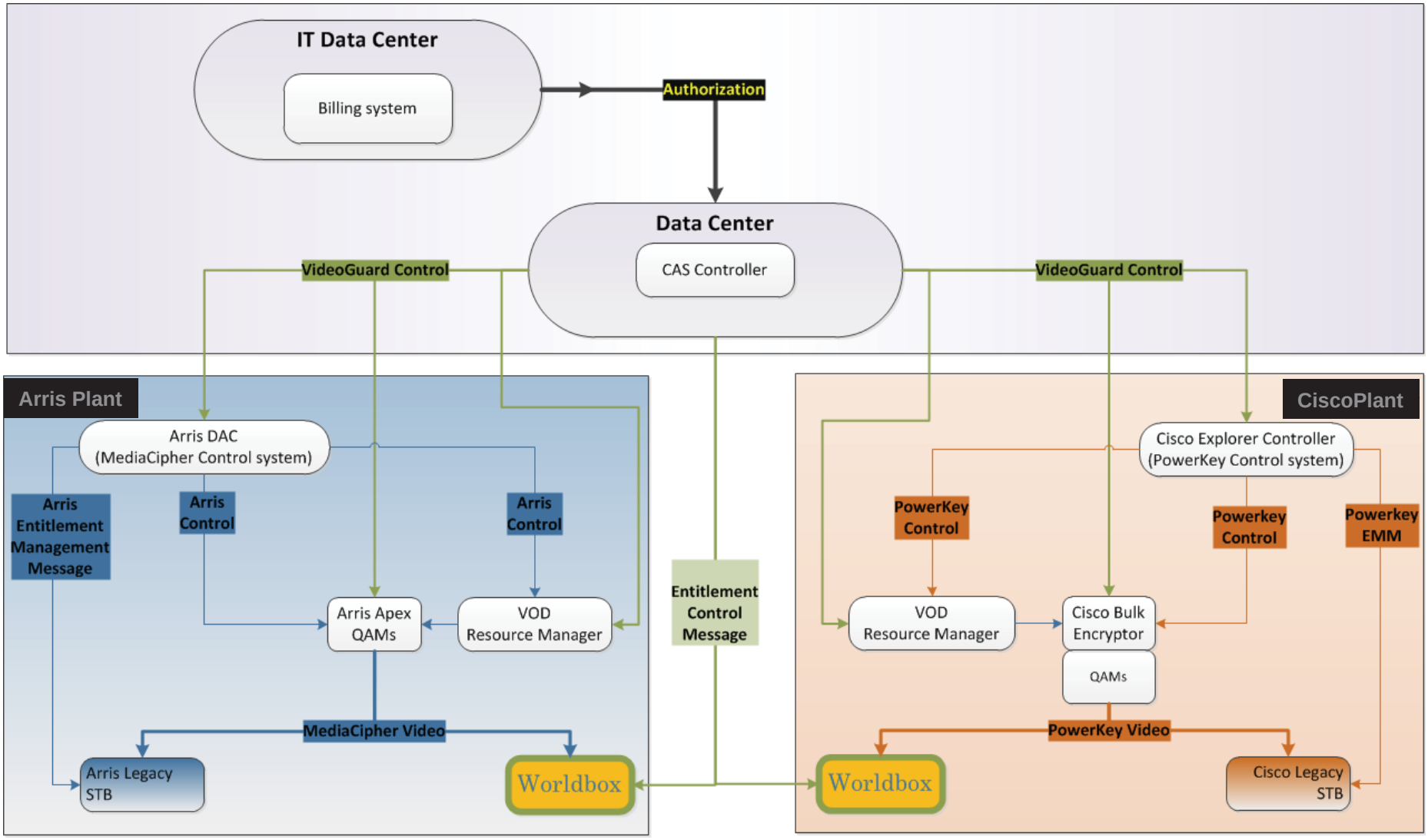
# OMS overview for DSTAC

Jim Alexander, Senior Director

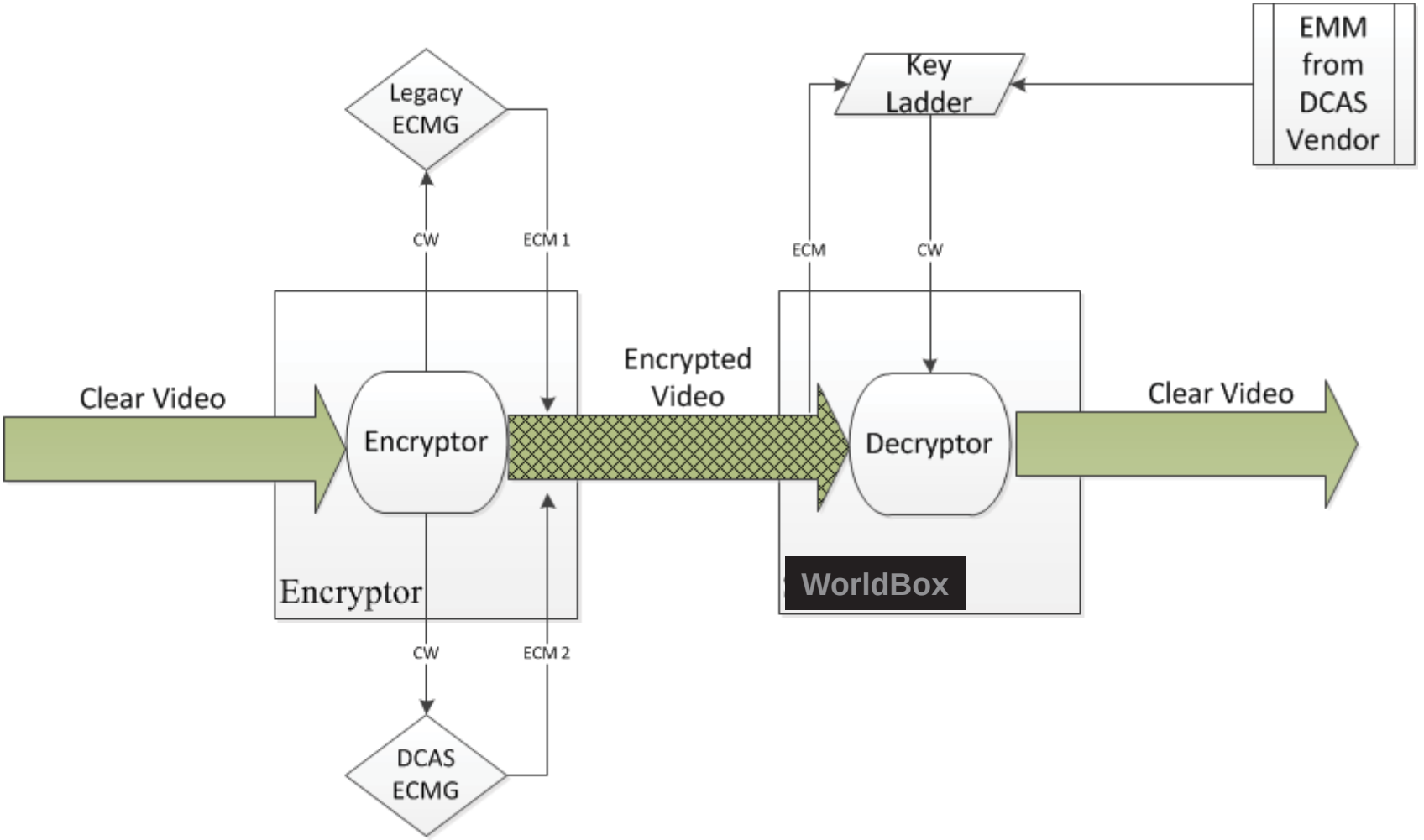
June 2, 2015

# Charter Supports Two Legacy Footprints




Charter COMMUNICATIONS

# Simulcrypt & a Worldbox



# Open Media Security (OMS) Overview

- OMS is designed to provide downloadable conditional access (DCAS) functionality for MVPDs. Supports multiple CAS Vendors.
- Enables consumer electronics (CE) manufacturers to build devices for retail sale and/or lease by service providers using qualified commodity chipsets that will be available from multiple chipset manufacturers.
- Designed to preserve the security of legacy CAS systems.
- Cablevision and Charter have both invested in extensive upgrades to their networks to support OMS. Both have deployed OMS set-top boxes, built on commodity.

# OMS: Solution Components

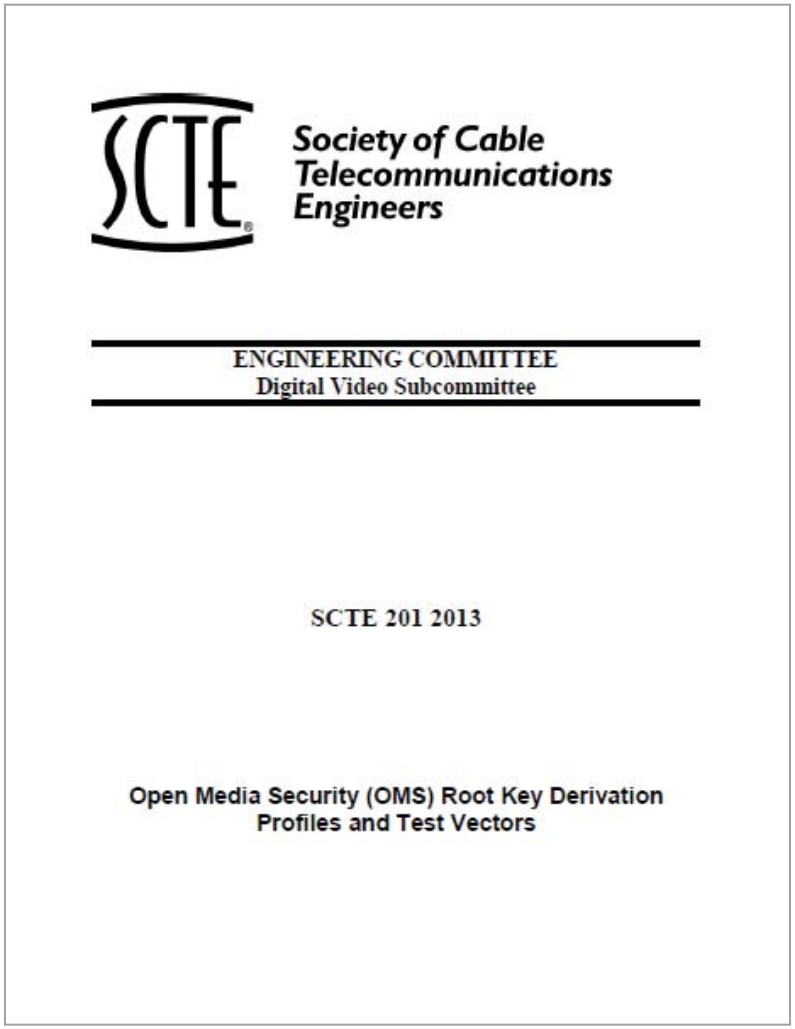
**OMS defines the components necessary to deliver all MVPD Services, and do so in conjunction with legacy networks.**

- Hardware – Definition of SoC and STB features and robustness rules.
- Software – Definition of downloader, boot-loader, CAS, and UI functionality, robustness rules.
- Network – Definition of network capabilities, attachment, authentication.
- Trust Structure – Definition of key generation, black-box process, and distribution of security secrets.

# OMS: Components– Hardware Requirements

- SoC with a secure processer that conforms with robustness rules and includes:
  - ETSI KLAD – Key ladder for decryption of video.
  - CSA, AES, and SCTE-52 decryption (licensing required).
  - Hardware root of trust OTP Key(s) from approved trust authority.
  - Boot loader functionality.
  - Other keys for secure messaging
  - Encryption tools for output of video (i.e., DTCP, or HDCP).
  - Robustness Rules
- STB or other digital devices
  - SoC Requirements
  - Keying elements
  - Robustness rules

# KLAD is an SCTE & ETSI Standard.

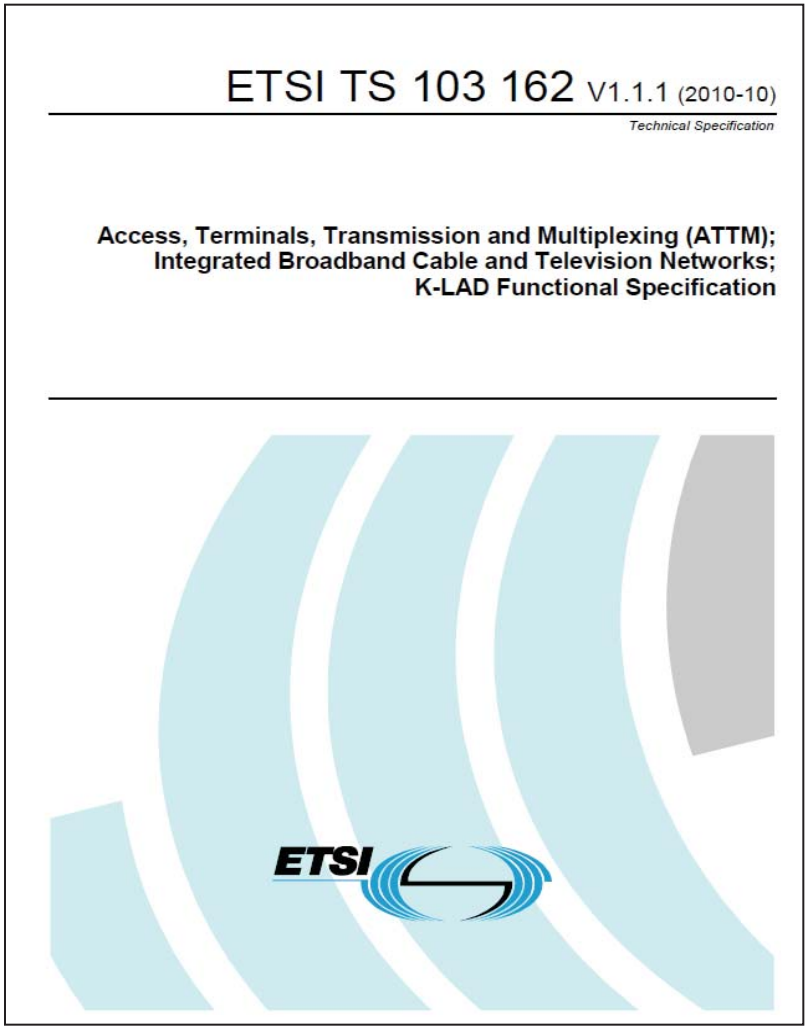


Society of Cable Telecommunications Engineers

ENGINEERING COMMITTEE
Digital Video Subcommittee

SCTE 201 2013

Open Media Security (OMS) Root Key Derivation Profiles and Test Vectors



ETSI TS 103 162 V1.1.1 (2010-10)

*Technical Specification*

Access, Terminals, Transmission and Multiplexing (ATTM);
Integrated Broadband Cable and Television Networks;
K-LAD Functional Specification

ETSI

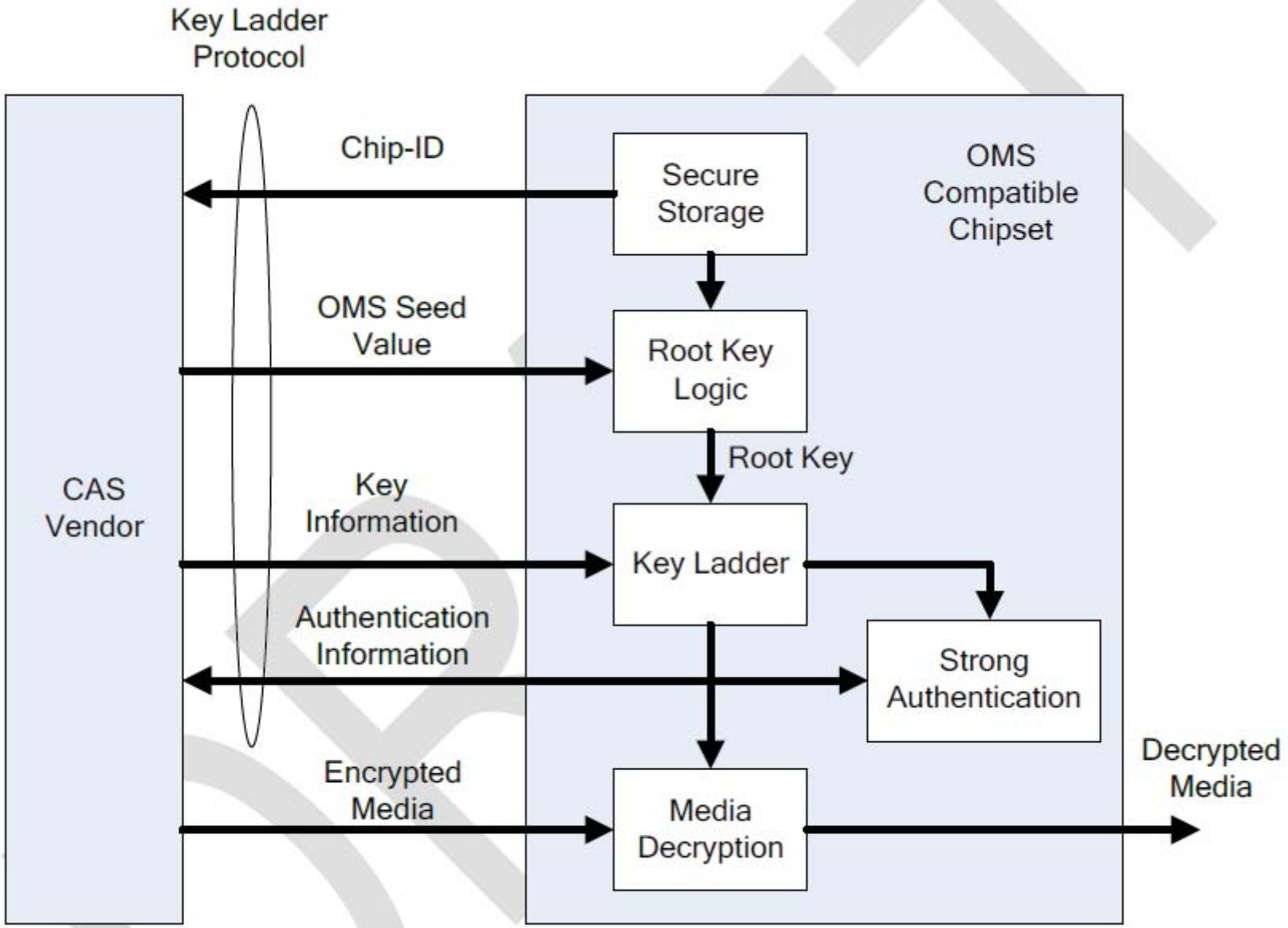



*Figure 2. OpenSAC Key Ladder in an OMS Compatible Chipset*

# OMS: Components – Software (1)

- CAS Client
  - APIs support a downloadable CAS client, which manages the keyladder and other decryption functions.
  - Specific CAS vendors are not defined, OMS can support most commercial CAS systems.
  - CAS Vendors or CAS versions can be replaced at any time to support business needs, or in case of a breach.
  - KLAD provides a mechanism to support keys for great numbers of CAS vendors.
  - DRM implementations are under development in labs.
- Secure execution environment
  - KLAD APIs.
  - CAS Client APIs
  - MVPD Service APIs (HTML5).
  - Robustness rules & evaluation processes.

# OMS: Components – Software (2)

- Applications
  - HTML5 controls all MVPD service features.
- Code Signing, Boot Loader & Downloader
  - The boot loader and downloaded code is validated by hardware root of trust.
  - All applications must be signed by the security solution or operator.

# OMS: Components – Network

- Requires two-way network
  - Challenge-Response Device Identification
  - Two-way authentication update processes.
- Includes requirements for deployment on legacy cable networks:
  - Powerkey with CSA Encryption
  - MediaCipher with SCTE-52 Encryption
  - Supports future networks, includes AES and other encryption technologies.
- Mechanisms for:
  - Network Attachment
  - Boot loading
  - Code download
- CAS Communication
  - Defined interfaces used by the CAS client

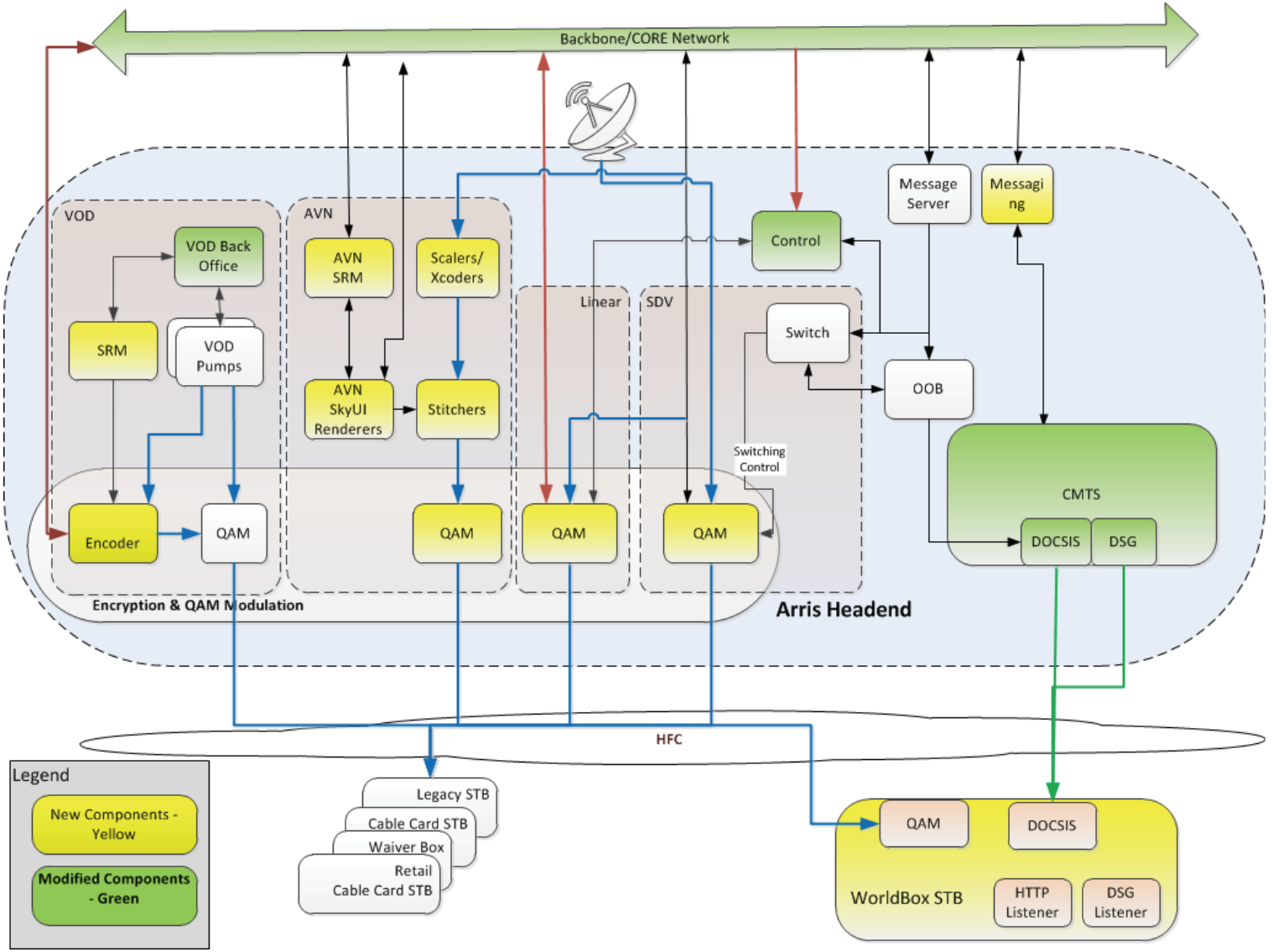
# OMS: Components – Trust

- A Trust Authority to defines, creates and manages keys
  - Black-box process for placing keys on a SoC.
  - Process for security elements on a device.
  - Key exchange process with CAS vendor(s).
  - Key exchange process with MVPD(s).
  - Whitelist, blacklist, remediation
  - Key security auditing.
- Multiple CAS vendor support
  - KLAD keys can support thousands of CAS vendors, through obfuscation functions.
  - Supports CAS updating and replacement.

# OMS: Cost elements

- OMS ensures the continued operation and security of deployed legacy CAS systems.
- The operator must upgrade their system to support Simulcrypting MPEG streams, this typically includes:
  - addition of a new CAS controller
  - integration of the CAS system with legacy billing systems
  - integration of the CAS controller with legacy control systems
  - integration of CAS with the guide, VOD, SDV, and PPV systems
  - upgrade of all encryptors to support a DVB Simulcrypt synchronizer.
- Teams throughout an MVPD.
  - Operations, warehouse, field technicians.
  - Networking and data center teams.
  - CSRs and support.
  - Legal, contracting, programming.

# DCAS Enabled Arris Market




Charter COMMUNICATIONS

# OMS: Summary

- Practical solution to support downloadable CAS, while preserving integrity of legacy MVPD systems.
  - Protects legacy security.
  - Deployed by Cablevision and Charter.
- Specifies hardware, software, network and trust structures to ensure security.
- Requires extensive network changes by MVPD.

# Thank you

Questions?

Jim.alexander@charter.com