Eleventh Street, NW, Suite 1000

Washington, DC 20004

(202) 637-2200

Counsel for Northeast Oklahoma IPTV Providers

¹⁷ Petitioners' approximately 1,100 subscribers make up less than 0.01% of the entire U.S. MVPD market of 94.2 million subscribers.

*Admitted in New York. Not licensed to practice law in the District of Columbia; all work supervised by a member of the D.C. Bar

Exhibit A – Myrio Statement

This letter is intended to provide you with information regarding the Myrio software provided by Nokia Siemens Networks, which, among other things, performs “conditional access” functions for “navigation devices” deployed by multichannel video programming distributors (“MVPDs”). As you may know, effective July 1, 2007, the U.S. Federal Communications Commission (“FCC”) has instituted a ban on the deployment, by certain MVPDs,¹ of new navigation devices that perform both “conditional access” and other functions in a single integrated device (the “integration ban”), as set forth in 47 C.F.R. § 76.1204(a)(1). Below, we are providing information regarding the Myrio software which we hope will assist in your evaluation of whether your navigation device(s) comply with the integration ban.

Background. The integration ban specifically prohibits subject MVPDs from placing into service, as of July 1, 2007, “new navigation devices ... that perform both conditional access and other functions in a single integrated device.”² Under the FCC's rules, a “navigation device” is a device such as a converter box, interactive communications equipment, and other equipment used by consumers to access multichannel video programming and other services offered over multi-channel video programming systems. “Conditional access” is defined as “[t]he mechanisms that provide for selective access and denial of specific services and make use of signal security that can prevent a signal from being received except by authorized users.”³ The integration ban applies regardless of whether the navigation device is for sale, lease, or use.

The FCC has previously explained that the “conditional access separation” (or “security separation”) requirement is applicable to “access controls directly applied by the MVPD to authenticate subscribers’ identification.”⁴ As you are likely aware, the conditional access separation required by the FCC's integration ban can be met either by using a separate hardware solution, or by using a “downloadable conditional access security solution” (“DCAS solution”) that allows for “common reliance” by both MVPDs and unaffiliated consumer electronics manufacturers.⁵

Functions performed by the Myrio software. The Myrio software consists of two separate software components: Myrio Interactive, a client portion that is downloaded by a navigation device upon its first startup, and Myrio TotalManage, a server portion that provides a navigation device identification and subscriber identification function which is used to grant or deny access to services based on the subscriber's subscriptions with the MVPD. The Myrio software does not provide signal security functions (in other words, encryption and decryption) for the protection of programming channels. This is handled by a third party system to which the Myrio server component provides entitlement management messages via an open interface.

¹ For various reasons, U.S. Direct Broadcast Satellite providers such as DIRECTV and the DISH Network are not subject to the integration ban.

² 47 C.F.R. § 76.1204(a)(1)

³ *Id.* § 76.1200(e).

⁴ *Implementation of Section 304 of the Telecommunications Act of 1996, Commercial Availability of Navigation Devices*, Report and Order, 13 FCC Rcd 14775, 14800 (¶ 63) (1998).

⁵ *Implementation of Section 304 of the Telecommunications Act of 1996, Commercial Availability of Navigation Devices*, Second Report and Order, 20 FCC Rcd 6794, 6807-6808 (¶ 27) (2005).

* * *

Nokia Siemens Networks believes that the Myrio software is consistent with the FCC's conditional access separation requirements. However, whether a navigation device complies with the integration ban depends on the characteristics of that particular device as a whole (including any hardware and non-Myrio software components that comprise the conditional access element of the device). Nokia Siemens Networks cannot respond on behalf of other components contained within a navigation device and you should request clarification directly from the manufacturers of these other components. In addition you may wish to consider requesting a clarification or waiver from the FCC in order to obtain greater certainty regarding a particular navigation device.

We hope that this information is helpful to your evaluation. If you have any questions on the above or additional questions regarding the Myrio software, please do not hesitate to contact us.

Exhibit B – Myrio Partners



Enriching the Digital Home with IP Video Solutions



Partners

[About Myrio](#)

[Products & Services](#)

[Partners](#)

[Customers](#)

[News & Eve](#)

- [Overview](#)
- [Content Providers](#)
- [Headend Encoders](#)
- [VOD Servers](#)
- [Core Network](#)
- [Network Equipment](#)
- [Set-top Boxes](#)
- [CA & Encryption](#)

[Myrio iDK Program](#)

[Documents](#)

[Request Info](#)

Set-top Boxes



Advanced Digital Broadcast is a leader in the design, development, and supply of high-quality products to the world-wide digital television market. The Company has deployed over 8 million set-top boxes, across high-volume markets, incorporating the industry's pioneering middleware, conditional access and hardware technologies.



Entone Technologies is a leading provider of open, standards-based solutions that uniquely address two revolutionary developments in home entertainment: on-demand television and in-home multimedia networks. The company's proven technology enables digital content providers to reliably deliver a variety of personal television services, such as video-on-demand (VOD) and network personal video recording (nPVR).



Fujitsu Siemens Computers is the leading European computer company. Serving the needs of large corporations, small- to medium-sized enterprises and consumers, the company operates in all key markets across Europe, the Middle East and Africa.



Samsung Electronics Co. Ltd. is a global leader in semiconductor,



With vast experience in our specialist area of digital video/audio/data reception, **Amino** has created a clear roadmap of products suitable for multiple markets requiring traditional broadcast or new on-line services, and with our shared risk and reward approach is the ideal partner for rapid implementation of cost effective services.



Espial is the leading provider of rapidly customizable software for set-top boxes and mobile handsets. Espial applications and enabling technologies include Graphical User Interfaces, Video On Demand, Electronic Program Guides, Content Portals, Web browsers and interactive applications. Espial software is deployed and accredited for more than 100 consumer designs.



Motorola is a world leader in integrated broadband access platforms for delivering any combination of voice, high-speed data and multi-stream digital video services into the home or office. A Fortune 100 company with global presence and impact, Motorola had sales of US \$36.8 billion in 2005.



Scientific Atlanta, a Cisco company, is a leading supplier of digital content

telecommunication, digital media and digital convergence technologies. The company consists of five main business units: Digital Appliance Business, Digital Media Business, LCD Business, Semiconductor Business and Telecommunication Network Business. Recognized as one of the fastest growing global brands, Samsung Electronics is a leading producer of digital TVs, memory chips, mobile phones, and TFT-LCDs.



Tilgin develops, markets and sells IP products for TV and video streaming, as well as telephony for use in IP-based networks. Customers come to us for turnkey solutions, as well as for individual set-top boxes, streaming servers, residential gateways and management systems.

contribution and distribution systems, transmission networks for broadband access to the home, digital interactive set-tops and subscriber systems designed for video, high-speed Internet and Voice over IP (VoIP) networks, and worldwide customer service and support. Scientific-Atlanta, Inc. is a wholly owned subsidiary of Cisco Systems, Inc.

[Myrio Home](#) | [About Myrio](#) | [Products](#) | [Partners](#) | [Customers](#) | [News and Events](#) | [Contacts](#) |
© 2007 Myrio - webmaster@myrio.com



Enriching the Digital Home with IP Video Solutions



Partners

[About Myrio](#)

[Products & Services](#)

[Partners](#)

[Customers](#)

[News & Events](#)

- [Overview](#)
- [Content Providers](#)
- [Headend Encoders](#)
- [VOD Servers](#)
- [Core Network](#)
- [Network Equipment](#)
- [Set-top Boxes](#)
- [CA & Encryption](#)

[Myrio iDK Program](#)

- [Documents](#)
- [Request Info](#)

Conditional Access & Encryption



Conax is a leading supplier of state-of-the-art, highly innovative solutions for smart card-based conditional access, security and payment solutions. Conax is a globally oriented player, with a solid base of clients in 40 countries.

Latens

Latens was founded in January 2002 to deliver a new generation of Content and Revenue Protection Solutions for the fast growing Broadband market. It was founded by a senior executive team with wide experience of deploying and managing systems for broadband cable networks, digital interactive TV and IP services.

PHILIPS

Philips Digital Networks CryptoWorks conditional access (CA) system provides a complete end-to-end solution for Pay-TV, data broadcasting and Internet multi-casting, with encryption at both MPEG-2 transport stream and IP-level.



Verimatrix was launched in 1999 with the goal of providing cutting edge (two-way) DRM security systems which include PKI, encryption and watermarking functions, tracking, and legal action management.



Irdeto Access is a world leader in content protection technologies for digital video and IP networks. For over 30 years, we have pioneered encryption and conditional access technology and standards, now used around the globe to protect the world's most valuable content.



Nagravision is a market leader in the field of conditional access for digital TV and broadband Internet. Leading operators are equipped with its technology which ensures secure access to their services via more than 40 million decoders (analog and digital).



SecureMedia is a leading provider of open platform, media agnostic digital encryption and rights management solutions for the delivery of video-on-demand, broadcast pay TV, and other digital content over broadband IP networks, through home networks, and on optical media.



Widevine Technologies, Inc. makes encryption and key-management systems which enable secure video services on broadband networks. Headquartered in Seattle, Widevine's products safeguard video services (VOD),

broadcast channels, etc.) over cable,
xDSL (telco), and fiber optic networks.

[Myrio Home](#) | [About Myrio](#) | [Products](#) | [Partners](#) | [Customers](#) | [News and Events](#) | [Contacts](#) |
© 2007 Myrio - webmaster@myrio.com

Exhibit C – Verimatrix Partners

[Customer Care](#) | [Contact Us](#)[Solutions](#)[Products](#)[News & Events](#)[Partners](#)[Company](#)

Valued Partners

- Access Vendors
- Browser Vendors
- Chipset Vendors
- CODEC Vendors
- Content Aggregators/Content Partners
- Headend Vendors
- Middleware Vendors
- Monitoring Vendors
- OEMs
- Resellers
- Set Top Box Vendors
- Splicing Vendors
- System Integrators
- VOD Server Vendors

Set Top Box Vendors



ADB

ADB offers three product lines: digital TV consumer premise devices, interactive app TV (IDTV) modules. ADB sells its consumer premise devices to digital cable, satellite operators as well as to distributors and consumer electronics companies. Typically, / with extensive engineering and system integration services from early architecture d design, on-site installation and debugging, to after-sales maintenance and future up



Alpha Networks

Alpha Networks is a global leader in the networking ODM/OEM industry. We are a pr networking companies, integrators, telecommunications firms and service providers



Amino

Amino Communications develops core software technologies and customer-premises

with world-leading companies in content aggregation, middleware, conditional acces



Atlanta DTH Inc.

Atlanta DTH, Inc. ("ADTH") is a leading supplier of set-top boxes to TV stations, dist organizations. ADTH's STB lineup includes satellite, cable, and terrestrial. Its IPTV br offices in Atlanta, LA, London, Sydney and Sao Paulo.



Buffalo

At the Melco Group, maker of Buffalo products, we have achieved growth by expans computer peripherals to Internet devices. As technological innovation fuels changes efforts to anticipate these changes. Our growth has been a function of our natural a new ideas. We believe one of these new growth areas is IPTV and have expanded ir



Celrun

Celrun Co., Ltd. (Kospi:013240) is a diversified IP set top box manufacturer that dev of customers. Since its inception in 1999, the company has been a dominant player world market leader currently expanding it's field to VoD service and DMB equipmen Tcom&dtvro Co., Ltd. is located in Seoul, South Korea.



COSHIP

Founded in 1994, COSHIP Electronics Co., Ltd is a leading designer, manufacturer a digital television market. Coship is built upon the strength of its people, products an

leading Set-Top Box (STB) provider in China and are currently building the largest S



Eagle

Eagle Broadband is a leading provider of IP-based set-top boxes and IPTV content d competitive service provider, hospitality, enterprise, and other vertical markets.



Entone

Entone is a leading provider of open and scalable solutions that enable operators to television services, such as VOD and network personal video recording (nPVR).



Hansun Technologies

Hansun Technologies Inc., the major IPTV equipment provider in China , designs an as IPTV, DVB/IPTV, Internet PVR (with embedded P2P technology), Video Pod (VPo) entertainment and communication center. The company has over 6 year R&D experi most cost-effective and reliable IPTV products in the world.



Humax

HUMAX Inc. was founded in 1989 with the sole vision of becoming a leader in the di recognition for our quick-to-market, innovative products engineered with cost-effect company to develop a Digital Video Broadcast Set Top Box (DVB STB) and is current worldwide. With global manufacturing capabilities, and well over half its total revenu

making advances in all facets of the consumer electronics industry with a truly international presence on the Korean stock exchange (KOSDAQ).



Hyundai Digital Tech

Hyundai Digital Tech. is expanding its sphere of activities from STB and Karaoke to provide its customers with total solution covering communication, broadcasting and



ImpressTek

Launched in 1998, ImpressTek has been developing, manufacturing and exporting IP STBs. We have been providing above equipment to domestic business operator with a KT as a launch our business to North America and Europe market based on our experience as a cable and HOTEL service provider.



InfoEQ

INFOEQ Co., Ltd. is one of the leading IP based set-top box manufacturers in Korea. In hardware, we produce and develop IP TV STBs that meet the customers' preference. Over time, we know IP STBs.



Motorola

Motorola is known around the world for innovation and leadership in wireless and broadband. In our vision of Seamless Mobility, we design and deliver products, experiences and power to be connected. Within IP Video Solutions this includes encoders, video servers and consumer IP set-top boxes and the KreaTV Application Platform.



NetGem

Founded in 1996, Netgem provides operators with end-to-end hybrid IPTV solutions. Boxes and a Linux based middleware. Netgem's solutions are fully customized and include neuf cegetel, AOL or Telefonica.



NUMA

NUMA Technology Inc. (NUMA) was founded in 2002 in Taipei, Taiwan with the vision of providing high quality in IP Set Top Box for turnkey solutions and finished products. NUMA's key management experience in digital technology and mainly come from communication extensive knowledge and experience with Video On Demand solutions.



Sagem

Sagem Communication (SAFRAN Group) is a major player in the Mobile and Broadband. Sagem has acquired a strong world-wide position thanks to renewed innovation. SAGEM product activities: mobile phones, printing terminals, residential terminals, digital TV, network.



Scientific Atlanta

Scientific Atlanta, a Cisco Company, is a leading supplier of digital content contribution networks for broadband access to the home, digital interactive set-tops and subscription services on Internet and Voice over IP (VoIP) networks, and worldwide customer service and support. It is a wholly owned subsidiary of Cisco Systems.



Sentivision

Sentivision is an innovative provider of cutting-edge media technologies and product. Sentivision is committed to providing its customers with solutions enabling secure and medium bandwidth IP-based networks, such as DSL lines. Sentivision products and hardware and software products, STB reference designs and STB Software Development.



SetaBox Technology Co., Ltd.

The leading IP set-top box solution provider in the world, SetaBox Technology (Seta established in 2000. SetaBox is specialized in developing and designing advanced multimedia integrated solutions for its customers. It provides IP set-top box total solution for different multimedia service requirements. Elite staff coming from NTU's Communication & Multimedia technologies in every aspect, including: Codecs (MPEG-1, MPEG-2, MPEG-4, wmv9, H.264) (Transport Stream, Program Stream, RTP, RTSP) and hardware design (decoder card adapter, PMP).



Softier

Softier supplies IPTV client application software to IPTV service providers, OEMs and quality TV entertainment and services to consumers. Softier's client application software has competitive BOM costs while ensuring compatibility with emerging media formats such as Windows Media Edition of Windows Media).



Stino

Launched in 2000, STiNO Media AG provides IPTV STB hard and software solutions for Voice over IP, IP Television and Video on-demand entertainment. Additionally STiNO

digital signage and other vertical market segments with its advanced s-box IP based H.264, WMV9, HDMI for HDTV 1080i/p and also DVB-IP Hybrid s-box platforms.



SEI

Since our foundation more than a century ago, we, Sumitomo Electric Industries, Ltd. mainly through the production and sales of products that support social infrastructure. Using our production and materials technologies for electric wires and cables, we have technologies that serve social needs, thus opening new business opportunities and creating value.



Suniwell

Suniwell Communications designs, develops hardware and software solutions enabling the delivery of new multimedia services to homes and hospitality outlets. Suniwell supports various video codecs, WMV9 including HD and H264, as well as having combined solutions, enabling the delivery of high-quality multimedia services.



Telergy

Telergy is a solutions provider covering IPTV, VOD, VoIP and DVB applications. Telergy's solutions enable multimedia services to be provided on TV screens around the world. Telergy's solutions cater for both home and business applications.



Telsey

Telsey is a worldwide leader in the design and production of Access Gateway, IP Set the distribution of broadband interactive services to residential and business end use



Tilgin

Tilgin (formerly i3 Micro) designs and delivers premier IP customer premise equipment. Internet access, Voice over IP, IP Television and on-demand entertainment.



WEGENER

WEGENER accelerates access to HDTV with consumer premise IP set-tops and video garnered from supporting a diverse client base drives WEGENER to engineer robust,



Wisembed

Wisembed has delivered IP Set-top boxes for closed network environment, such as for an IPTV platform business for general audience.



Yuxing

Yuxing InfoTech Holdings Limited (Yuxing) is a company listed on The Growth Enterprise of Hong Kong Limited. With its comprehensive capability on R and D, mass production positioned as an e-home application solution provider based on digital media applications. Yuxing has been focusing on technology and product innovation, especially in the internet and the specific demand for customers.

Download the Yuxing Leaflet for more information.



ZyXEL

ZyXEL, headquartered in Taiwan, is a leader in developing and manufacturing broad businesses and home users. With 19 sales offices, three R and D centers and over 2 customers in more than 150 countries on five continents. As part of our global chain partnered with local distributors in 70 countries to promptly deliver product and services, sales revenue reached a record of NT\$12.9 billion (US\$400 million), driven by increa

[Solutions](#) | [Products](#) | [News & Events](#) | [Partners](#) | [Company](#)

[Customer Care](#) | [Contact Us](#) | [Home](#) | [Site Map](#) | [Terms of Use](#) | [PRIVACY](#)

© 2005-2007 Verimatrix, Inc. All Rights Reserved.

[Customer Care](#) | [Contact Us](#)[Solutions](#)[Products](#)[News & Events](#)[Partners](#)[Company](#)

Valued Partners

- [Access Vendors](#)
- [Browser Vendors](#)
- [Chipset Vendors](#)
- [CODEC Vendors](#)
- [Content Aggregators/Content Partners](#)
- [Headend Vendors](#)
- [Middleware Vendors](#)
- [Monitoring Vendors](#)
- [OEMs](#)
- [Resellers](#)
- [Set Top Box Vendors](#)
- [Splicing Vendors](#)
- [System Integrators](#)
- [VOD Server Vendors](#)

Middleware Vendors



Adtec

Adtec Digital is a leading developer of digital and IP television solutions including en middleware. With over 20 years experience in media distribution and control, Adtec features and the ability to generate unmatched bottom line revenue.



Conklin

Providing an Intelligent Personal | TV P solution using our fs|cdn platform to deliver view, UMS, on screen chat, VoIP, callerid on TV, weather, and sports data overlays.



Digisoft

Digisoft specializes in Interactive TV Application development and management. We and back-end server support to allow our customers and partners to design, deploy IPTV solution. This experience can be based entirely on their custom business mode architecture and Software Development Kits we provide.



Dreampark

Dreampark is the leading provider of IPTV Middleware software in the Nordic countries. The Middleware product is known for its attractive User Interface.



Espial

Espial is a leading provider of client middleware and applications for set-top boxes. Applications include User Settings Management, EPGs, VOD, Interactive Content, and Beyond Brandable™ user interface that enables operators to customize their offerings.



IMAKE

IMAKE is the major provider of open, intelligent solutions and integration services for broadband digital media, Video On Demand (VOD) and Internet Protocol Television. IMAKE serves telecommunications companies, and content providers. Founded in 1993 and headquartered in the United States, IMAKE solutions impact millions of users of broadband content across the United States.



ITonis

ITonis delivers end-to-end entertainment platforms specialized in IPTV and Video on Demand. ITonis solutions run on standard PC servers and require minimum integration costs. Thanks to its low entry costs, ITonis targets primarily small and medium access providers.



Kasenna

Kasenna, Inc., the IPTV company™, is a leading provider of VOD programming and service delivery. Kasenna's carrier-grade solutions enable telecommunications industries to maximize their profit by offering new video entertainment services that experience. The company's products and solutions suite consists of IPTV middleware distribution services for triple play offerings.



Myrio

>Myrio Corporation - A Siemens company, is a leading provider of software, content IPTV revenue opportunities for broadband operators by leveraging their infrastructure. Myrio Interactive, a full-featured end-user application enabled via a set-top box, and content management solution. Myrio's products and expertise enable operators subscribers a full range of IP-based digital television and on-demand entertainment through operational efficiencies and hardware choice. A pioneer in the industry, Myrio provides broadband service providers worldwide.



Netris

Netris is a Russian leader in IP-communications software development and system integration solutions development and delivery for growing international markets including IPTV/VoD, IPTV applications, OSS/BSS, CRM and other advanced solutions for service providers and operators. One of the elements of Netris's solution portfolio is a carrier-class middleware for IPTV - IPSoft platform is built with the use of open standards and can be seamlessly integrated with



Orca

Orca Interactive (LSE-ORCA) is a leading IPTV middleware provider. Orca empowers services including broadcast TV, EPG, VOD, PVR, and home media, leveraging a flexible unique offering includes a subscriber user interface SDK and an IPTV service Deliver



SeaChange

With billions of streams delivered in deployments worldwide, SeaChange International market proven on-demand systems and software. SeaChange automates entire on-c down to settop applications. Its solutions combine fault-resilient and highly scalable SeaChange Axiom video operation system software. Axiom manages sessions and re including streaming and application network services, thereby ensuring that bandwidth access for settop applications.



Syntek

Launched in 1997, Syntek is the leading provider of IPTV middleware and TV portal SMS management. With proven IPTV VOD deployments and offices in Korea, Syntek management system and system integration needs.

[Solutions](#) | [Products](#) | [News & Events](#) | [Partners](#) | [Company](#)

[Customer Care](#) | [Contact Us](#) | [Home](#) | [Site Map](#) | [Terms of Use](#) | [PRIVACY](#)

© 2005-2007 Verimatrix, Inc. All Rights Reserved.

Exhibit D – Verimatrix Statement



VCAS™ for IPTV Security Overview

6825 Flanders Drive
San Diego, CA 92121
Telephone: 858 677 7800
Fax: 858 677 7804
www.verimatrix.com



Introduction

The rollout of IPTV systems offers infinite promise for an expanding world of consumer entertainment in terms of breadth and depth of programming choices coupled with new interactive capabilities. However, the very technologies that make IPTV architectures possible also pose a threat to the business model that underpins such services. Sophisticated content piracy and widespread broadband Internet access are a legitimate concern to the owners of valuable content. It is of the utmost importance to the success of the IPTV industry that robust security technology can be deployed in such systems to eliminate theft of service and subscriber fraud.

The Verimatrix Video Content Authority System (VCAS™) offers an advanced suite of technologies that address content security challenges for the networks of today, and those of the future. Traditional conditional access systems are architected around one-way communications, while Verimatrix has designed its solutions from the ground up using the power and elegance of modern two-way IP infrastructure. Cryptographic and e-commerce technologies proven on the Internet enable VCAS to offer a more sophisticated level of content protection than traditional smartcard-based systems.

VCAS incorporates pioneering features that provide the broadest security perimeter of any content protection system, enabling complete transparency for legitimate content consumption while significantly raising the level of protection against content piracy.

VCAS security has been approved by all major studios for protection of premium content as well as by all the major broadcasters including Disney, Discovery, HBO, Showtime and ESPN. The VCAS security architecture described in this document has received very favorable results in independent audits and is the approved security choice in pay-TV operator deployments on a worldwide basis. As the global leader in software-based security, VCAS offers flexibility in choice of client devices, broad middleware interoperability and proven scalability.

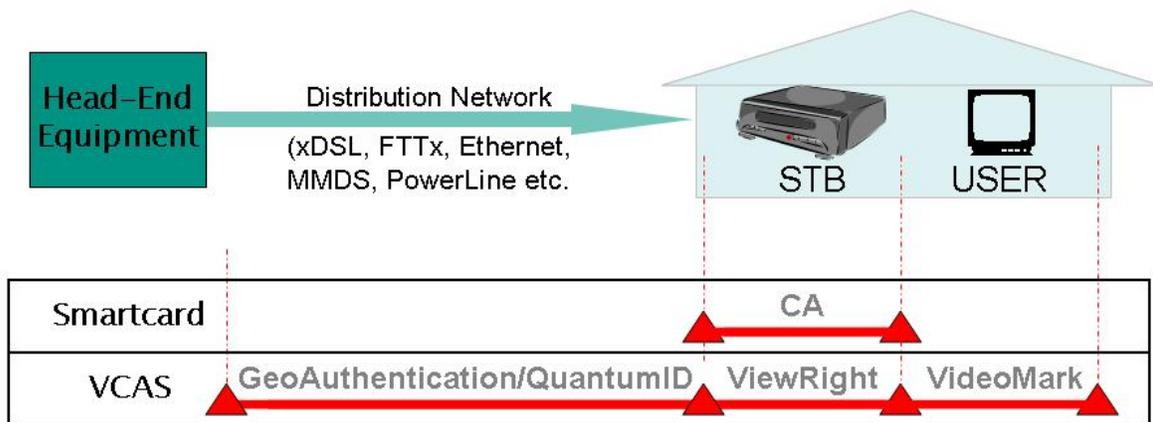
VCAS for IPTV Security Architecture

The “security perimeter” of any location or system defines the area of a physical or networked environment that is determined to be defensible. The security perimeter of a military installation is the fortified strip or boundary protecting a defended facility. The security perimeter of an IPTV system is the boundary defined by network devices protecting the integrity of the system and the content within that system. Today’s most widely deployed Conditional Access (CA) or content security systems use a smartcard as a physical security element that defines the security perimeter of the system. Code and variable data outside the smartcard in such systems tends to be regarded as vulnerable – sometimes obfuscated, but likely to be eventually compromised. Since the focus of system security rests on the removable components, the security technologies of the smartcards themselves are subject to very sophisticated attack and cloning



techniques. Consequently, fighting breaches of security on today's cable and satellite systems is an ongoing challenge.

In the VCAS for IPTV software-based content security solution, Verimatrix eliminates the vulnerabilities related to smartcard based architectures through the leverage of mature, proven two-way Internet security protocols, a Public Key Infrastructure (PKI) public/private key pair system and X.509 digital certificates. A downloadable security system for IPTV clients is not only more secure, it enables less expensive STB hardware and renewable security software can be updated as required to combat the pirates attacks. Verimatrix also extends the IPTV security perimeter by offering additional, significant security technology options that can detect and alert to the presence of content theft through cloning of clients.



Important components of the VCAS architecture for IPTV systems include:

- Content Security Manager (CSM) server
- Real-Time Encryption System (RTES)
- Video Pre-Processor (VPP)
- Patent-pending GeoAuthentication™ clone detection
- Patent-pending QuantumID™ clone detection
- ViewRight STB hardened client library
- ViewRight PC Player
- Patent-pending VideoMark™ user-specific forensic watermarking
- PiracyWatch watermark extraction service

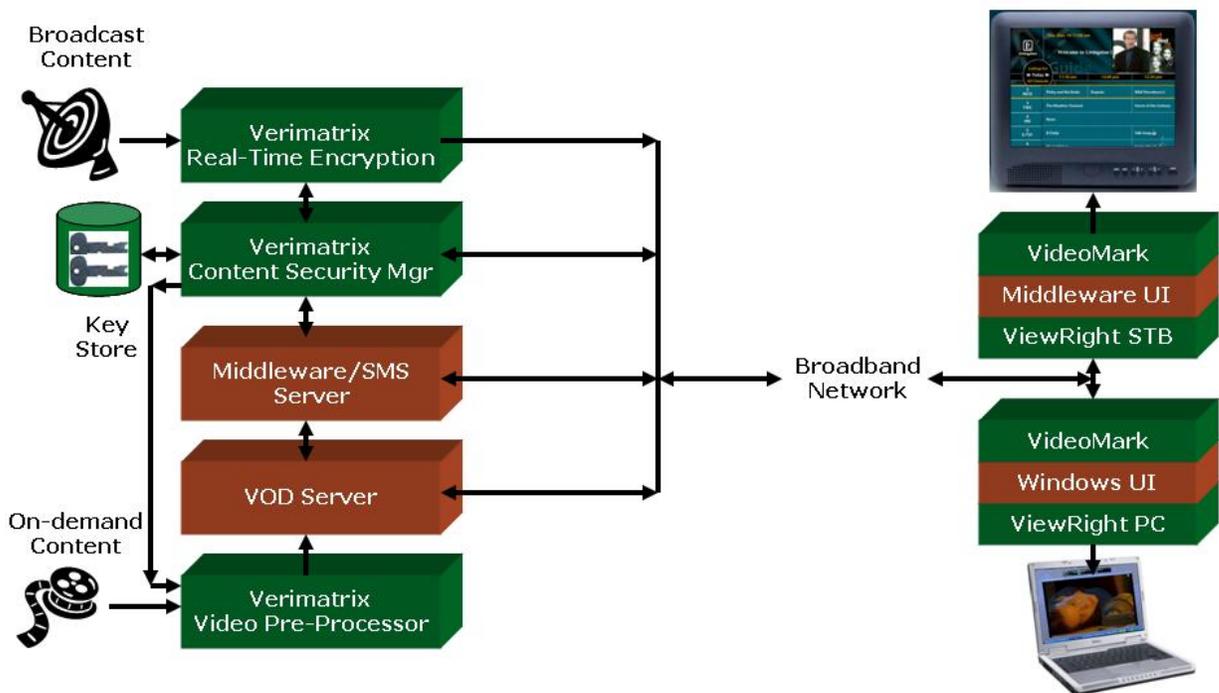


The VCAS architecture implements a sophisticated model of key generation and management, coupled with offline encryption for on-demand video content and flexible real-time encryption of broadcast streams. VCAS uses the best-of-breed AES and RC4 algorithms for content encryption and a Public Key Infrastructure (PKI) public/private key pair system using X.509 certificates to ensure the integrity of all components in the broadcast chain. All content is encrypted on a packet-by-packet basis and is constantly maintained in an encrypted state throughout distribution and storage until the point of playback in authorized client set-top boxes and other client devices.

Beyond the immediate security perimeter of the digital IPTV system, Verimatrix offers a digital watermarking solution for forensically tracking copied content – even content that has been captured in analog formats – back to the last legal recipient. Verimatrix VideoMark™ imprints video content with an invisible yet robust identifier which refers back to the individual set-top box, video session, time of day, and other characteristics that can identify the network and subscriber involved in any unauthorized redistribution of content.

System Components and Features

A typical VCAS for IPTV implementation within an IPTV deployment would be configured as outlined in the diagram below.





The key product components of VCAS for IPTV identified in the diagram are:

- Content Security Manager (CSM) server which contains all of the VCAS security component servers necessary to support authentication, key distribution and user control. The server components of CSM and the associated key store database can be distributed across physical machine clusters in order to provide capacity for the anticipated number of network subscribers.
- Real-Time Encryption System (RTES) which offers encryption of multicast streams of encapsulated video content.
- Video Pre-Processor (VPP) providing offline encryption of video-on-demand content files before storage on one or more dedicated VOD servers.
- ViewRight STB integration as a part of one or more 3rd party set-top box products.
- ViewRight PC Player running on a subscriber PC.

Also key components of the head-end system are the 3rd party streaming server and a middleware server which provides all content presentation, subscriber management and application services in conjunction with specialist software on the STB clients.

The key features of the VCAS for IPTV implementation are detailed in the following table.

Platform OS	Solaris 10, Linux (RHE 4.0), Windows 2003 Server
Video codecs	MPEG-2, H.264, VC1, DivX
Video encapsulation	MPEG-2 TS
Encryption	128bit AES, 128bit RC4, 1024 bit PKI (2048, 4096 optional), DVB-CSA
Digital certificates	X.509 compliant
Network management	SNMP
Database support	SQL Server, Oracle (8, 9i, 10i), MySQL
Content ingestion	Manual or automatic
Head-end integration	XML-RPC, SOAP, DVB-Simulcrypt
Clone detection	GeoAuthentication and QuantumID options



Basic System Setup

During system installation and initialization all server components of the VCAS system are authenticated within a Public Key Infrastructure (PKI) hierarchy. Once the hierarchy is established, all subsequent communication between the trusted components of the entire head-end system can be secured and encrypted as required.

To prepare content for Video-on-Demand delivery, the incoming content files are passed through the VPP server where a metadata description of each piece of content (the movie id) is used to request a specific encryption key from the CMS. Using this key, the content is stamped with this specific ID, encrypted and optionally watermarked by VPP. This process is usually a subset of an automated content ingest process which also serves to populate the VOD catalog maintained by the system middleware.

For broadcast content, each defined channel is assigned a multicast IP address and part number within RTES and its specific encryption strategy is established. Again, this security setup is synchronized with the system middleware to enable program guide display and channel surfing.

As each client device is added to the system, a check is performed on the integrity of the ViewRight client implementation within the device against the expected parameters for this network. This includes version identification, static code signatures and derivation of a unique client identifier. If these checks pass, the client is issued its own X.509 digital certificate referencing the established PKI hierarchy. The certificate exchange establishes the unique client identity within VCAS and enables subsequent secure client to head-end communication. Each client is also linked with a specific subscriber identifier within the system middleware.

Basic System Operation

During normal operation, the VCAS system operates in a very similar way with all types of content to enable correct decryption and display, with a number of important optimizations that enhance the users overall experience.

VOD operation involves the following flow:

- A subscriber browses VOD content display on his/her client device using the presentation and filtering options provided by the middleware client implementation.
- Upon selection of specific content, the middleware request is processed for that subscriber at the system head-end, including registering any charges to that account. A successful request is then communicated to the VOD content server and, optionally to the CSM.
- At the VOD server, the request creates a streaming connection between the server and the client and encrypted content flows towards the subscriber.



- At the CSM, the content request creates a secure connection to the client and a “push” of the necessary content decryption keys from its database. If the middleware does not initiate the key request as soon as content reaches the ViewRight client, the embedded content ID is used to create a secure connection to the CSM key database and the necessary keys are “pulled” down.
- The ViewRight client code filters and decrypts the content stream using the key data before presenting the video data to the MPEG decoder and a picture appears on the screen.

For broadcast content, the process is very similar but is optimized to enable fast channel changes:

- On a periodic basis (often daily), each client device establishes a secure connection to the CSM and requests the current broadcast decryption key block. This block contains all decryption key information for the current system channel line up as authorized for that client device.
- During the transaction, the CSM authenticates the client, retrieves the necessary key block from its database and encrypts the data before communication with the client.
- In the ViewRight client code, the current broadcast decryption key block is the primary reference data for obtaining the necessary keys when the client device is tuned to a multicast channel. Changing channels is optimized as no server request is necessary before a picture can be presented to the subscriber.

In all cases, key requests are communicated with the middleware system and validated against the subscriber entitlement data associated with that client device. This loop can be optimized through “caching” of entitlement data within the CMS interface.

GeoAuthentication™

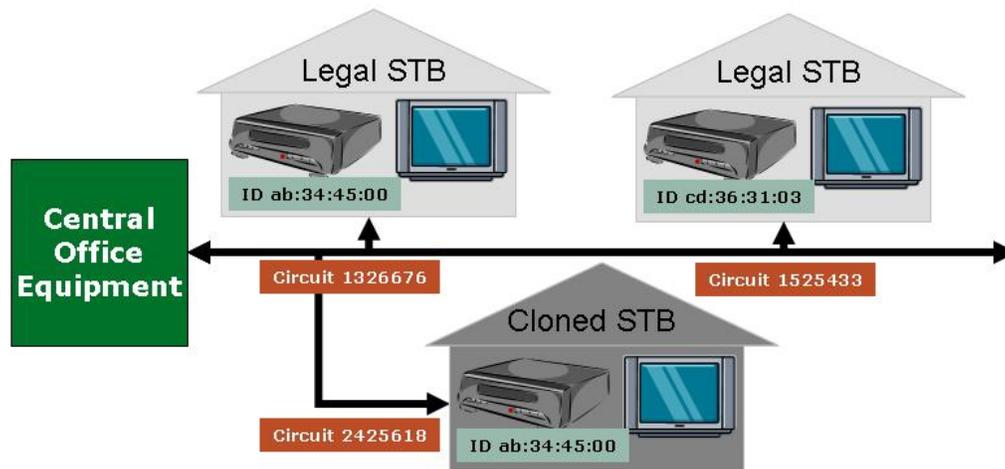
Assuring content delivery and viewing is limited to specific authorized client devices is a fundamental VCAS design goal and every aspect of the architecture attempts to limit the potential for theft of service. One type of attack on system integrity comes from duplication of client device credentials in authorized set-top box devices on the network. This includes replication of MAC address information and other supposedly unique unit identification codes.

GeoAuthentication is a patent-pending Verimatrix technology that can be deployed within VCAS for IPTV to preserve service revenues through detection and identification of cloned clients. The basis of GeoAuthentication is the collection and analysis of additional physical network topology information to augment the unique identifiers internal to STBs and other client devices. This physical connectivity information can be gathered from DHCP server option 82 records and other network management databases. Routine cross referencing of STB authentication requests with extended network topology data generates exception conditions related to changes in location,



duplicated credentials or other irregular activity which can then be investigated more thoroughly.

The figure below provides a high-level view of the physical network and GeoAuthentication.



From a system security perspective, GeoAuthentication extends the security perimeter of the distribution system from a uniquely identified set of STB and CPE equipment all the way back to the Central Office, maintaining the integrity of the system from head-end to the subscriber base. GeoAuthentication can also provide the operator with an indication that a valid (non-cloned) STB has been moved from one house to another without the subscriber account information being updated, providing a check on the integrity of billing and support information.

GeoAuthentication is not limited to DSL based IPTV systems, but is also appropriate for switched Ethernet connections, fiber connections, and other distribution architectures where there is an unambiguous relationship between a valid subscriber account and the network topology that serves that account.

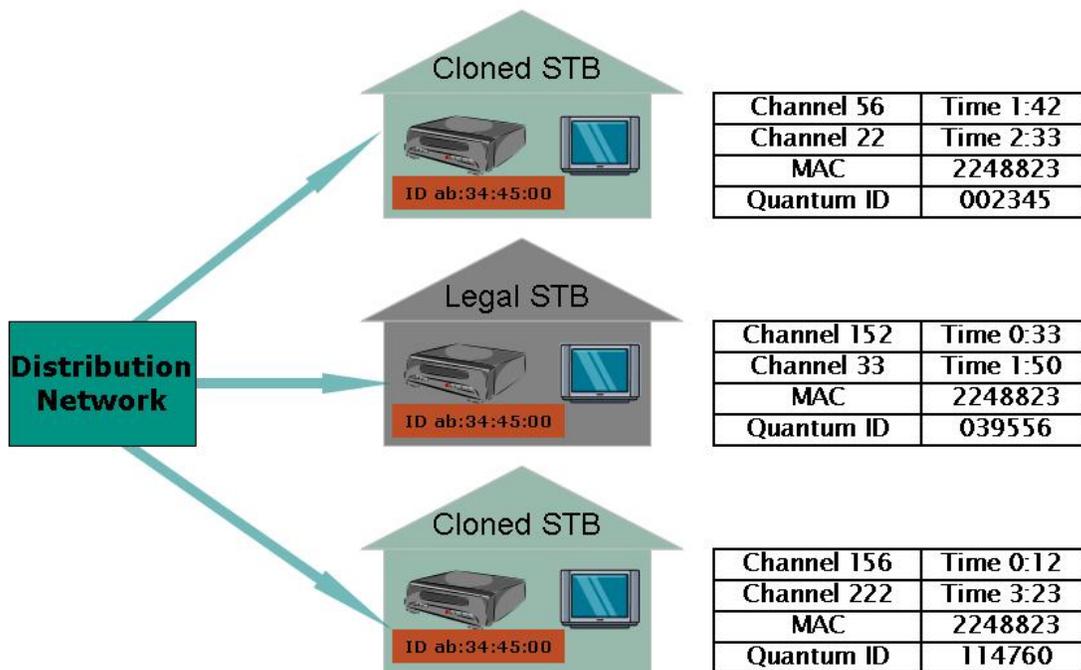
QuantumID™

In the battle between system operators and content pirates, creation of “perfect” cloned client devices can potentially lead to theft of video services and reduce an operator’s service revenues. Perfect clones with a simple out-of-band key delivery network, such as those that have been illegally created in attacks on existing pay-TV systems, have the potential to compromise security of any unprotected system. As an additional tool to help protect operator revenue in the face of such attacks, Verimatrix has designed and developed its unique QuantumID technology. QuantumID is truly a breakthrough in



security that enables even “perfect” clones to be readily identified and reported to the network operator. QuantumID technology running in the client devices creates a totally unique identifier for each client device during normal usage. This is done by combining the physical identifiers of the client device with a specific fingerprint related to operational events and client usage patterns.

The figure below illustrates the QuantumID™ concept as applied to a hybrid network architecture.



QuantumID enables unique client identification on any type of content distribution system. This includes architectures where the physical network topology connecting a subscriber to the network cannot be uniquely identified, or where a single physical connection may support multiple clients. This makes the use of QuantumID extremely attractive to operators with broadcast network architectures, especially where client devices do not have a permanently connected back-channel.

ViewRight STB

The Verimatrix ViewRight STB client is a robust package of portable embedded code that implements VCAS security functions within each set-top box (STB) in a pay-TV system. ViewRight STB code has been designed to require only a minimum of resources from the STB hardware and run-time environment and to use a standardized



set of simple interfaces to the middleware code also running on the STB. As a software-based security solution, ViewRight STB operates without the need for smartcard or other interface hardware. It offers best of breed content security and revenue protection functions in a hardened implementation that incorporates signing, multiple levels of integrity checking, debugger detection, key obfuscation, and intrinsic renewability.

The Verimatrix ViewRight VCAS STB client library is a system of security hardened real-time software that runs in authorized client of an IPTV deployment

ViewRight STB has been architected to be highly portable to differing hardware architectures and run-time environments. It is also designed to be network updatable in a highly secure manner. ViewRight employs best of breed standards-based encryption such as 128 bit AES encryption and 1024 bit (optionally 2048 bit and 4096 bit) PKI public/private key pairs to complement the head-end components of VCAS. Another important aspect of this element of the system is the careful approach to client implementation discussed later in this document. This approach can take full advantage of secure processing and tamper resistant features within newer generation of advanced VLSI devices used to build STBs and consumer electronic devices, including the ARM Trust Zone, Intel's Wireless Trusted Platform and Next Generation Network Architecture (NGNA) secure processors.

ViewRight's transient key mechanisms take full advantage of the two-way technology behind IPTV. Transient keys enable usage of decryption information that is valid for a short period of time, typically in the range of a few hours to at most a couple of days. Transient keys are delivered in a secure manner, ensuring any update messages that are captured out-of-band cannot be used by cloned client devices. Another important element of transient key is that they are updated at random times by the VCAS head-end systems.

ViewRight PC Player

The Verimatrix ViewRight PC Player turns any broadband connected PC into a fully functional, interactive IPTV client that complements the STBs in the subscriber household. The ViewRight PC player securely decrypts broadcast and VOD content within VCAS protected IPTV systems using a flexible, "lean forward" user interface style that includes program guide information for current broadcast channels and available VOD content. This content is adapted from the PC screen to the middleware data maintained in the system.

At installation time, a HW dependent unique identification code is associated with the subscriber identification and the player license obtained from the head-end CSM server. The ViewRight PC Player application provides the same level of content security and revenue protection as dedicated consumer set-top box (STB) equipment, including offering support for GeoAuthentication and QuantumID clone detection tools.



ViewRight PC player enables the subscriber to more fully leverage the networked home to distribute entertainment and extends the competitive advantage of IPTV services over legacy alternatives.

VideoMark™

While the ViewRight, GeoAuthentication, and QuantumID components of the VCAS suite combine to provide best of breed content security and revenue protection, at some point video content must exit the compressed digital domain in order to be seen and enjoyed. When presented in decoded form, content is vulnerable in different ways, particularly through copying of the analog signal. Sophisticated content pirates have been known to make illegal copies of movies by taking digital camcorders into movie theaters or capturing video from unprotected analog (e.g. S-Video) STB ports - even to check into hotel rooms to copy pay-per-view movies from hotel TV systems. This type of vulnerability is known as the “analog hole” and can defeat most attempts to preserve a digital format of watermark. The incentive for this type of attack increases as the quality and value of the source material increases – especially as High Definition (HD) video and earlier release windows are evaluated.

The VideoMark user-specific forensic watermarking technology is designed to counter this threat by marking decompressed video streams with a unique, robust identifier that is traceable to the place and time of viewing. VideoMark is applied using a very efficient algorithm running on the CPU or DSP of the set-top box client or PC host processor. The VCAS head-end generates the unique forensic payload used to identify individual client device sessions with time and hardware identifiers. The VideoMark algorithm then embeds these forensic tracking ID's into the video pixel information in a manner that is imperceptible and transparent to the viewer.

The VideoMark™ payload is extremely robust and secure. The embedded information will be recoverable following a wide variety of attacks and distortions such as:

- Re-compression: e.g. H.264, DivX and MPEG-2 down to 500 Kbps
- Geometric Distortion: e.g. scaling, rotation, aspect-ratio change, shifting, cropping and change of frame rate
- Analog recapture, including camcorder capture or multiple D-A/A-D (S-video or VHS)
- Signal enhancements: e.g. contrast, blur, color modification, de-flicker
- Malicious attacks: e.g. frame shuffling, random bending, attack on synchronization

In short, virtually any usable video stream derived from an unauthorized copy of the original content will contain a detectable VideoMark payload and retain a unique accountability. Using this patent-pending technology, it becomes possible to accurately trace the source of content that has been recorded and distributed illegally - on p2p file sharing networks, bootleg DVDs and other unauthorized channels.



The application of VideoMark extends the protection of VCAS beyond the analog hole and provides a more trusted secure distribution platform that is better suited to deter piracy than competing digital or analog techniques. Although completely transparent to the legitimate consumer of digital video content, the deterrent effect of the watermark will make piracy from VideoMark protected systems much less attractive. In the competition for licensing of premium content, the most secure and comprehensively protected systems are likely to be preferred by content owners. The interlocking solution set provided by the VCAS combination of digital content security and VideoMark is unique in the industry.

ViewRight Client Library Hardening

ViewRight and VideoMark technology running in an STB or other IPTV client device protects high value digital content from unauthorized viewing and enables identification of the source of any copied materials. To maintain an unquestioned level of system protection in the face of potentially very sophisticated code analysis, monitoring or tampering, a wide range of techniques are employed in the code architecture to detect and deter attempts to alter normal execution, or to illegitimately obtain unencrypted versions of protected digital content.



Some of the techniques employed include:

- Symbol obfuscation – library code symbols are obfuscated after linking to prevent the symbol name from giving a hacker useful clues to code operation. The symbol names are transformed from a functional ID such as “process_packet” to a meaningless string such as 01332145.
- Key Smearing – All the client library decryption keys and encryption keys used in the system are either smeared in physical memory or encrypted before being stored. Key smearing prevents a hacker from analyzing memory contents to find unsecured keys.
- Eliminating exposed APIs – the ViewRight library features a C++ based design that does not contain any exposed APIs that can be used to gain insight into the encryption and decryption processing within the libraries. All of the important security related processing code is obfuscated by the C++ compilation/run-time invocation processing.
- Stack and Heap scrambling – the client libraries have been hardened to avoid buffer overflow exposures and stack and heap variables are explicitly overwritten with random data when no longer needed. All dynamically allocated memory used for security related variables is also filled with random data before that memory is freed.
- Continuous debugger detection – a variety of run-time mechanisms are employed to detect breakpoint insertion and to detect run-time thread attachments.
- Code fingerprinting – frequent secure checks determine if the code image has been tampered with before or during execution. Validation is implemented using an MD5 hash algorithm resulting in a 16 byte fingerprint that can be used to determine if the code has been altered at any point before or during execution.

The code hardening mechanisms are designed to be portable across multiple client operating systems . Development environments are updated and augmented on a release by release basis. The code obfuscations are combined with private read-only data segments that hold any sensitive signature keys, code image fingerprint hashes, signing timestamps, and public string identifiers. Where possible, secure facilities on the specialist processors used in STB equipment are exploited to maximize operational integrity.

During development and code release, a proprietary post-processing application takes the ViewRight binary files and performs the necessary signature generation, hashing, time stamping, and labeling of the binary objects, while stripping the image of all human readable symbol table data. The binary code modules, after signing, will only execute on the specific VCAS installation that has access to the key pair used to build the library. In essence, each ViewRight client implementation will only operate on the distribution network that has access to the correct code signature key. These signatures also change at each point the security core is renewed over the lifetime of the network.



Independent Auditor Findings

In 2005, Verimatrix asked the Hollywood Studios which security auditing firm they would recommend to perform an independent audit on the Verimatrix VCAS system. Telcordia Labs was highly recommended. Verimatrix commissioned Telcordia Labs to perform an independent audit of the Verimatrix VCAS system. Unlike other content security vendors whose focus is limited to the properties of the various encryption algorithms, this audit included a comprehensive analysis of the entire system architecture.

The Telcordia audit confirmed 0 security exposures in the VCAS system. Telcordia also offered a range of very favorable comments including:

- “Impressively sound cryptographic paradigms”
- “Verimatrix has gone to great lengths to incorporate security into their product”
- “The Cryptographic architecture of the Verimatrix VCAS system has been well thought through”
- “The intended and achieved security goals are essentially the best possible given the state of the art”

The report was provided to all major content owners and broadcast organizations.

Conclusion and Further Information

Additional information on all Verimatrix products and the VCAS approach to content security and revenue protection are available under NDA agreement to partners and potential customers. Verimatrix can also provide a complete copy of the Telcordia Labs independent audit of the VCAS architecture upon request.

Verimatrix Location & Contact Information

Verimatrix, Inc.
6825 Flanders Drive
San Diego, CA 92121
Main: +1.858.677.7800
Fax: +1.858.677.7804

www.verimatrix.com

Sales/Business Development Contacts

sales_americas@verimatrix.com

sales_europe@verimatrix.com

sales_asia@verimatrix.com

Copyright © 2007 Verimatrix, Inc. All rights reserved. Reproduction or redistribution of Verimatrix web site or collateral content is prohibited without prior written consent.