Over the Top (OTT) Content Delivery

Secured Internet TV Deployment with Envivio 4Caster C4² and Verimatrix VCAS™

September 2010
# Contents

1. TELEVISION TRANSFORMED ................................................................. 3
   1.1 Introduction .................................................................................. 3
   1.2 Key Requirements for Deploying Premium Content OTT ............... 3
   1.3 Technologies for Over-the-Top .................................................... 4
   1.4 Requirements ............................................................................. 5
   1.5 Joint Envivio and Verimatrix OTT Solution ................................. 5

2. SOLUTION OVERVIEW ................................................................. 6
   2.1 Architecture ................................................................................. 6
   2.2 Key Solution Components ....................................................... 7
   2.2.1 Headend ............................................................................... 7
   2.2.2 Content Protection workflow ................................................... 8
   2.2.3 User Experience & Viewing Components ............................... 9
   2.2.4 Complete Solution for Multi-Screen Environments ................ 10

3. CONCLUSION ................................................................................ 12

4. ABOUT THE COMPANIES ......................................................... 13
   4.1 Envivio ....................................................................................... 13
   4.2 Verimatrix .................................................................................. 13
1. **Television Transformed**

Any Viewer · Any Device · Any Network · Any Time

1.1 Introduction

The appetite for online video is growing at an unprecedented pace. It started with YouTube, and has been fueled by new service launches like Hulu and Vevo. In the U.S., Netflix is transforming itself from a DVD rental company to an online streaming service. Consumers seem to devour content online as fast as it can be posted, and there doesn’t appear to be anything that will slow the pace.

With huge audiences finally embracing new television distribution models, leading technology companies have begun developing new services that take advantage of the new devices: Internet TV and over-the-top (OTT) content delivery of catch-up or on-demand services enable users to capture and view their desired programs at any time.

OTT delivery has created a break-through that is not limited to the PC screen, but extends to any connected device: connected TV, gaming consoles, smart phones, connected tablets, and more. Imagine the freedom of enjoying your favorite sporting event—like the Olympics, The Masters and the World Cup—live as they unfold, without being tied to the typical living room television. Now that is viewing freedom.

This represents a new path for broadcasters who are looking for innovative vehicles through which to deliver their premium content directly to the users. For network operators, it is an opportunity to develop and implement a multi-screen strategy that not only provides added-value services, but also enables new and untapped revenue streams. For the Pay TV operator the challenge is to extend their service brand and subscriber relationships beyond the living room, to satisfy demands for personalized choices and flexible viewing models.

This has impact on service delivery technology and business models: how to optimally monetize valuable content and services across a multi-network, multi-screen environment becomes the key challenge for both traditional and new operators.

1.2 Key Requirements for Deploying Premium Content OTT

As traditional pay-TV broadcasters and new operators begin looking at offering Internet TV and OTT content delivery services, it is important to understand the key challenges and requirements for achieving a successful implementation.

1. **Quality of Experience (QoE):** The aim of an Internet TV is to offer the same level of experience as IPTV and other managed networks. The viewing experience is expected to be continuous and without interruption due to network congestion. Insuring this on an unmanaged network is one of the key technical challenge to solve

2. **Content Security and Usage Rights Management:** The distribution of “Hollywood content” requires the use of proven and trusted content security technologies. Right holders need to
ensure their content is protected from piracy while operators need to guard against service theft. Managing and protecting the content, and the associated usage rights, means ensuring that each participant in the ecosystem, from the producer to the distributor, remains in control. Content protection and digital rights management (DRM) is a strong requirement from producers to allow distribution of their content to PCs and other connected devices. Content security and usage rights solutions are usually based on two essential notions:

- **Protected delivery**: The content, if distributed over a public medium (here the “public Internet”) needs to be protected during transport and storage. Encryption and secured exchanges are typically used to implement the content protection.

- **Digital rights and Business models**: This refers to how the user can consume the media, based on its associated usage rights, and how the revenue streams flow between the end user, the distributor and the producer.

3. **Operational**: From an operational standpoint, 24/7 broadcast environment is essential, further reinforced with the use of robust content security.

### 1.3 Technologies for Over-the-Top

Several major vendors have now proposed frameworks and technologies to satisfy the key requirements for a successful OTT deployment. Three of the most prominent include:

- Apple, with HTTP Live Streaming supported in their core products through QuickTime and iOS based products
- Microsoft, with its Silverlight and PlayReady framework
- Adobe, with Flash HTTP dynamic streaming

Interestingly, the approach taken by these vendors to address Quality of Experience (QoE) is based on the same fundamental technologies:

- **Efficient Video Compression**: Using the latest standard codecs, and notably H.264 as key foundation for a good experience.

- **HTTP Delivery**: HTTP is universal and works on any public network. This basic but essential characteristic means that firewall, scalability and heterogeneous issues that might come up with other distribution mechanisms are non-existent with HTTP.

- **Adaptive Bitrate Streaming**: This is the ability to encode a video stream into chunks of various sizes at different bitrates and resolutions in order to cope with bandwidth variations. Different container formats are available for these chunks, with similar properties. The most common are based on MPEG-2 Transport Stream (TS) segments or on Fragmented-MPEG-4.
1.4 Requirements

Flexibility is essential to mobile and Internet TV/OTT which require answers to the following challenges:

- Open standards-based approach to foster innovation, interoperability, and expansion of suppliers options
- Adaptation to variable QoS to ensure optimized user experience
- Highly scalable, straightforward technology for network deployment
- Multiple network support – broadband, 3G/4G wireless, Wi-Fi, etc.
- OTT streaming using shared codecs and formats with IPTV and DVB networks.

Additionally, various technologies are required to address Content Protection and Rights Management for OTT delivery of premium content to enable revenue models for successful multi-screen service delivery:

- **Device authentication:** Prior to entitling a user to any services, the device must be authenticated as a valid device, preferably based on Public Key Infrastructure (PKI) and X.509 certificate principles.
- **Entitlements checking:** Before a decryption key can be issued, it is necessary to determine if the requesting user has the rights to consume the content.
- **Secure key distribution:** Upon positive entitlements verification, a key needs to be provided to the user’s device(s) in a secure manner.
- **Secured content delivery:** Encryption, typically based on the proven and robust AES algorithm with a 128-bit key.

1.5 Joint Envivio and Verimatrix OTT Solution

The combined Envivio and Verimatrix OTT solution outlined in the next chapter implements support for the HTTP Live Streaming protocol, which has been proposed to the Internet Engineering Task Force (IETF) as a standard for adaptive streaming (http://datatracker.ietf.org/doc/draft-pantos-http-live-streaming/). While originally implemented by Apple, the proposed protocol is supported by a growing ecosystem of encoder and web server suppliers, including Envivio and Verimatrix. The protocol is further enhanced by Verimatrix security techniques applied to premium IPTV services.

The joint solution thus fulfills all of the above requirements and provides the requisite foundation for deploying premium Internet TV/OTT services successfully. It can be deployed by existing managed network operators, providing cable and satellite or IPTV services with an Internet TV outlet parallel to their other services. It is also an appropriate solution for “greenfield” OTT operators, perhaps intent on competing with established pay-TV operators using the new format of Internet TV. The solution supports both linear and on-demand services, and DVR support for programmed recording, catch-up and go-back TV.
2. Solution Overview

2.1 Architecture

The solution architecture consists of Envivio 4Caster C4\textsuperscript{2} encoders in combination with the Verimatrix Video Content Authority System, VCAS\textsuperscript{TM} 3 for revenue security and usage rights management. Monitoring and N+M failover management is achieved using Envivio 4Manager Network Management System (NMS). The 4Caster C4\textsuperscript{2} and 4Manager are integrated with the VCAS 3 system as depicted below:

![Figure 1 - Envivio and Verimatrix Internet TV Architecture](image-url)
For operational aspects and robustness of the ecosystem, a tight interaction has been designed between Envivio 4Caster C4² and VCAS 3. This interaction is referred to as “Key provisioning”. The objective is to automate the exchange of encryption information between the encoders and VCAS 3.

In addition, content owners required this interaction to be secured. This led to the definition of a communication interface and joint development between Envivio and Verimatrix.

2.2 Key Solution Components

2.2.1 Headend

The integrated head-end includes VCAS for Internet TV and the Envivio Three Screen Head-end, thus forming a multi-format solution supporting OTT pay-TV services to multiple screens and across multiple transports. The combined solution support for HTTP Live Streaming and offers:

- Support for MPEG-2 or H.264 sources from satellite, terrestrial or baseband signals
- Encoding, encapsulation and packaging based on H.264 codecs, MPEG-2 TS and AES encryption, thus enabling straightforward integration into existing pay-TV head-ends.
- High availability and 99,999% uptime thanks to N+M or 1+1 redundancy and the Network Management System
- Support for live, near-live and file-to-file for VoD and NPVR services
- Native support (QuickTime player) by popular consumer devices, including Apple iPhone, iPod Touch, iPad, as well as the Mac.
- Rapidly growing ecosystem of vendor support, including, VoD and streaming servers, Content Management System, client-side platforms (e.g. Android) and devices (e.g. STBs and TVs).
- Open standard allowing tight integration of the technology into client-side products.

The joint head-end is composed of the following elements:

- **VCAS Operator Management Interface (OMI)** – The core administrative VCAS 3 component, OMI provides a single VCAS integration point for customer care, billing and middleware systems through a set of content, device and entitlement management interfaces.

- **VCAS Adaptive Content Security Manager (ACSM)** – ACM contains the VCAS for Internet TV security components for networks implementing HTTP streaming, including OTT services. ACM secures cross-platform content delivery to a variety of device categories, including PC/Macs, mobile handsets, web pads, STBs, connected TVs, etc.

ACSM supports authentication, key distribution and user control and acts as the root Certificate Authority in a PKI hierarchy. It uses X.509 certificates to validate and authorize all content protection communication within the pay-TV network, including messaging between VCAS sub-system components as well as between the head-end system and authenticated subscriber receivers.
• **VCAS MultiCAS™/Adaptive and VPP/Adaptive** - Encryption keys are generated by the ACSM and provided to 4Caster C4² via the MultiCAS or VPP interface. Envivio encoder then undertakes the actual AES encryption of the streaming chunks prior to downstream distribution.

• **4Caster C4²** - Envivio three screen encoder/transcoder for live TV channel encoding. The encoder encodes the same video input in multiple resolution and multiple bit rates suitable for Adaptive streaming, performs AES encryption with the key distributed by the VCAS ACSM system, cuts the video streams into chunks and distributes them to the origin server.

• **4Caster C4² - On Demand**: performs the same encoding and encryption functionalities as 4Caster C4², but in a file to file workflow to create VOD assets. Integrated with Envivio 4Balancer and leading Content Management System, the On-demand solution ensures the creation of high-quality multi-rate assets in record time.

• **4Manager**: Within Envivio encoders, signal routing and power management are fully redundant. Fault tolerance is increased by redundant components administered via the Envivio 4Manager™ management system, which provides automatic 1+1 or N+1 redundancy protection and high-level service supervision.

### 2.2.2 Content Protection workflow

An important aspect of Internet TV distribution, as with any video service, is the secure transport of the content.

The management of the encryption process, and the control of secured delivery of these keys to clients, is at the heart of the Verimatrix enhanced security layer applied to the HTTP Live Streaming standard. All HTTP based streaming protocols implement a mechanism to encrypt the individual video chunks. In the case of the HTTP Live Streaming protocol, each chunk can optionally be encrypted using the AES-CBC-128 block encryption algorithm to provide the first level of delivery security.

The Envivio encoder is responsible for receiving the video and encoding it into different bit-rates. Once the different bit-rates are encoded, they are sliced into chunks which are synchronized and assigned sequence numbers. At this point, the chunks are ready for encryption.

The encoder contacts the VCAS server via a well defined key exchange interface and requests a key. The encoder then takes this key and encrypts each chunk using the AES encryption algorithm. These encrypted chunks are placed on the HTTP Server along with a regularly updated live streaming playlist that includes the key references.

The HTTP Server is a standard HTTP server which hosts the encrypted chunks and playlist files. The Envivio encoder places these files on the HTTP server at the appropriate times and is also responsible during live broadcasts for removing the chunks at the appropriate times.

Verimatrix enabled client devices are able to read the playlist for any asset and extract the key references. During the playing of the stream, the client requests a key from this VCAS server over a secure connection, and a device unique identifier is sent along with the request. The VCAS server uses its entitlement reference database to determine if this unique client identifier is authenticated and entitled to the video being played. If so, the VCAS server will return the 16-byte key to the client. This key will be used to decrypt the video chunks so the device can proceed with playback of the video content.
Verimatrix VCAS for Internet TV is the key management solution for the OTT head-end encoders and client devices. The tight integration with VCAS includes important extensions to the standard model that improve the capability to support subscription and transaction based pay-TV services. In particular, VCAS for Internet TV ensures that decryption keys are managed and selectively distributed to authorized clients only. This solution provides secure OTT content delivery to authorized clients via entitlement checks and provides the foundation for premium OTT pay-TV services.

![Diagram of Verimatrix Adaptive CSM and Keyfile Requests](image)

**Figure 4 - Example: Apple iPhone**

### 2.2.3 User Experience & Viewing Components

A great subscriber experience begins with a service that is on air all the time. Envivio’s high-availability platform delivers 99.999% uptime and unshakeable performance thanks to the broadcast-grade fault management provided by Envivio 4Manager. Furthermore, support for adaptive rate streaming technologies, including HTTP Live Streaming, ensures continuous viewing even under changing network conditions. Combined with interactive multimedia capability and economical HTTP delivery technology, the head-end makes it possible to create a unique experience for subscribers at substantially lower cost than dedicated or proprietary transport protocols.

The end-to-end solution is designed to optimize the user experience by giving operators precise control over key parameters of an HTTP Live Streaming service to achieve the best results, including:

- Range of bitrate choices – more bitrates gives better ability to optimize quality on a given client
- Chunk length – compression optimization to adjust for bandwidth variations
- Key mutation rate – enable finer grain entitlement control and resilience against sharing attacks
• Playlist length – enables clients to navigate forward and backwards over a substantial period of content.
• Step-up and step-down heuristics – how frequently to change rates for smooth playback experience.

The Verimatrix ViewRight Web client is a robust package of portable code that implements VCAS™ device authentication functions in devices that can support HTTP Live Streaming video services. ViewRight Web secures video delivery to a variety of devices, including:
• PC/Macs,
• iPhone OS 3.0+ based devices (iPhone, iPad, iPod Touch),
• Android OS-based devices
• Set top boxes.

Figure 5: ViewRight Web for PC with Envivio Encoded/Encrypted Content

2.2.4 Complete Solution for Multi-Screen Environments

VCAS can support HTTP Live Streaming in stand-alone OTT service configurations or it can be utilized as part of a unified security head-end supporting multi-screen deployments pairing OTT delivery alongside IPTV or DVB services as depicted below.

Envivio encoders support multi-screen distribution models and can be configured to encode content for these other applications.

A single content authority, VCAS plays a vital role in the transition towards multi-screen services. Operators benefit from a unified revenue security architecture, which not only brings significant cost and operational savings from managing just one platform, but also enables the deployment of a transparent security regime across all the network and device permutations that subscribers demand. A unified revenue security approach eliminates the potential impact of disparate usage rights policies, allowing consumers to simply enjoy what they have acquired.
The core administrative VCAS 3 component, OMI provides a single VCAS integration point for customer care, billing and middleware systems through a set of content, device and entitlement management interfaces. OMI enables VCAS domain-based business models for multi-screen digital TV services by providing homogenous subscriber and rights management for heterogeneous networks and devices: DVB, Hybrid, IPTV, Internet TV/OTT and Mobile TV.
3. Conclusion

This paper describes the ecosystem, dataflow and components required to deliver a complete and secured Internet TV/OTT television experience to a variety of devices. This solution is pre-integrated and tested by Envivio and Verimatrix, and it is currently undergoing evaluations and trials by a number of operators planning OTT services. The feedback received on technical issues and the operational architecture is very positive.

Based on Envivio 4Caster C4², Verimatrix VCAS and ViewRight technologies, the integrated solution delivers the key ingredients for an optimal, premium Internet TV service:

- **Protected Delivery**: Tightly integrated with secure VCAS key management, strong and standard AES-128 encryption is applied right inside 4Caster C4² in order to protect the content delivery from its origin to the subscriber.

- **Digital rights and Business Models**: Based on rules established by the operator’s business and subscriber management system, and realized through the Verimatrix VCAS for Internet TV solution, devices are authenticated and the user is granted consumption rights, described in entitlements, based on the specific subscription properties. Encryption keys are generated by VCAS and provided to the Envivio encoder via the Verimatrix MultiCAS/Adaptive interface. VCAS ensures that decryption keys are managed and selectively distributed to authorized clients only.

- **User experience**
  The entire solution has been designed to provide an excellent quality of experience for consumers that will support the growth and retention of subscription services. Content security is transparent to viewers, ensuring easy access to the uninterrupted experience offered by adaptive streaming technology.

Thanks to the combined technology and expertise delivered by Envivio and Verimatrix, the solution is ready for immediate customer deployment and can be used by any service operator that wishes to extend its reach beyond managed networks by launching Internet TV to STBs, connected TVs, PCs/Macs and a variety of mobile device classes.

For further details on adaptive rate streaming and corresponding pay-TV network evolution, see the Verimatrix white paper “Adaptive Rate Streaming: Pay-TV at an Inflection Point”. 
4. About the Companies

4.1 Envivio

Envivio is the leading technology provider of IP-based MPEG-4 video systems and solutions for telcos, enterprises, and broadcasters. Using its encoding technology as a foundation, Envivio provides complete solutions that take advantage of modern networks to deliver live and on demand video services to consumers. With the most complete range of advanced compression codecs on the market, from standard H.264 through the exclusive Elite™ and Extreme™ codecs developed in our labs, Envivio optimizes the viewing experience for the widest range of devices and delivery networks, from mobile to HD including mobile video services, video to the desktop, video-on-demand, and interactive IPTV. Built-in support for multiple codecs and resolutions enables a single head-end to serve any combination of mobile, PC and traditional TV screens.

4.2 Verimatrix

Verimatrix specializes in securing and enhancing revenue for multi-screen digital TV services around the globe. The award-winning and independently audited Verimatrix Video Content Authority System (VCAS™) and ViewRight® solutions offer an innovative approach for cable, satellite, terrestrial and IPTV operators to cost-effectively extend their networks and enable new business models. As the recognized leader in software-based security solutions for premier service providers, Verimatrix has pioneered the 3-Dimensional Security approach that offers flexible layers of protection techniques to address evolving business needs and revenue threats. Maintaining close relationships with major studios, broadcasters, industry organizations and its unmatched partner ecosystem enables Verimatrix to provide a unique perspective on digital TV business issues beyond content security as operators seek to deliver compelling new services.