

DSTAC WG2 Background Prepared for DSTAC WG3

June 2, 2015

Presented by: Ralph W. Brown

Diversity of MVPD Conditional Access Systems

- MVPDs deploy a diversity of security solutions for their set-top boxes
 - Most deploy CAS, one deploys DRM
- Key differences:
 - Proprietary ECM/EMMs
 - Core Cipher used
 - Trust infrastructure
- Leads to non-interoperable security solutions

MVPD	CAS (MVPD STB)	Core Cipher
Cable	<ul style="list-style-type: none">• DigiCipher 2• MediaCipher• PowerKey• NDS VideoGuard• Conax• Nagravision• OMS• BBT	<ul style="list-style-type: none">• DES-CBC• DES-CBC• DES-ECB• CSA• CSA• CSA• CSA/DES/AES• AES
Satellite	<ul style="list-style-type: none">• NDS VideoGuard• Nagravision	<ul style="list-style-type: none">• DES/AES• CSA/DES/AES
Telco	<ul style="list-style-type: none">• Mediaroom DRM• MediaCipher & PowerKey	<ul style="list-style-type: none">• AES• CSA

WG2 Presentation Materials: <https://owncloud.cablelabs.com/public.php?service=files&t=b8db53318e0c2f9184e92adc4be6c583>

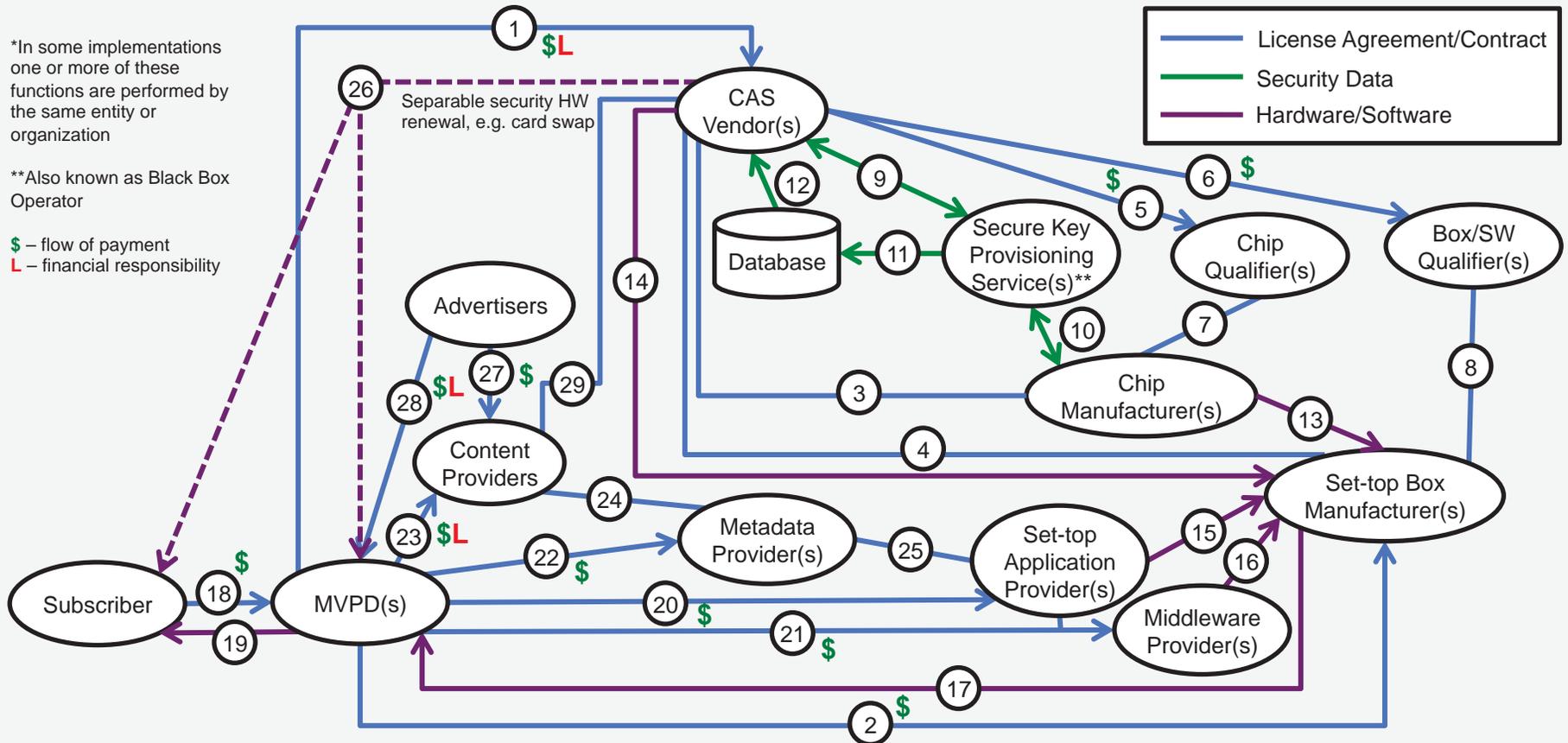
WG2 Report: <https://transition.fcc.gov/dstac/wg2-report-01-04212015.docx>

Diversity of MVPD DRM Solutions

- MVPDs deploy a variety of security solutions (DRM) for retail devices
- DRM is either embedded in MVPD's App or provided by platform
- DRMs use proprietary key (license) distribution systems

MVPD	DRM (retail devices)
Cable	<ul style="list-style-type: none">• PlayReady• Adobe• FairPlay• NDS VideoGuard Connect
Satellite	<ul style="list-style-type: none">• NDS VideoGuard Connect• Nagra
Telco	<ul style="list-style-type: none">• PlayReady• SecureMedia & PlayReady

Example MVPD CAS Trust Infrastructure*



*In some implementations one or more of these functions are performed by the same entity or organization

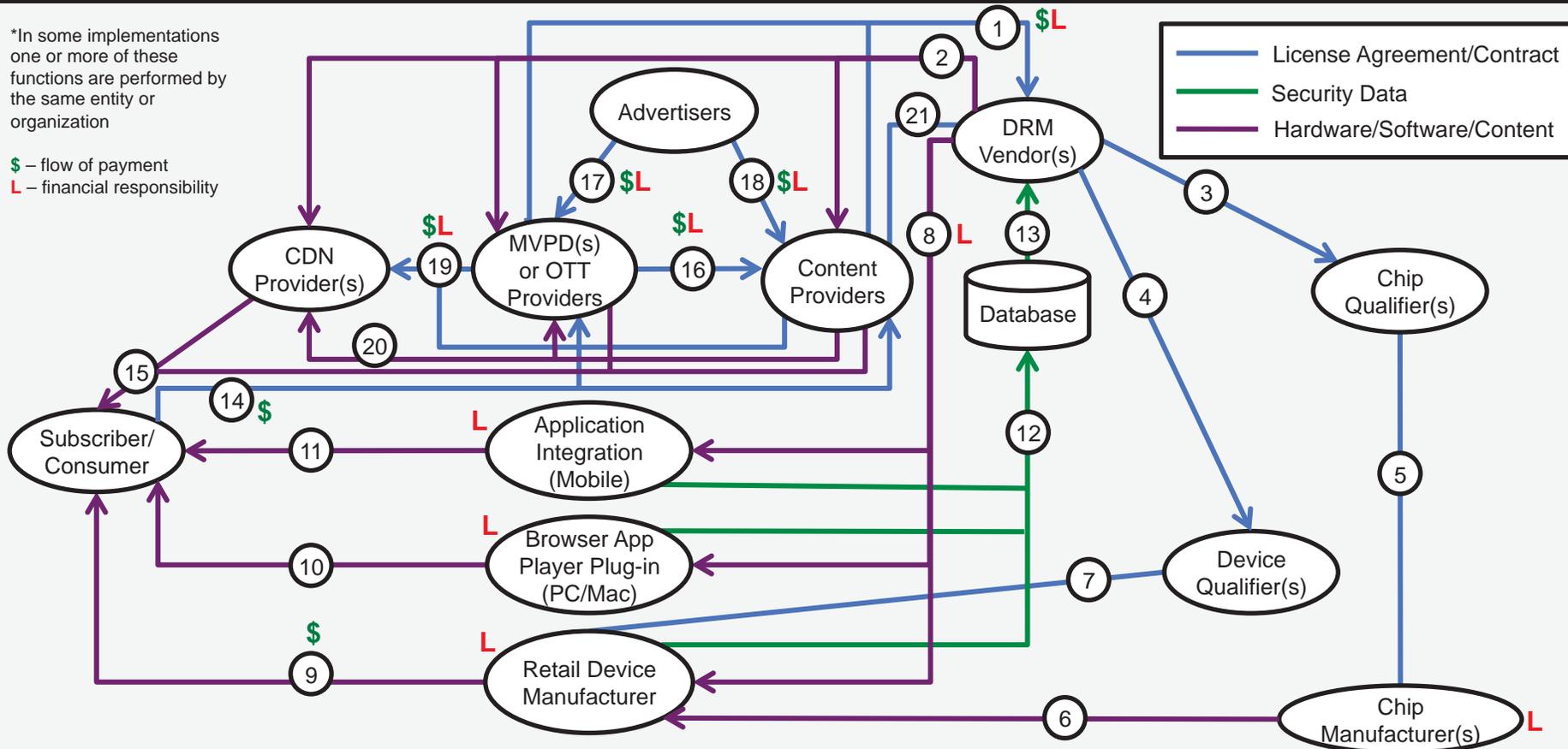
**Also known as Black Box Operator

\$ – flow of payment
L – financial responsibility

Example DRM Trust Infrastructure*

*In some implementations one or more of these functions are performed by the same entity or organization

\$ – flow of payment
L – financial responsibility

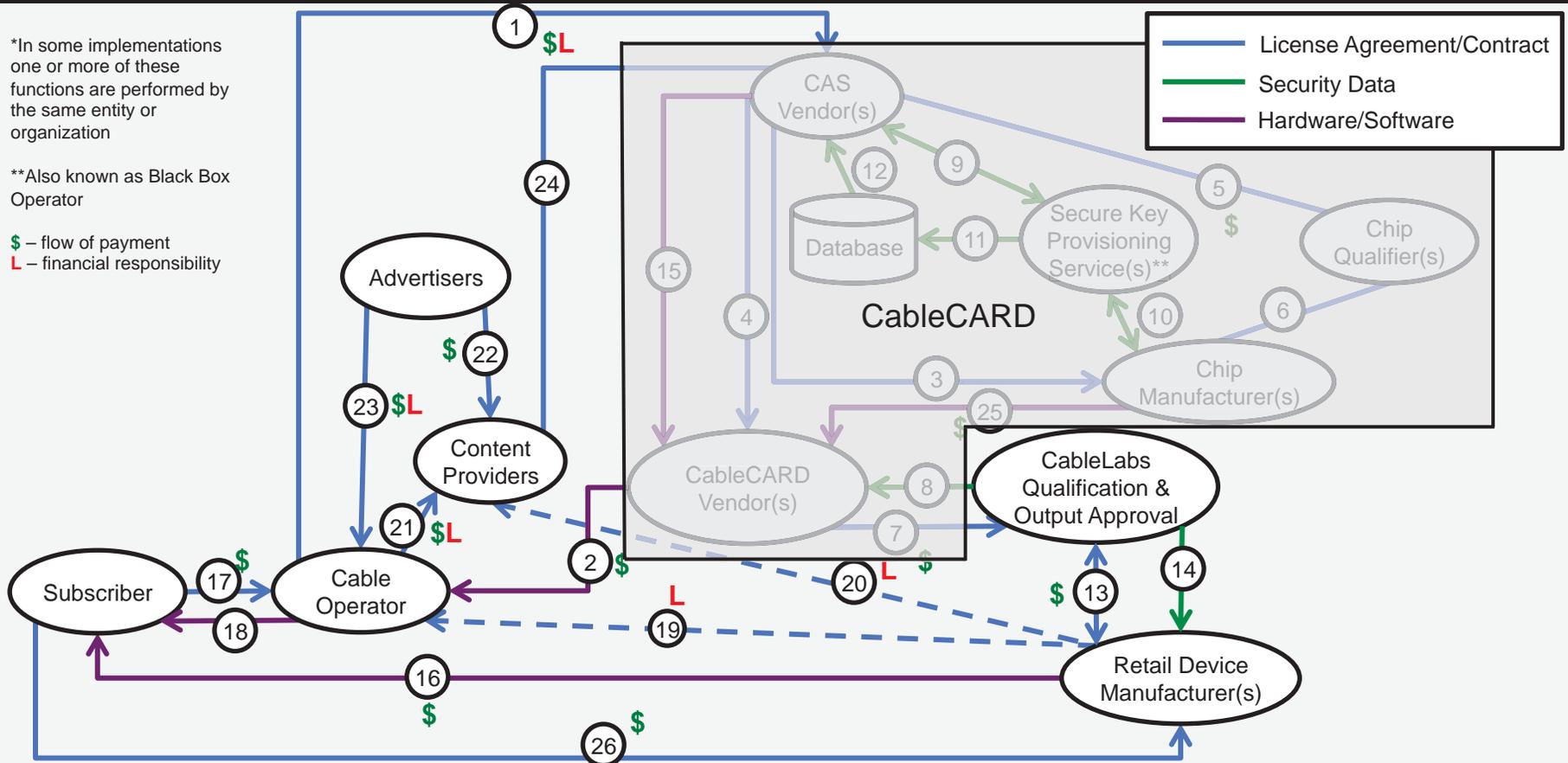


CableCARD System*

*In some implementations one or more of these functions are performed by the same entity or organization

**Also known as Black Box Operator

\$ – flow of payment
L – financial responsibility



DSTAC WG2 Backup Material

MVPD CAS & DRM

MVPD	CAS (MVPD set-top box)	CAS Core Cipher	DRM (retail devices)
Cable	<ul style="list-style-type: none"> • DigiCipher 2 • MediaCipher • PowerKey • NDS VideoGuard • Conax • Nagravision • OMS • BBT 	<ul style="list-style-type: none"> • DES-CBC • DES-CBC • DES-ECB • CSA • CSA • CSA • CSA/DES/AES • AES 	<ul style="list-style-type: none"> • PlayReady • Adobe • FairPlay • NDS VideoGuard Connect
Satellite	<ul style="list-style-type: none"> • NDS VideoGuard • Nagravision 	<ul style="list-style-type: none"> • DES/AES • CSA/DES/AES 	<ul style="list-style-type: none"> • NDS VideoGuard Connect • Nagra
Telco	<ul style="list-style-type: none"> • Mediaroom DRM • MediaCipher & PowerKey 	<ul style="list-style-type: none"> • AES • CSA 	<ul style="list-style-type: none"> • PlayReady • SecureMedia & PlayReady

MVPD Network Technologies



MVPD	Physical Layer	Modulation/Transport	Control Channel	Video Codec
Cable	HFC RFoG	QAM/MPEG-2 TS	SCTE-55-1 only SCTE-55-1/DOCSIS-DSG SCTE-55-2/DOCSIS-DSG In-Band DOCSIS only	MPEG-2 only MPEG-2 & AVC
Satellite	Ku BSS Ku FSS Ka FSS Terrestrial Off-air	QPSK/DSS TS, DVB-S2/MPEG-2 TS QPSK, 8-PSK Turbo/MPEG-2 TS 8-VSB/MPEG-2 TS	In-Band In-Band N/A	MPEG-2 only MPEG-2 & AVC MPEG-2 only
Telco	Twisted Pair (VDSL) FTTP (B/GPON)	Multicast & Unicast-IP QAM/MPEG-2 TS & Unicast-IP/ATM AAL5	IP/VDSL & IP/FTTP SCTE-55-1/SCTE-55-2 & IP	AVC only MPEG-2 & AVC

MVPD Customer Premise Equipment (CPE)



MVPD	Network Interface	Customer Premise Equipment (CPE)	In-Home Distribution
Cable	Coax & RFoG Optical Network Termination (ONT)	DVR & Non-DVR set-tops	Cable RF & MoCA
Satellite	Out Door Unit (ODU) – Satellite Dish Low noise block down-converter (LNB) Multi-switch (RF switching unit)	Genie Server (DVR) & Genie Mini clients Hopper (DVR) & Joey clients	802.11 & MoCA MoCA
Telco	VDSL Modem or Gateway B/GPON Optical Network Termination (ONT)	DVR & Non-DVR IPTV set-tops	802.11 Cable RF & MoCA

MVPD Retail Device Support

MVPD	Mobile Apps	TVE	PC (Windows/Mac OS X)	Other Retail Device Support
Comcast	✓	✓	Flash Browser Plug-in	Samsung TV, Xbox 360
DirecTV	✓	✓	Flash Browser Plug-in Cisco/NDS VG Connect DRM	Samsung TV, Sony TV, Toshiba TV, & LG TV with RVU NFL Season Ticket – PlayStation 3 & 4, Xbox 360 & One
DISH	✓	✓	DishWorld Application	LG TV Virtual Joey
TWC	✓	✓	Flash Browser Plug-in	Samsung TV, Xbox 360, Roku
AT&T U-verse	✓	✓	Flash & Silverlight Browser Plug-in	
Verizon	✓	✓	Flash Browser Plug-in	Samsung TV, LG TV, Xbox 360
Charter	✓	✓	Cisco Browser Plug-in	
Cox	✓	✓	Cox TV Connect Application	
Cablevision	✓	✓	Optimum Application	

Estimated Downloads of MVPD Mobile TV Apps*

CableLabs®

Mobile App	Android	iPhone	iPad	Total
DirecTV	10,000,000	6,100,000	2,700,000	18,800,000
Xfinity TV Go	5,100,000	2,300,000	1,400,000	8,800,000
DISH Anywhere	5,200,000	1,800,000	1,700,000	8,700,000
AT&T U-Verse	2,200,000	2,400,000	1,600	4,601,600
TWC TV	2,300,000	882,000	788,000	3,970,000
Verizon FiOS Mobile	1,200,000	756,000	729,000	2,685,000
Cablevision Optimum	508,000	617,000	607,000	1,732,000
Charter TV	510,000	147,000	89,000	746,000
Bright House TV	268,000	256,000	184,000	708,000
Cox TV Connect	146,000	80,000	366,000	592,000
Total	27,626,000	15,357,000	8,573,400	51,556,400

*Source: <http://xyo.net> (accessed 2/6/15)

PolyCipher Background

Prepared for DSTAC WG3

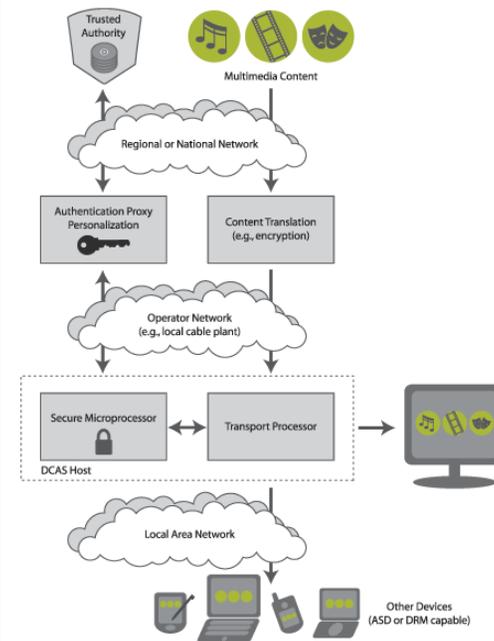
June 2, 2015

Presented by: Ralph W. Brown



- Cable industry JV (Comcast, TWC & Cox) to develop a new software downloadable CAS as a replacement for CableCARD (circa 2005-2009)
- Designed as unitary approach for two-way cable systems, not for one-way networks (different goal than DSTAC)
- Based on a mandated specific secure micro and a qualified transport processor and introduced a new key management infrastructure

PolyCipherSM Downloadable Conditional Access



A DCAS Host (a set-top box, TV set, or other compliant device) establishes its bona fides by contacting a trusted authority (a database of all authorized devices) via an authentication proxy.

Once authenticated, the DCAS host is personalized with the appropriate security client that will allow it to decrypt and display content transmitted over the cable network (typically, video & audio). Content can also be translated for use by ASD- or DRM-capable devices elsewhere on a local network.

- Diverse, competitive market of hardware-based content security solutions emerged
 - Massive investment required to invent new security solution from scratch; but other security solutions were emerging faster
 - Technology moved to diversity of target as opposed to the PolyCipher unitary approach
- Regulatory uncertainty
 - FCC denied the integration ban waiver for boxes that would have provided test bed