Beyond Content Protection to Revenue Security™

VCAS™ Ultra for DVB and DVB-Hybrid – Overview

Advanced Content and Revenue Security for Digital Video Broadcast Services

Verimatrix, Inc.
6059 Cornerstone Court West
San Diego, CA 92121, USA
Telephone: +1 858 677 7800
Fax: +1 858 677 7804
www.verimatrix.com

Table of Contents

Executive Summary – DVB as Part of the Whole

As video content becomes more diverse and ubiquitous, pay-TV operators must adapt their service offerings and operations to higher subscriber expectations. In response, they are increasingly targeting three or more screen types, i.e. TVs, PCs and various mobile devices, in their attempts to offer attractive competitive services and reach the widest possible audience, anywhere and anytime. Service convergence has become a market-driven imperative representing an upside opportunity for innovative service providers to expand revenues and differentiate service offerings.

However, even in this irreversible trend towards two-way networks and connected devices there is still a need to serve large viewer populations via satellite, cable and terrestrial broadcasting. There is also an analog-to-digital transition underway in several countries, or even whole regions, where one-way may be the first step while preparing for a connected future.

Part of the VCAS Ultra multi-network platform, VCAS Ultra for DVB is a full featured CA solution supporting satellite, terrestrial and cable/MMDS networks, proven in 100+ deployments since 2003:

- Flexibility in deployment
  - Range of cardless and card-based clients, incl. state-of-the-art secure SOC implementations such as trusted execution environment (TEE).
  - B2C and B2B configurations
  - OEM and hosted solutions
  - Cost effective, small form factor, scaling to tier 1 pay-TV operations with millions of subscribers
- Multi-network extensibility
  - Part of the broader VCAS Ultra multi-network platform for IPTV, DVB and Internet TV/OTT
  - Extensible with hybrid DVB-OTT services
  - Optional software- or hardware-based forensic watermarking (VideoMark™ and LiveMark™)
  - Single security authority integration

Verimatrix VCAS solutions address the complexity of revenue security in today's multi-network world.

From flexible, cost-effective cable and satellite DVB conditional access to adaptive rate streaming and harmonized multi-DRM management, Verimatrix offers advanced security architectures and ecosystem partnerships that enable the next generation of video delivery systems.

VCAS Ultra for DVB offers a full range of pay-TV functionality:

- PPC, PPV, IPPV, PPT
- DVR, Push VOD

The core design and technology features, among else:

- Web services API for system control
- Pre-integration with a broad range of set-top boxes (STB) with a choice of security level
- Fully standards-compliant DVB Simulcrypt support
- Independent security audits by both Merdan and Farncombe with excellent results
- Fully meets the requirements as outlined in *MovieLabs Specification for Enhanced Content Protection*, including Ultra High Definition (UHD / 4K) and other high value content security.

A key value add by Verimatrix is the common VCAS entitlement and management interface, which provides a single point of integration with back-end systems such as middleware and subscriber management/billing. Uniquely, while a single DRM may support a multi-device domain concept as such, VCAS enables *cross-DRM domain management* (i.e. VCAS Super Domains). When content is entitled to a subscriber's domain (as opposed to a device), it is automatically available to all the domain's devices, whether IPTV, DVB, Hybrid, HLS, or DASH clients.

1 VCAS™ Ultra – The Proven Multi-Network Solution

The Verimatrix Video Content Authority System (VCAS™) market-specific solutions are built on a common system core with modular extensions per segment. It implements a single security authority for multiple networks and devices, supporting various video and DRM formats while providing harmonized content rights management.

The VCAS Ultra revenue security solutions support digital TV operators in these market segments:

- VCAS Ultra for IPTV, supporting:
  - IPTV services for managed networks
  - Broadcast-OTT hybrid networks and receivers
  - Wholesale/Retail content distribution model
  - Hospitality-optimized version
- VCAS Ultra for DVB ("one-way" broadcast networks), and DVB-Hybrid with integrated IP video
- VCAS Ultra for Internet TV for unmanaged networks (Adaptive Bitrate Streaming)
- Verimatrix MultiRights Ultra, supporting third-party DRMs: Microsoft PlayReady, Google Widevine, Adobe Primetime and Apple FPS
- VideoMark™ and LiveMark™ user-specific forensic video watermarking

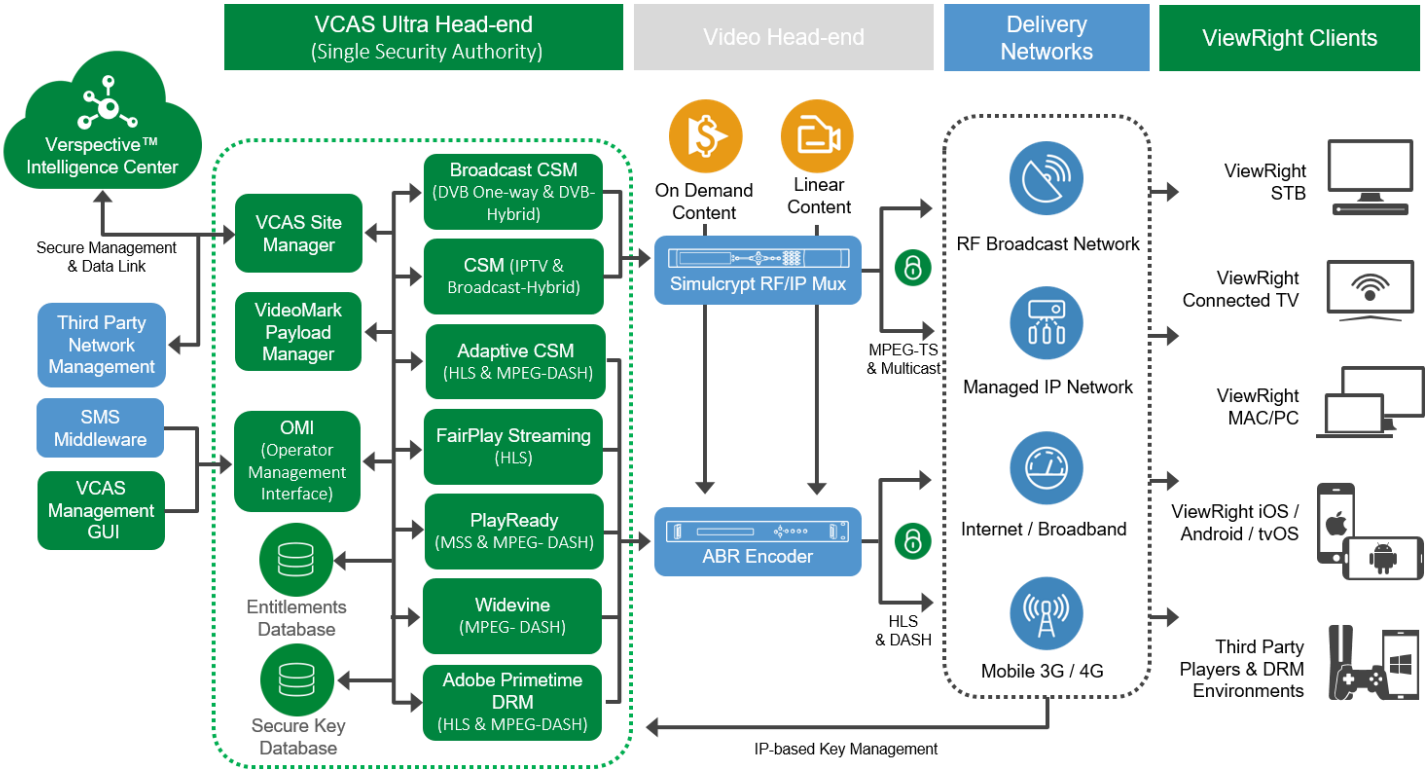


Figure 1: VCAS Ultra – High-level Architecture

The market specific solutions are described in documents like this and can be downloaded from www.verimatrix.com or obtained from a Verimatrix representative.

2 VCAS Ultra for DVB: Solution Overview

2.1 System Architecture and Key Components

The VCAS Ultra head-end consists of several server components that perform key and content rights management for DVB, IPTV, and OTT pay-TV services, including hybrid broadcast-OTT delivery. The resulting solution is a single security authority for multiple networks and devices, supporting various video and DRM formats while providing harmonized subscriber rights management. This document focuses on the architecture and components for DVB one-way broadcast services over cable, satellite and terrestrial networks, and DVB-Hybrid delivery.

The VCAS Ultra for DVB architecture diagram is followed by key component descriptions.

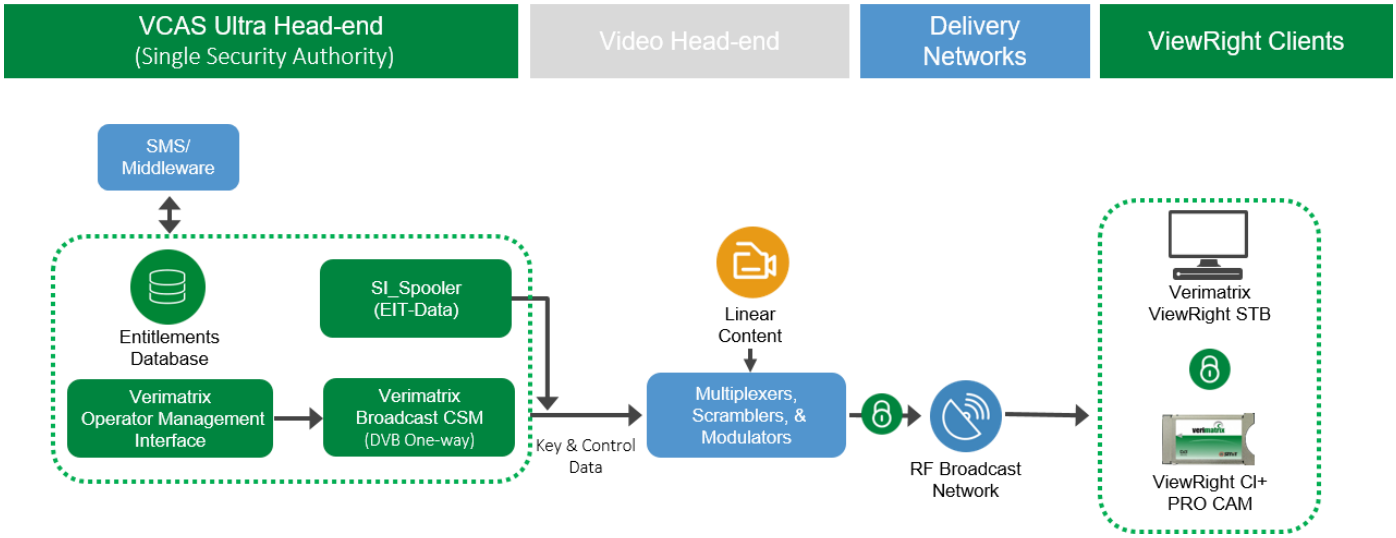


Figure 2: VCAS Ultra for DVB - One-way Network

VCAS Ultra for DVB key components:

- **VCAS Ultra Operator Management Interface (OMI)** – The core administrative component of VCAS, 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, IPTV, Internet TV/OTT, and hybrid combinations thereof.

  OMI offers a unified API for network management and transparent subscriber experiences, and a comprehensive entitlement data model, featuring:

  - 'Push' subscriber management system (SMS)/middleware integration via OMI server
  - Common entitlements database for advanced services bundling
  - Common rights arbitration logic for parallel license delivery mechanisms and subscriber domain management.

- **VCAS GUI** – A sophisticated graphical user interface that allows the operator to manage entitlements, content, devices, domains etc., even without the help of an external subscriber / content management system.

- **VCAS Ultra Broadcast Content Security Manager (BCSM)** – BCSM enables advanced pay-TV business models within VCAS secured broadcast (one-way) networks. It provides each operator with unlimited flexibility to define pay-TV services, and it manages authentication, key distribution and user control. BCSM includes an entitlement control message (ECM) and entitlement management message (EMM) generator, implementing DVB Simulcrypt with DVB multiplexers, which enables MPEG-compliant Multi-Program Transport Stream (MPTS) encryption.
- **Verimatrix EncryptionEngine** – This high-performance hardware device encapsulates all cryptographic operations to protect ciphers and control mechanisms, and operator keys.
- **VCAS Ultra SI Server** – A middleware-independent spooler for electronic program guides (EPG), it builds and plays out DVB-compliant data tables with TV schedules.
- **ViewRight® (Ultra) STB for DVB** – In contrast to the legacy approach, Verimatrix offers multi-level client security with a choice of software-based clients, cardless secure SOC implementations (e.g. TEE), and advanced smart cards, which allows operators to match STB technology with revenue potential. Beyond Ultra STBs, support is also provided for the Verimatrix Standard and Advanced STB security.
- **ViewRight DVB CI** – Choice of single-stream or multi-stream DVB Common Interface modules for consumer and professional decoding applications.
- **ViewRight CI+** – Common Interface Plus module providing support for copy protection and output control.

Verimatrix works with each customer to define the hardware that meets the desired redundancy plan. Generally, VCAS Ultra for DVB redundancy is based on 1:1 configurations. A high-availability Oracle database is used by VCAS to store all critical information.

2.2 Product Features

Platform OS	Red Hat Enterprise Linux
Database	Oracle Enterprise Edition
GUI	Flexible Java-based secure administrative functions via OMI component, or via web-based GUI
Monitoring and logging	Comprehensive and secure
Head-end interfaces	DVB Simulcrypt: ETSI TS 103 197, ECMG and EMMG (v2, v3)
Content scrambling	Performed by DVB Mux, using 64-bit DVB-CSA or AES
Capacity	Hundreds of channels per multiplexer, and thousands of channels in total, subject to Mux model and key mutation rate
DVB Multiplexer / Scrambler compatibility	AppearTV, Arris, Cisco, Ericsson, Harmonic, RGB Networks (now Imagine Communications), Thomson and others
Form factor	Several million STBs in 2RU (3.5”); 4RU if 1:1 redundant (BCSM + EE)
SMS/middleware API	API via OMI for rapid integration
Scalability	From trial system to millions of subscribers

3 VCAS Ultra for DVB – Supported Pay-TV Functions

3.1 Business Models and Features

- Pay-per-Channel (PPC): The consumer subscribes to one video or audio channel.
- Pay-per-View (PPV): The subscriber purchases single events only. VCAS provides features to define, schedule, entitle and de-entitle these events. Mass events are scheduled using a pre-defined XML format.
- Pay-per-Time (PPT): The subscriber purchases a fixed amount of time (whether minutes or hours). VCAS provides features to define, schedule, entitle and de-entitle these events.
- Impulse Pay-per-View (IPPV): While IPPV works like PPV, the subscriber entitlement is triggered either by the STB return channel, if available, else via credit or debit over-the-air. Credits are loaded to the subscriber's smart card over-the-air using the VCAS secure control messaging ("Virtual Wallet"). IPPV is a more user friendly solution compared to PPV.
- Pairing of smart card and STB: After pairing, an individual card can only be used in the STB it is paired to. Pairing effectively merges STB and card into a single trusted platform. There are several levels of pairing available. Pairing requires integration with a suitable STB.
- Prepaid / Scratch Card based (I)PPV or PPT, Push VOD (video on demand) purchase and credit loading: This allows the consumer to buy events and tokens by using scratch card codes that can be sold anonymously or on a registration basis. The codes can be activated by the customer via a call center, mobile phone text message or via a web server.

- Pre-entitlement/Demo Subscription: Valid for a pre-set period of time for first-time-use smart cards, typically used for promotional purposes.
- Prepaid Booking: This allows the customer to purchase e.g. 10 events out of a set of 30 in advance. Prepaid booking can be profitably employed to market sporting events, such as a football or basketball games season, where the subscriber does not know beforehand which games (events) will actually be watched later during the upcoming season.
- On-Screen Messages: Send text messages to individual customers, groups of customers or all customers. Such messages can be used for e.g. customer relations and promotions.
- User Data: Individual data can be stored in the smart card of each subscriber. This can be used for marketing or customer care, or customer convenience (e.g. to transport STB configuration data; project specific STB integration required).
- Parental Control: This provides the subscribers with a control mechanism that cannot be altered by STB manipulations. This feature is independent of any STB middleware security.
- Fully flexible output control and copy protection mechanisms
- OSD Fingerprinting (e.g. smart card number display) and watermarking
- Integration with a Customer Care & Billing System (CC&B, or Subscriber Management System) is facilitated through an open OMI SMS API.

3.2 Push VOD

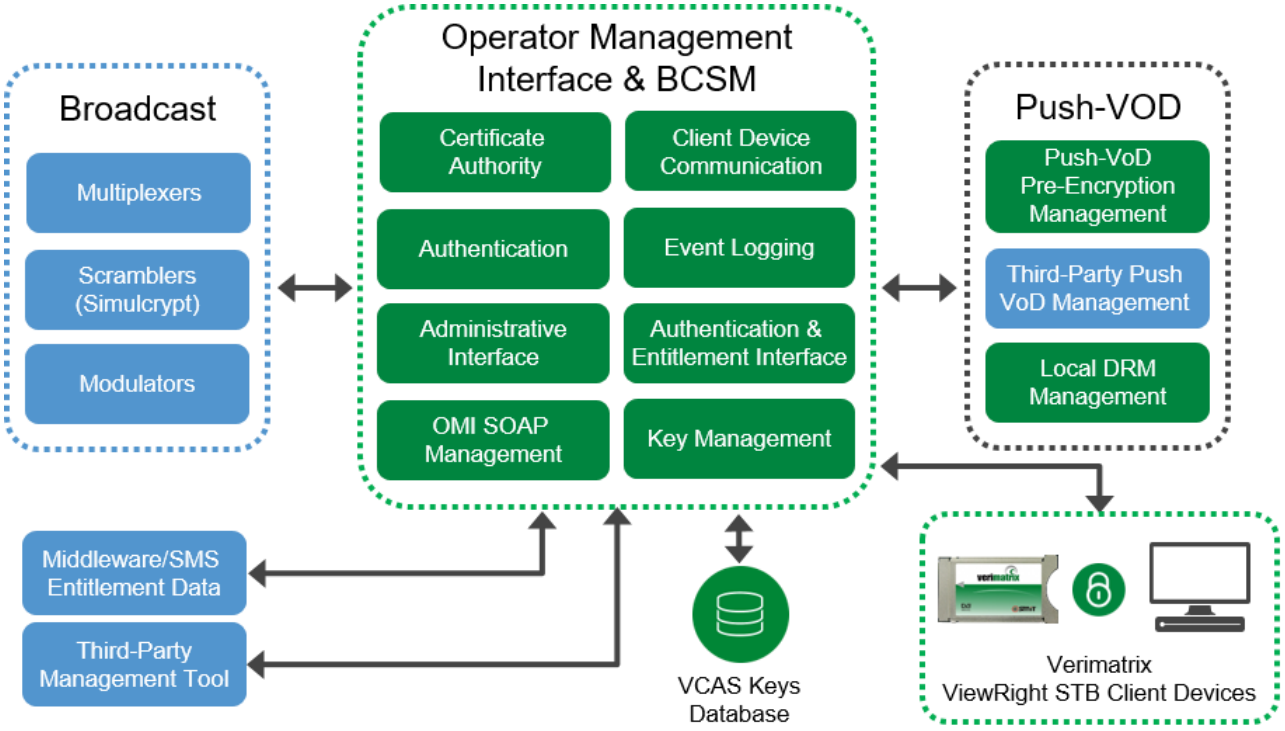
Push VOD, a form of video-on-demand for one-way broadcast systems, is supported by VCAS in several ways depending on the subscriber devices used and the service operator business model.

The DVB Push VOD model is highly efficient especially when the content is demanded frequently by the subscribers (e.g. top ten day & date movies). Even in advanced hybrid networks supporting direct OTT based VOD delivery, DVB Push VOD can provide a more efficient and less resource- consuming distribution model. For Push VOD, spare transponder capacity, e.g. during the night, can be utilized.

In order to provide these localized on-demand services content must first be pre-encrypted and pushed – usually cut into chunks to allow resuming of interrupted downloads – over the one-way broadcast-link to a Digital Video Recorder (DVR). The content is then available for transactional or event based purchases. The subscriber can thus watch the content on-demand, by playing it back from the DVR. The pushed content continuously stays under control of VCAS.

VCAS generally manages pre-encryption (in the head-end) and the local decryption (in the STB) of the content as well as the entitlement procedure. The push-based content delivery including the local storage mechanism in the STB is provided by third-party vendors. Verimatrix is open to integrate with any third-party manufactures as requested by the operator.

Encryption keys (in ECMs) are stored with the content, while the EMM retains the key required for play-back. It is also possible to change the play-back key over the air at a later point in time.



The entitlement mechanism can be asynchronous with respect to the content download. One or more products, represented by pushed content, can be entitled to one or more STBs.

For purchases, a direct (hybrid STB) or indirect return channel may be used, such as the Web, telephone call centers, or mobile phone text messages. The EMM has to be available in the STB prior to play-back, whether requested via indirect means or transmitted during the content download.

4 VCAS Ultra for DVB - Head-End Operations and Functions

4.1 Operator GUI

The VCAS Ultra for DVB head-end is configured via the universal VCAS GUI, which allows combined operation of all VCAS market solutions under a single security authority.

The additional monitoring interface provides an overview over the system state in one glance. The operator is notified of any critical alarms by means of acoustical signals. Extensive monitoring information and benchmarking data is provided via the GUI.

4.2 Service Configuration

Pay-TV services (“products”) and subscriber entitlements are defined and communicated from the CC&B or GUI via the OMI SOAP interface in order to control typical features:

- Defining products (channels and program tiers)
- Defining events
- Scheduling events
- Entitling subscriber(s)
- De-entitling subscriber(s)
- Definition of which service (“channel”) shall be included in each product (program group or “tier”). Many combinations of channels and tiers are possible.
- Definition whether a service shall be access restricted with parental control.
- Definition whether a service shall be part of a pre-entitlement subscription. (Pre-entitlement means a demo-subscription valid for a specific period of time.)
- Definition and automatic scheduling of PPV and PPT events (definition of the service used, start time, stop time, interrupts, repetitions, etc.). In these business models the subscriber is only allowed to have access to a service for a specific event or period of time that has been purchased in advance.

VCAS Ultra for DVB features flexible client messaging to a unique STB, a group of STBs, or all:

- Explicit payment reminder, promotion, emergency messages
- Trigger STB actions for:
  - Upgrade
  - Rescan
  - Service change
  - Emergency service switch handling
  - Operator defined triggers

Other configuration options include:

- Automatic subscription extension until explicit subscription suspension from SMS
- Automatic subscription ends if no extension EMM is received.

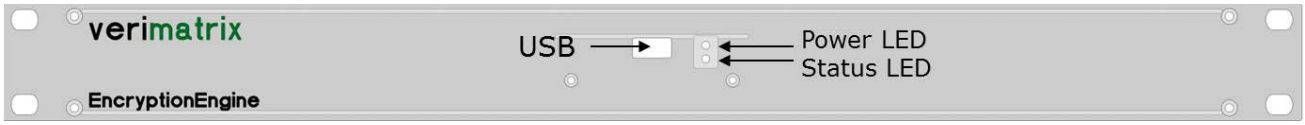
4.3 *Verimatrix EncryptionEngine™*

The Verimatrix EncryptionEngine is a hardware-based, high-performance product that manages all VCAS Ultra for DVB head-end cryptographic operations. It protects cryptographic ciphers and control mechanisms, including the set of operator keys. It also holds the operator-specific Super Master Key (SMK), which is used to encrypt subscriber-related information.

All VCAS keys are provided to operators in encrypted form. Keys are never stored in the clear. Keys are processed, and messages are encrypted and encapsulated, in the EncryptionEngine only. VCAS keys are never transmitted in the clear and no unencrypted information ever leaves the device. All information is lost if the device is tampered with or powered off.

The device supports cryptographic operations for up to millions of STBs in only 1 RU space. Multiple units can be configured for redundancy and larger STB populations.

Front



Rear

Product Features

- Proprietary, high-performance encryptor card
- Supports cryptographic operations for up to 1 million STBs
- Ethernet/RJ-45 connector
- USB connector for Key Injector interfacing
- Power LED
- Status LED
- Dimensions – H: 1.75” (1RU), D: 5.50”, W: 19”

Arming Cards and Key Injector: The EncryptionEngine is initialized with key data during start-up using a Key Injector and a set of EncryptionEngine Arming Cards. The initialization procedure entails the transfer of the SMK to the encryptor. Three unique EncryptionEngine Arming Cards, each holding part of the SMK, are issued to each service operator, together with a 16-digit PIN code for each. Three trusted employees each receive one card together with a PIN code. Any two out of the three cards are required and sufficient to initialize the encryptor using the Key Injector (connected via USB interface). The cards can be inserted in any order. When the PINs have been entered, and accepted for any two cards of the three, the initialization is complete. The initialization procedure is performed at system boot-up and after any power cycling, and only needs to be carried out once even if multiple encryptor units are configured.

Figure 3: Set of Three Arming Cards

5 VCAS Ultra SI Spooler

5.1 Overview

The VCAS Ultra Service Information Spooler (SIS) is an optional component of VCAS Ultra for DVB. It enables the operator to import or create, edit and play out standards-compliant DVB Event Information Tables (EIT) with TV program schedule information, containing the name of the event (program), start and end times, and an optional event description such as movie synopsis and names of the director and actors.

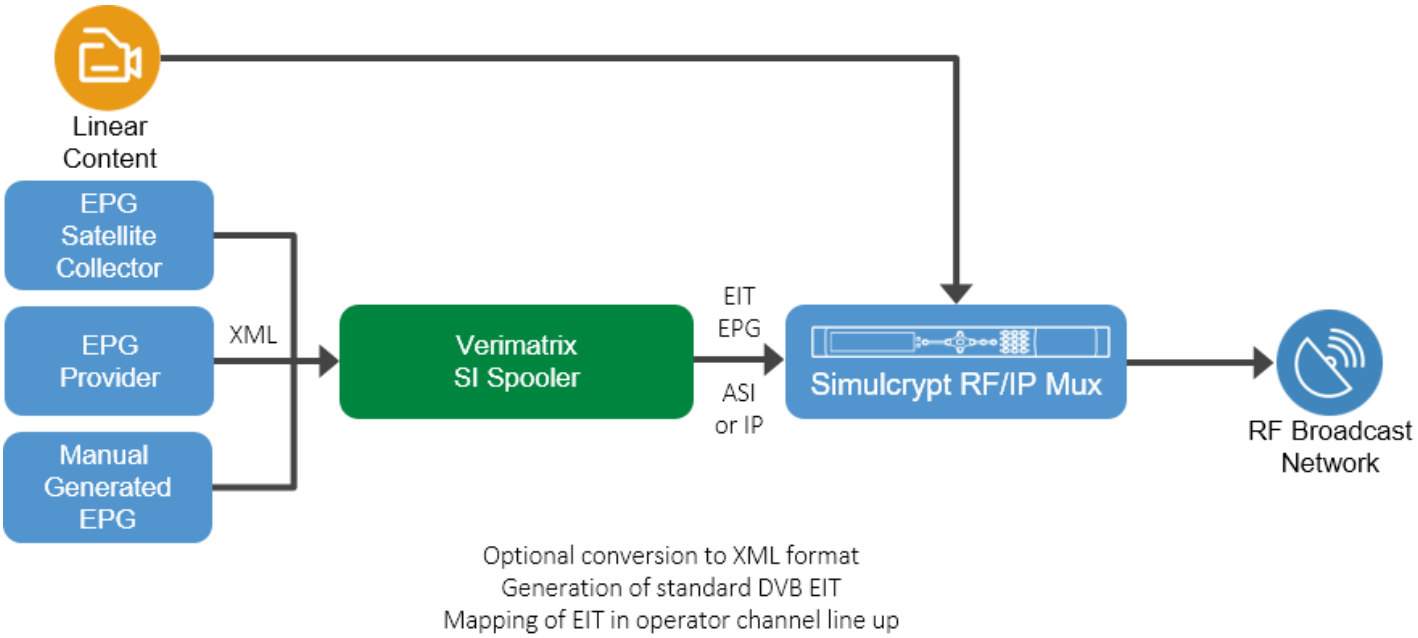


Figure 4: Verimatrix SI Spooler in Context

Apart from the EIT, the SIS can also generate and play out other tables including NIT, SDT, TDT/TOT and BAT.

The data is broadcast in the MPEG-2 Transport Stream, via the DVB multiplexer, and used by each STB to fill the EPG the pertinent information. The subscriber chooses events to watch or record from the EPG. The data can also trigger automatic recording by a Digital Video Recorder (DVR).

The SIS ingests an XML file containing program schedules, from which it extracts the information and builds the EIT tables. The tables are played out, timed, and repeated according to the event schedule, so that the information is available at any time on-air. Parameters such as the maximum bandwidth allocated for SI information, and the play-out repeat rate, are set via the operator GUI. The repeat rate is reduced automatically if the bandwidth limit is reached.

SIS is completely middleware-independent and offers several data ingestion methods:

- Programming package providers such as HBO
- Free Internet data sources such as TV.com
- Third-party providers, like Tribune Media Services (pre-integrated)
- XML interface facilitates data import

Several options for creating and editing data include:

- HTML interface to create event data from scratch
- GUI can be used for on-the-fly edit of imported data
- External editing tools can be used via the XML interface

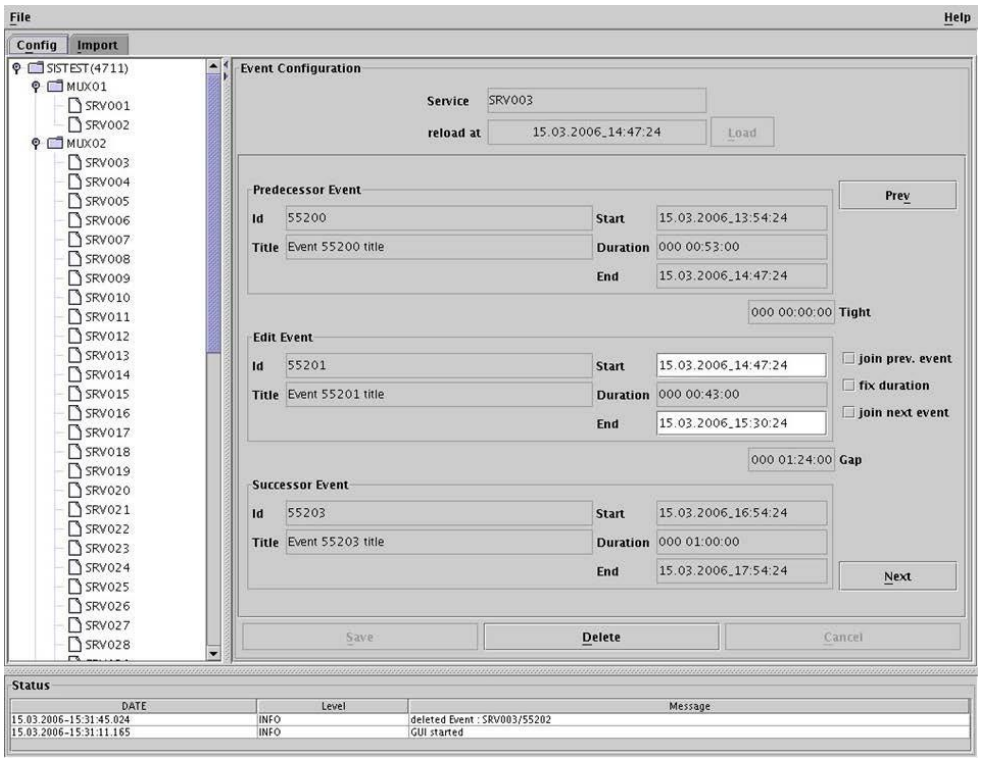


Figure 5: SI Spooler GUI - Example

5.2 Product Features

Platform	Runs on Verimatrix Broadcast CSM hardware platform or, optionally, on a stand-alone, rack mount server (1RU)
Standards	DVB, ETSI TR 101 211 V1.6.1
File import	XML
EPG database range	Up to 64 days look ahead
Max. no. of multiplexes per network	Limited only by DVB specification, and output bandwidth
Max. no. of services per multiplex	Limited only by DVB specification, and output bandwidth
Max. size of the event description	Limited only by DVB specification, cycling time and output bandwidth

6 ViewRight® STB for DVB – One-way Networks

6.1 Overview

Verimatrix ViewRight® STB for DVB is a robust package of portable embedded code that implements the VCAS security functions within each STB in a pay-TV system. The ViewRight STB code has been designed to require only a minimum of resources from the STB hardware and run- time environment and use a standardized set of simple interfaces to any STB control software and/or middleware. ViewRight STB has been architected to be highly portable to different hardware architectures and run-time environments.

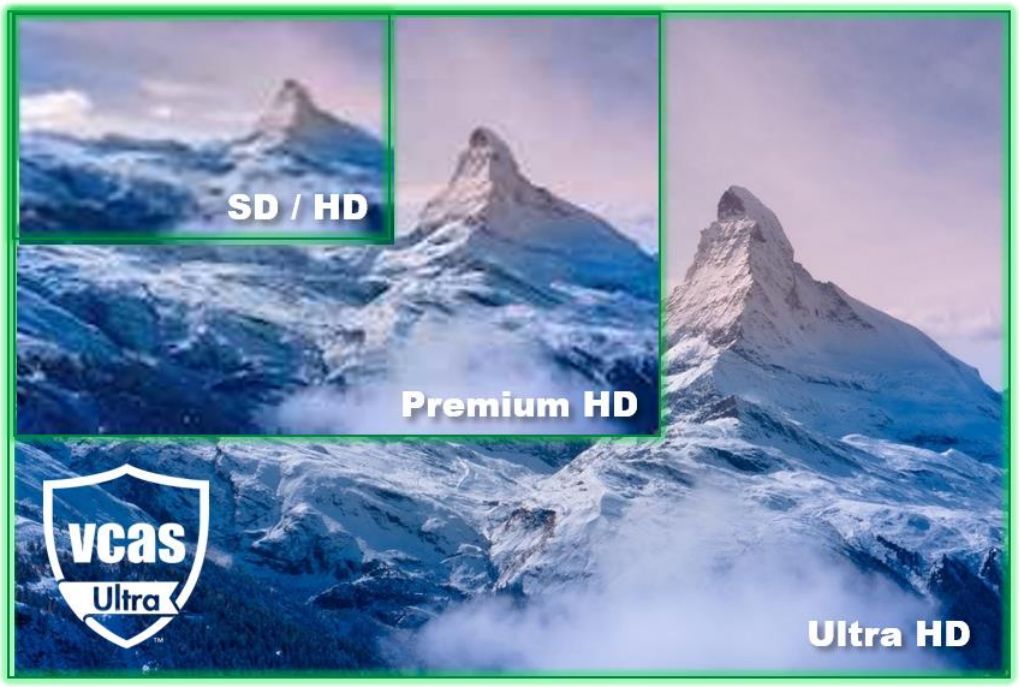


Figure 6: ViewRight STB for DVB - Client Security and Content Quality Options

In contrast to legacy systems with a singular focus on card based security, Verimatrix offers both cardless and card based clients, including advanced chip security integrations, with a choice of three levels to adapt the security to the value of the content and subscriber revenue potential:

Standard Security

- Verimatrix standard software based security
- Protects Linear TV SD and HD content

Advanced Security

- Hardware based security
- Required for premium HD or early release window content

Ultra Security

- Highest level of security to address MovieLabs recommendations
- Protects premium UHD / 4K content (VOD and Linear TV)

The embedded, secure system-on-chip (SOC) and TEE based clients provide hardware-level security without card logistics, including professional CI CAMs and consumer CI+ CAMs.

The NSC (No Smart Card, or cardless) software-based client offers best-of-breed content and revenue protection in a hardened implementation that incorporates signing, multiple levels of integrity checking, obfuscation and other advanced security features.

Secure SOC implementations are available, combining the best of hardware- and software-based security by utilizing the security features of modern SOCs. This client is the perfect choice for operators wishing to deploy hardware-supported security but without the logistics of cards. The secure SOC client utilizes the advanced security of modern STB chipsets, including TEE, and features secure boot, control word obfuscation, secure code execution, protected memory and encrypted data paths securing the video pipeline. This protects the system against threats such as control word re- distribution and card sharing.

Smart card-based security is available for operators preferring removable security, including a DVB-CI (Common Interface) and CI+ CAM modules. The smart card implementation utilizes a state-of-the-art Common Criteria (CC) EAL5+ High Profile chip together with an advanced client design incorporating passive, active and adaptive security features, making it an elusive and moving target for potential hackers.

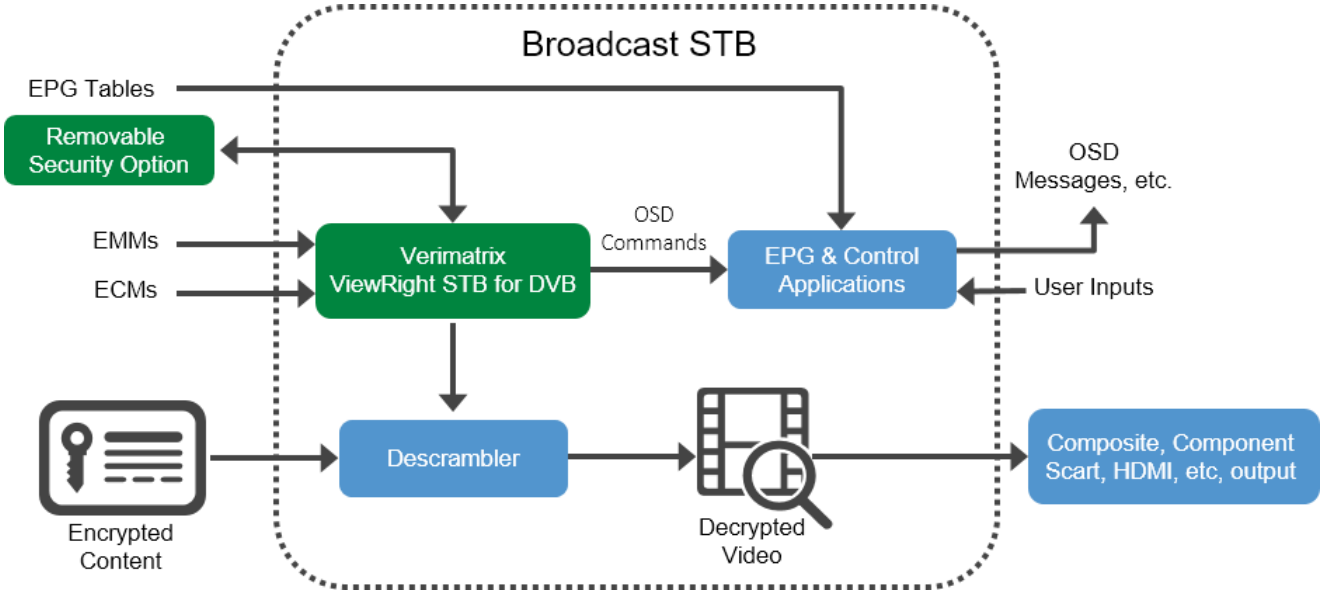


Figure 7: ViewRight STB for DVB - Context

The clients have different personalization processes and characteristics as follows:

- HW-based client model
  - Personalization resides in Smart Card
    - Process performed by Verimatrix prior to delivery
  - Personalized Smart Card is unique to a service operator
  - Same STB model can be used by other operators
    - Each operator uses a unique Smart Card personalization

- Cardless client model utilizing secure SOC
  - Personalization resides in STB
    - Individualization process performed during STB manufacture
    - Optional utilization of TEE based security
  - Personalized STB is unique to a service operator
  - Smart card not required

To prevent “Trojan Horse” attacks the secure SOC and smart card code cannot be updated over-the-air, to safeguard against introduction of malicious code. Various counter measures can be executed OTA, which may activate back-up algorithms and keys but not change the code itself.

6.2 General Product Features

Basics	EMM, ECM, OSD Messaging, (I)PPV, Push VOD
STB secure chipsets	Ali, Broadcom, Fujitsu, MStar, NEC, ST, AMLogic
Smart card chip	Common Criteria (CC) EAL5+ High Profile
DVB-CI Module	Available from SMiT & Neotion; others upon request
STBs	Variety of DVB-C/C2/S/S2/T/T2 and MMDS pre-integrated models, several IP capable and ready for hybrid DVB-IP/OTT services.
Memory footprint, SW- based client	500-750KB (depends on platform and security level)
Scrambling algorithms	DVB-CSA; also AES if supported by STB
Broadcast support	MPEG-2 Multi-Program Transport Streams (MPTS)

6.3 ViewRight Ultra STB for DVB Security Features

- Hardware Root of Trust
  - Formal SoC Certification for Ultra Security Content
- Secure Video Path Support
  - Verified at the SoC platform level using TEE
- HDCP 2.2 Protection and Signaling
  - Controlled asset by asset from head-end
- Third-Party Audits
  - Riscure hardware audits: including side channel attack and TEE verification
  - Farncombe VCAS Ultra system audit passed
- VideoMark™ Forensic Watermarking
  - Hardware based watermarking integrated at the SoC level
  - Optional component

6.4 ViewRight DVB – CI Professional

Verimatrix offers a high-performance DVB CA Module (CAM) based on the DVB Common Interface (DVB-CI) standard. Features:

- Descrambling of 1-6 MPEG-2/MPEG4 video services simultaneously contained in MPEG-2 Transport Streams
- Transport Stream processing bandwidth: Up to 96 Mbps
- Up to 64 configurable PID filters to support TS packet filtering or section data
- Supports over-the-air (OTA) software upgrade
- Secure Loader for highly secure and efficient software upgrade
- DVB-CI standard (EN50221)

It is used for B2B video distribution applications, where it is paired with a Co l IRD (Integrated Receiver Decoder)

6.5 ViewRight DVB – CI Consumer

The ViewRight DVB-CI Consumer is a secure CAM intended for STBs and TVs with CAM expansion slots. It provides a single service decryption. The advantage with this type of product is that the STB can be CA agnostic since no CA client integration is required.

6.6 ViewRight CI+

The ViewRight CI+ CAM is a low-cost consumer device based on the SMiT SM1660 platform, offering a choice of an embedded cardless ViewRight client and a smart card client.. It implements support for CI+ v1.2 and v1.3, and supports copy protection and output control according to CI+ specification.

6.7 Full Operator STB and Key Control

The Verimatrix goal is to achieve the highest levels of security and integrity without imposing vendor lock-in on the operator's STB population. To that end, Verimatrix provides each operator with options for signature ownership and integrity management, which is achieved through:

- Creative use of generic SOC security features where available
- Enable, where possible, third-party SOC personalization services with escrow option
- Provide option for operator bootstrap ownership
- Provide options for application image ownership and signing logistics.

Verimatrix works closely with each operator to tailor the solution to actual needs. In this way, each operator can be assured of the best content protection and solution integrity while retaining flexibility for future security needs.

7 VCAS Ultra for DVB-Hybrid: Combining DVB and OTT Services

Early incarnations of hybrid architectures were realized by combining DVB and managed IP networks. This has shifted towards combinations of DVB and Internet TV (OTT) delivery, fueled by the broad adoption of adaptive bitrate (ABR) streaming protocols, such as HLS and MPEG-DASH, which power broadcast quality OTT video services and thereby enabling an efficient service upgrade strategy for DVB operators:

- Linear content DVB services
- Zapper and advanced DVB-Hybrid STB clients
- Linear and on-demand OTT services using adaptive bitrate streaming
- Broadest range of CE device support through ViewRight Web clients

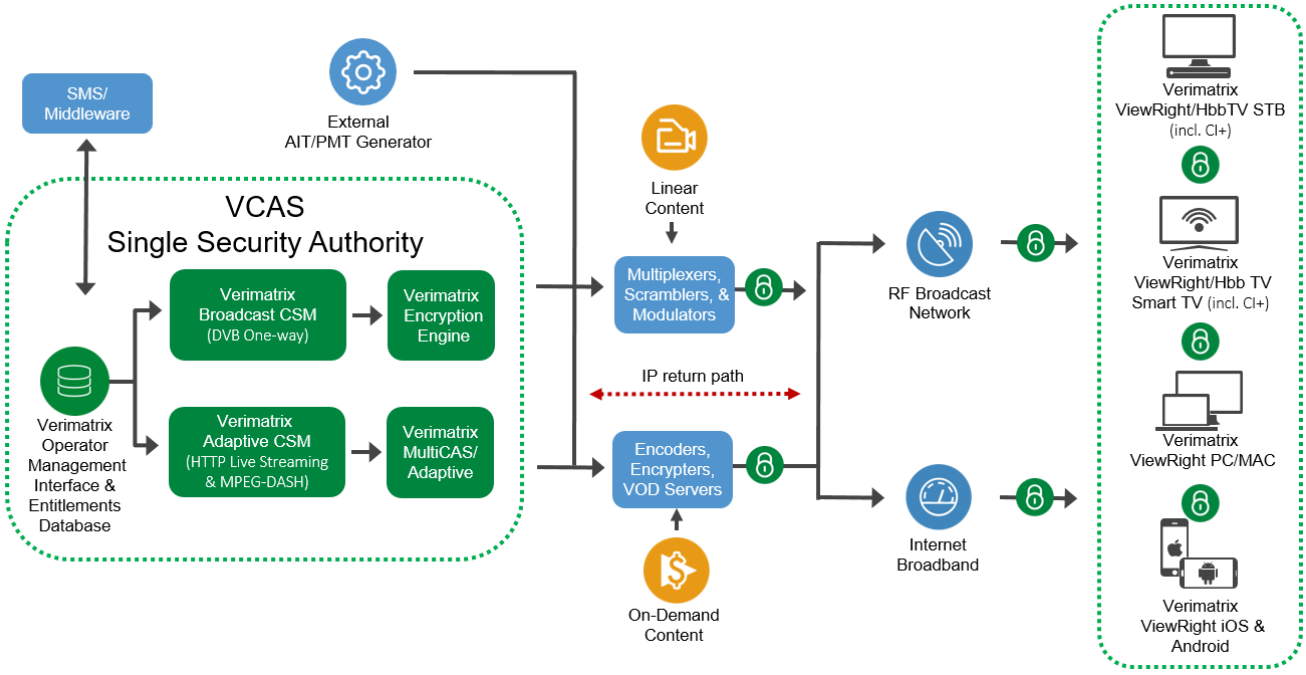


Figure 8: VCAS Ultra for DVB-Hybrid Architecture

In the diagram above, VCAS provides cross-network domain-based rights management: when a subscriber's domain (as opposed to a single device) is entitled to specific content, all the devices of the domain are entitled automatically, enabling a frictionless user experience.

The ABR delivery method makes use of what the Web does best – efficient and massively scalable delivery of data, in this case video – using the HTTP protocol. ABR is also particularly well-suited to mobile content delivery, as it replaces the concept of fixed network managed quality of service (QoS) in favor of a client optimized experience.

The focus on quality of experience (QoE) is particularly important given that an enjoyable television experience has traditionally been best supported in a controlled, managed network. Achieving an effective QoS over the multi-hop Internet has always seemed daunting. The ABR protocols HTTP Live Streaming (HLS) – originally defined by Apple – and MPEG-DASH are well-positioned to address QoE challenges.

ABR technology has emerged as an ideal complement to DVB network delivery. Consumers with high-bandwidth connections and newer hardware can experience HD quality video streaming, while those with lower bandwidth receive a stream optimum to local conditions. Each user enjoys an uninterrupted experience with the highest quality possible. It even permits extension of services across different screen resolutions, and seamless roaming between Wi-Fi and 3G/4G networks.

Another ABR protocol advantage is that content delivery networks (CDNs) already have massive deployments of acceleration servers supporting HTTP protocols (the Web file delivery standard).

Leveraging HLS enables new hybrid video service architectures and business models, and it offers a fast and cost-effective route for adding interactive services to previously broadcast-only pay-TV networks. Thus a new breed of multi-network architectures is born, referred to as Hybrid DVB+OTT.

HLS and MPEG-DASH are particularly attractive for DVB operators as widespread vendor support for these standards simplifies the deployment process while also facilitating the development of new business models and increasing revenue security. A deft combination of a managed DVB network foundation complemented by HLS and DASH delivered services can hit a number of important bases, including:

- High quality television presentation on the household main screen.
- New business models that include on-demand services as well as live DVB+OTT subscriptions.
- Seamless catch-up TV and time shift services over unicast connections.
- Unified program guide navigation for managed and unmanaged network content feeds.

As the leading IPTV content security supplier, Verimatrix has applied its extensive experience in protecting premium TV services delivered over IP networks. VCAS Ultra for Internet TV includes enhancements to the baseline HLS and DASH protocols, making it suitable for delivering high-value pay-TV content in both live and on-demand scenarios.

Verimatrix provides secure HLS and DASH key management and other security related features required in IPTV and DVB pay-TV systems, in order to protect both content and service revenue. This includes device authentication and entitlement management, to assure that client devices are attached to paying customers.

Using a combination of DVB and HLS / DASH provides operators with an ideal environment for deploying hybrid STBs with a unified security regime. The resulting hybrid service delivery is fully protected by VCAS, which provides a unified multi-network platform, protecting multi-screen services to hybrid STBs, HbbTV enabled devices, PC/Macs, tablets and smart phones.

8 Security Considerations and Conclusion

8.1 Security Strategy and Changing Threat Models – Future-Proofing the Platform

The potential content security threats posed to one-way broadcast systems, without any return channel from the STB to the head-end, are more challenging compared to a two-way, IP-based network. In this regard, VCAS Ultra for DVB is designed not only to make hacking as difficult as possible, but also highly unrewarding in that any attempt that may appear to have succeeded will quickly be foiled by pre-defined counter measures. A document, available under NDA, outlines and highlight the steps Verimatrix has taken from a technology choice and implementation perspective, and the operational steps that will be taken in case of a security challenge.

As the video distribution industry is undergoing rapid changes, Verimatrix is focused on providing future proof – investment proof – solutions. VCAS Ultra for DVB is part of the multi-network VCAS platform that addresses, among else, the following aspects:

- ✓ Extension to video delivery over IP, either as IPTV or OTT, and hybrid combinations
- ✓ Video watermarking, a requirement for licensing of content in the early release window, and for Ultra HD/4K video services. Verimatrix VideoMark enables watermarking at the STB level. Since online content re-distribution is now the main form of piracy, watermarking must be considered from the outset.
- ✓ SOC hardening, increased security and countermeasures in cardless solutions. Verimatrix chipset partners feature enhanced security technology, utilized by the ViewRight Ultra STB client when operators choose the latest SOCs with support for TEE.

8.2 Benefit from the Verimatrix Partner Ecosystem

The Verimatrix business strategy includes building and sustaining a network of strategic alliances with a broad range of the most significant pay-TV technology providers and CE manufacturers. These relationships, which emphasize seamless technology integration, ease of operation and extended value, enable Verimatrix to offer pre-integrated best-of-breed solutions to our customers and their users. The range of established partnerships is very wide and includes companies that offer products and services such as content aggregation, system integration, video processing, VOD servers, subscriber management and middleware systems, set-top boxes, connected/smart TVs, tablets and smart phones.

8.3 Conclusion

The introduction of hybrid RF and IP/OTT pay-TV systems offers the potential for a tremendous expansion of entertainment services coupled with revenue generating capabilities such as VOD. Key to making such services cost effective is the optimization of the content security architecture to enable a single system to handle linear content, whether over one-way or two-way networks, and IP- based VOD. VCAS Ultra for DVB is the answer for operators seeking a lower total cost of ownership while positioning them favorably in a competitive environment that is moving inexorably towards two-way connectivity and interactivity. The end result is the most optimal pay-TV security solution that is ready to tackle any challenges, now and into the future.

Verimatrix offers a cost-effective content and revenue security approach that is ideal for:

- ✓ Cardless security in client devices with secure System-on-a-Chip (SOC) facilities
- ✓ DVB-Hybrid services, including OTT delivery to STBs, TV sets, tablets and smart phones
- ✓ Greenfield deployments, whether B2C or B2B, and analog-to-digital transitions
- ✓ Operators wishing to complement or replace aging and legacy DVB CA systems

9 Verimatrix – Beyond Content Protection to *Revenue Security*™

About Verimatrix

Leveraging a combination of established video standards and proven Internet technologies, Verimatrix has become recognized as the global number one in revenue security for connected video devices. Today, we are the trusted specialist in this space, with a range of VCAS™ security solutions that address multiple video delivery networks with a unified approach to rights management. Our global deployment footprint and deep management expertise give Verimatrix an unparalleled insight to technology and market trends. As a result, we are now extending our market leadership position with Verspective™ Intelligence - a globally interconnected security platform. This cloud resource enables operators to take advantage of global scale to address operational challenges, while improving competitiveness through visibility of service usage and consumer behavior.

Why Verimatrix

Verimatrix specializes in securing and enhancing revenue for multi-network, multi-screen video services around the world. We offer fast deployment through unmatched numbers of partner integrations, highly responsive customer support, and award-winning technology. Our forward-thinking solutions boast multiple industry awards for innovation, deployment, and flexibility.

Trust

Over 850 operators have deployed Verimatrix solutions in more than 110 countries, protecting content on over 110 million screens. Based on the favorable results in independent audits, and an excellent service record, VCAS is the approved pay-TV and revenue security choice by operators on a worldwide basis. VCAS operators benefit with the most favorable access to premium content, from e.g. Discovery, Disney, ESPN, HBO, Showtime and Turner.

Ease of Deployment

Verimatrix is integrated with a vast ecosystem of partners, accelerating speed to market.

Scalability

Verimatrix technology and solutions are highly flexible and customizable to scale with an operator's business.

Headquartered in San Diego, California, Verimatrix is an ISO 9001:2008 certified company with direct and indirect representation in 100+ countries while offering 24/7/365 customer care globally.
www.verimatrix.com info@verimatrix.com