Response of Dish TV India Limited

to the

Pre-Consultation Paper dated April 04, 2016

on

Set Top Box Interoperability

Submitted by:

Ranjit Singh
e-mail: ranjitsingh@dishtv.in

Response of Dish TV India Limited to "Pre Consultation on Set Top Box Interoperability":

Introductory Comments

Dish TV welcomes the industry pre-consultation on STB interoperability since the present pre-consultation will enable the TRAI to understand the factual position in respect of the Technical Interoperability. We note that the TRAI has analyzed the prevailing scenario in the industry and noted the reasons why interoperability is not practical with current methodologies used.

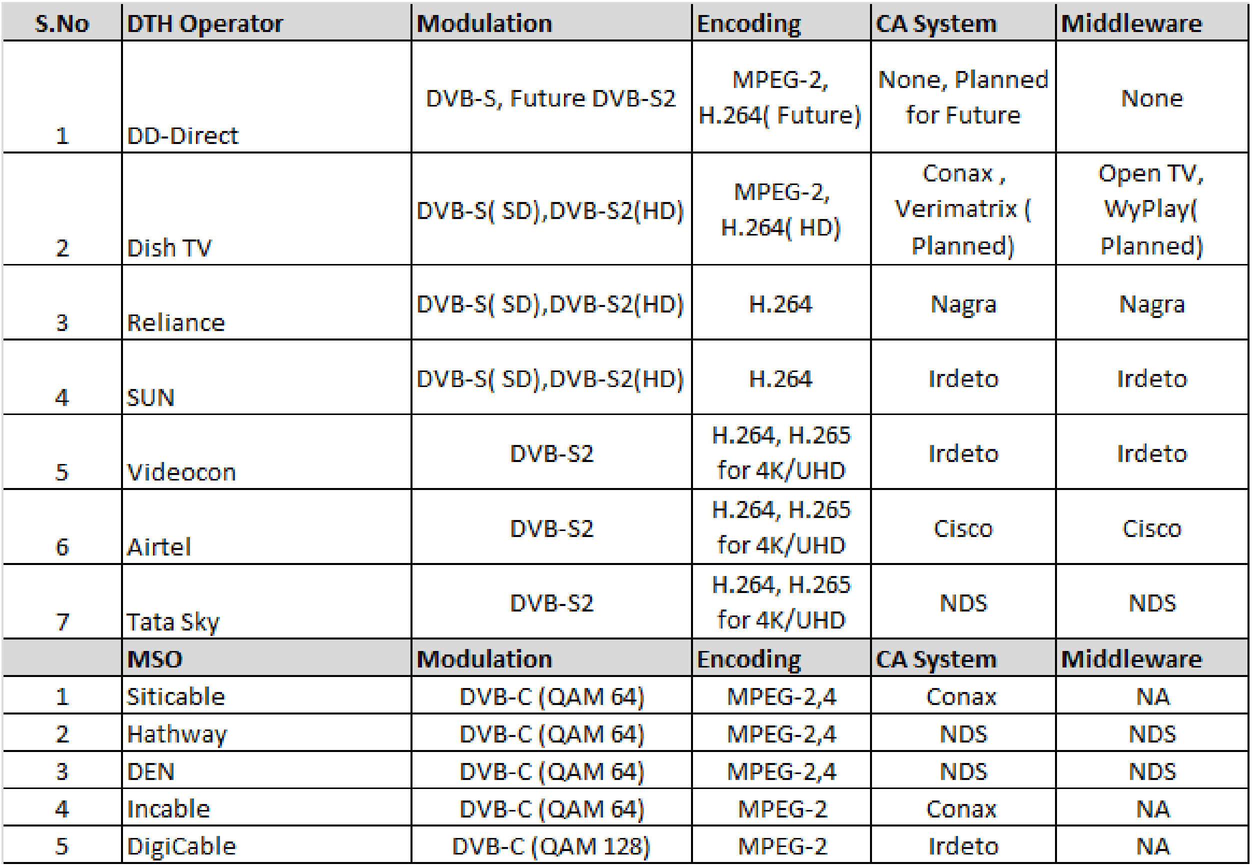
The prevailing methodology for adopting Interoperability in India was mandated to be a CI slot and availability of a CAM card which would have enabled a subscriber switching between two operators to switch the CAM module. However in practice this was not feasible due to the different standards of modulation and compression used, apart from the cost of CAM cards and the lack of suitable middleware which is essential for various features including EPG, on-demand services, and content management.

The status today remains the same, i.e. the DTH operators and MSOs in India use different compression, modulation, middleware and encryption systems. These are summarized below for DTH operators:

DD-Direct: MPEG-2, DVB-S (present), H.264 DVB-S2- Possible future additions
Dish TV: MPEG-2, DVB-S for SD, H.264 DVB-S2 for HD
Reliance, SUN: DVB-S, H.264 for SD; DVB-S2, H.264 for HD
Videocon, Airtel, T-Sky: DVB-S2, H.264, H.265 for 4K/UHD

In our introductory comments, we would like to analyze these points, before reverting to reply to the issues of consultation pointwise.

Moreover they also follow different CA systems (Conax, Nagra, NDS, Irdeto), and the complete table is as follows:



S.No	DTH Operator	Modulation	Encoding	CA System	Middleware
1	DD-Direct	DVB-S, Future DVB-S2	MPEG-2, H.264(Future)	None, Planned for Future	None
2	Dish TV	DVB-S(SD),DVB-S2(HD)	MPEG-2, H.264(HD)	Conax , Verimatrix (Planned)	Open TV, WyPlay(Planned)
3	Reliance	DVB-S(SD),DVB-S2(HD)	H.264	Nagra	Nagra
4	SUN	DVB-S(SD),DVB-S2(HD)	H.264	Irdeto	Irdeto
5	Videocon	DVB-S2	H.264, H.265 for 4K/UHD	Irdeto	Irdeto
6	Airtel	DVB-S2	H.264, H.265 for 4K/UHD	Cisco	Cisco
7	Tata Sky	DVB-S2	H.264, H.265 for 4K/UHD	NDS	NDS
	MSO	**Modulation**	**Encoding**	**CA System**	**Middleware**
1	Siticable	DVB-C (QAM 64)	MPEG-2,4	Conax	NA
2	Hathway	DVB-C (QAM 64)	MPEG-2,4	NDS	NDS
3	DEN	DVB-C (QAM 64)	MPEG-2,4	NDS	NDS
4	Incable	DVB-C (QAM 64)	MPEG-2	Conax	NA
5	DigiCable	DVB-C (QAM 128)	MPEG-2	Irdeto	NA

The TRAI has also analyzed in brief the Interoperability efforts in USA and Europe. In USA, initially the interoperability was sought to be achieved by mandating the use of Cablecards in each STB. However, as per data provided by TRAI, only 0.45 million Cablecards were sold as against 17.7 Million STBs proprietary to DTH and MSOs as of 2010.

As a matter of record, the last NCTA report to the FCC states, "**There have been over 617,000 CableCARDs deployed for use in retail devices** by **the nine largest incumbent cable operators. By contrast, those nine companies have more than 53,000,000 operator-supplied set-top boxes with** CableCARDs currently deployed." **This means that only approximately 1% of the CableCARDs deployed are for retail devices, the rest are deployed in cable operator-supplied set-top boxes".**

This implies that in order to meet the interoperability requirements of FCC, 53 Million Cable Cards, with a cost of $2.5 Billion were thrust on the subscribers, even though these subscribers used Cable operator supplied boxes and would not have required to pay $ 50 each extra just to meet the requirements of the regulator for the “Interoperability”. This shows that some notions of customer friendly nature conceived by regulators can in fact be counterproductive unless analyzed in proper context.

While interoperability is a desired objective, its practical implementation raises issues of :

-Cost to Customer for Interoperability in terms of royalties and STB cost
-Heightened risk of Piracy
-High operating costs for maintenance of Software stacks, New STB additions & repeated certifications from all vendors
While Dish TV responses to points under consultation are enclosed below, we would like to state that the solution to interoperability does not lie in a downloadable CAS system.

In the above backdrop, we provide our response to the issue for consultation as under:

ISSUES FOR CONSULTATION

Q i. In your opinion, what are the concerns that should be taken care of at the time of development of framework of interoperable of STBs?

The following issues need to be examined in relation to the use of STBs:

(i) STB features, and the costs (with and without STB interoperability),
(ii) Susceptibility to piracy
(iii) Operator provided features through middleware
(iv) Upgradations ,Replacement with future Chipsets and features.
(v) Maintenance and Management costs for Interoperable software structure

(i) STB Features, Costs and Interoperability

The types of STBs used in the DTH/ MSO networks in India are widely different in terms of their architecture and functionality. While some operators use DVB-S2, H.264 others are DVB-S, MPEG-2, and there are STBs with HD. UHD or 3D functionalities. The middleware used is different, and the Chipset, Memory Size (Flash & RAM) can vary over a wide range based on the use of active services and middleware planned.

The high end boxes of some operators would need to use advanced chipsets (measured in terms of DMIPS) and larger memory footprints.

On the other hand, the maximum sales are happening in the low cost segment such as Zing Boxes in Dish TV, and similarly with other operators, which have a subscription of Rs 99 Per month and are designed for just basic features with low cost STB architecture.
The prices of these boxes can range from Rs 800-Rs 2100 ($20), while the full feature STB can cost upwards of Rs 3500 ($50).

If there is an intention to use a downloadable or operator interoperable CAS, middleware and other components such as Key Ladder, Crypto firewall etc. the cost of the box will be on the higher end. **Consequently subscribers which could have been served with a low cost box will now need to buy a box at double the cost with the hope that in case, one day, if they change the operator, then it will somehow be able to download a new CAS and other software components in this high cost box**.

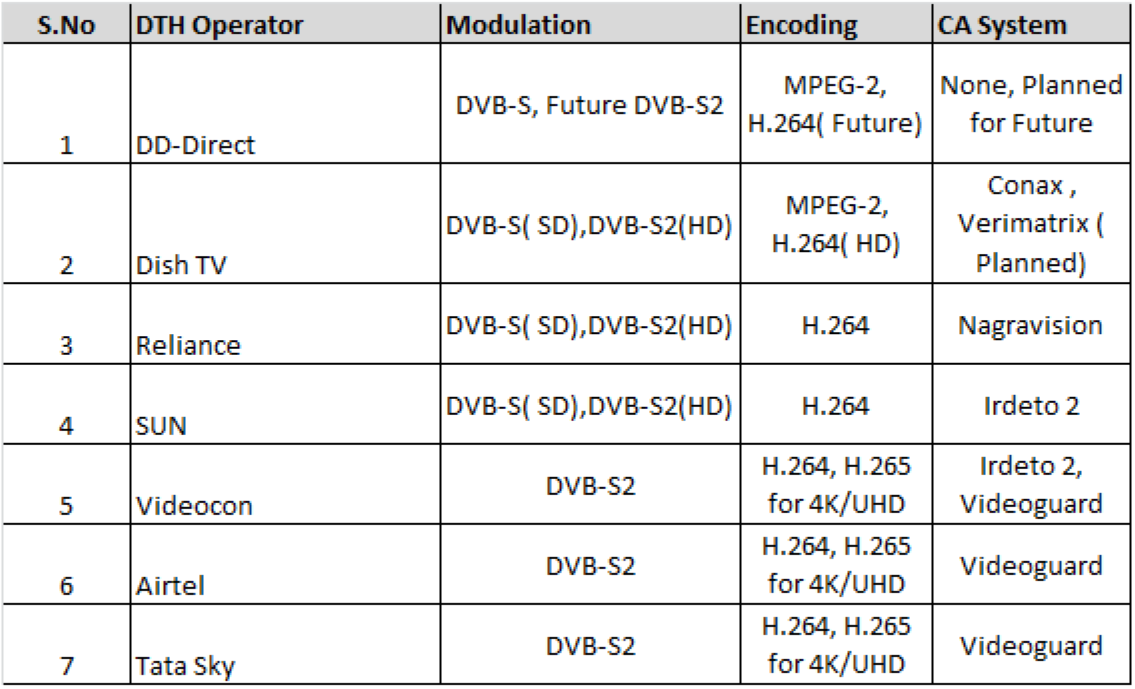
Instead the customer is better off in being able to buy a low cost box from the new operator, for which he may be paying less even if the boxes are not interchangeable.

The situation here is similar to the interoperable cableCard in USA where the interoperability was mandated at a high cost, but was rarely used and it inflicted very high cost ultimately borne by customers.

Placed below are the provisions which will need to be considered and appropriately implemented in all the STBs:

- **Specifications of Box which can meet All CAS+ All Middleware requirements**

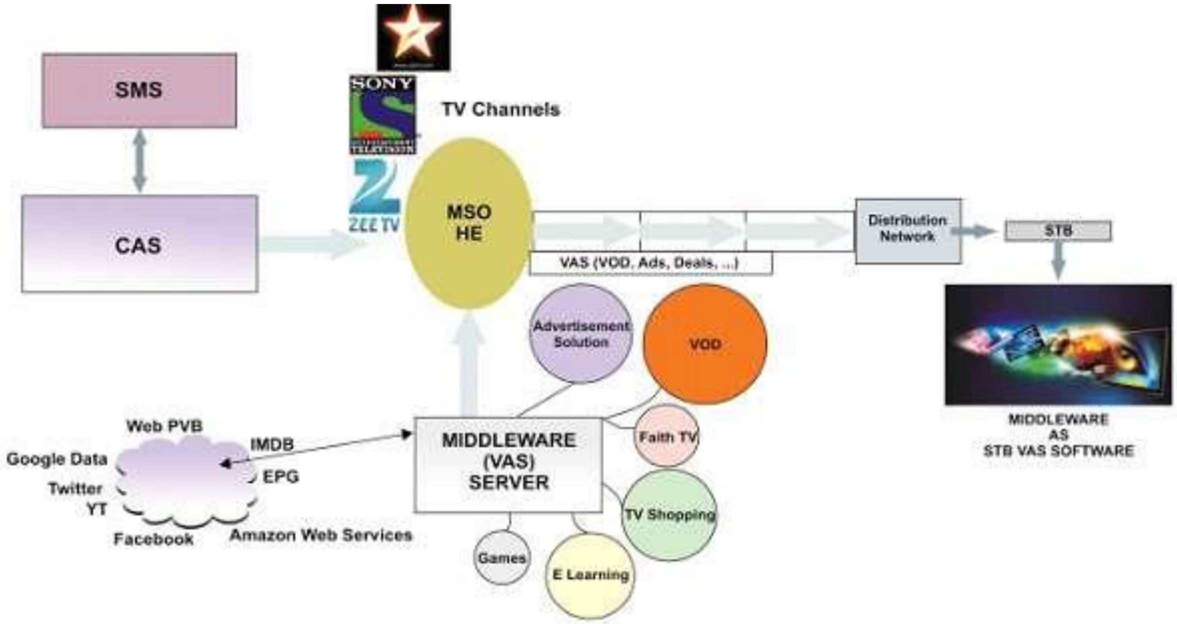
  As laid out in the table in our introductory comments, all the DTH vendors follow different CAS which currently include, or would have in near future Conax, Irdeto 2, Videoguard, Nagravision and Verimatrix.



S.No	DTH Operator	Modulation	Encoding	CA System
1	DD-Direct	DVB-S, Future DVB-S2	MPEG-2, H.264(Future)	None, Planned for Future
2	Dish TV	DVB-S(SD),DVB-S2(HD)	MPEG-2, H.264(HD)	Conax , Verimatrix (Planned)
3	Reliance	DVB-S(SD),DVB-S2(HD)	H.264	Nagravision
4	SUN	DVB-S(SD),DVB-S2(HD)	H.264	Irdeto 2
5	Videocon	DVB-S2	H.264, H.265 for 4K/UHD	Irdeto 2, Videoguard
6	Airtel	DVB-S2	H.264, H.265 for 4K/UHD	Videoguard
7	Tata Sky	DVB-S2	H.264, H.265 for 4K/UHD	Videoguard

Middleware

As cable TV digitization gains momentum, monetization through TV value-added services will grow exponentially. Middleware plays a crucial role in enabling those value added services apart from providing state of the art User experience for content navigation and search. This article puts forward implementation and operation support strategies for digital TV value-added services on a middleware platform in three aspects viz: Service Deployment, Service Recommendation, and Service Management & Control.



In order that a box be interoperable(amongst all operators of DTH today), it would need to be DVB-S2, H.264 with the highest memory map out of all the current systems, with down word compatibility so as to accommodate MPEG-2 and DVB-S transmissions from other operators. Such a box would therefore be of the highest possible cost ab-initio. Moreover it would be necessary that the middleware be downloadable, in the absence of which the user experience will be no different than using a CAM card which gave only encryption compatibility without middleware features.

In order that the growth path of STBs be adhered to the following are the minimum STB features which will need to be supported as an interchangeable CAS STB:

High Definition (HD) or H.264/H.265

- 2 Tuners (One tuner may work for non-recorder STBs)
- 500 GB HDD (for recorder STBs)
- DOCSIS 3.0 DSG modem (eCM) (for Cable Broadband STBs)
- OOB Tuner (may not be present)
- IR or RF4CE Interface
- CI-Interface
- 512 MB of Memory
- HDMI, Component, 1394 (optional), and RF outputs
- Two USB Ports, with compatibility for USB Modems

Optional: Home Networking (HN), gateways

STBs will need Fusemap of All CAs_ Multiple security Blocks & OTP

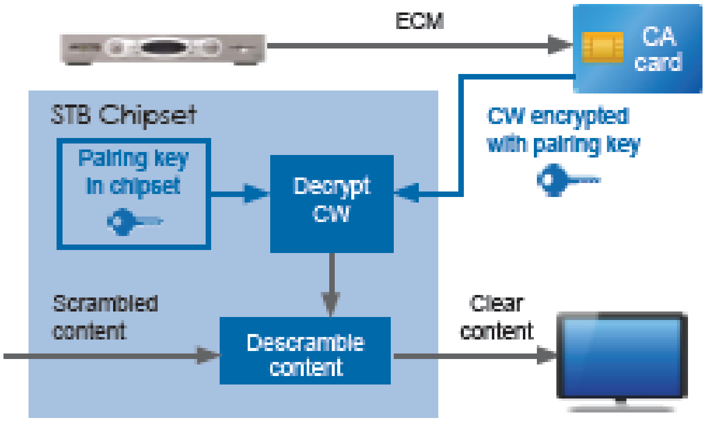
In order that the STBs will have a provision for a “downloadable CAS” i.e the customer could buy a STB and join a DTH / MSO operator network and ask the operator to download its CAS and middleware, it will be necessary at the manufacturing and design stage to have the core of each CA system fused on the Chipset SoC. In the absence of this, the manufacturers close out all the other fusemaps except the installed CA. This will also mean that a Royalty will need to be paid out to all the CA vendors for which the cores have been fused as a potential usage. Hence one time cost of the STBs will rise due to Royalty Payments to multiple CAS operators.

(ii) Susceptibility to Piracy

Piracy or breaking down the encryption is one of the key risks which an Operator faces in the provision of Pay TV services. The current methodology used in CA systems still requires the use of a Smart card which is paired with the STB. Advancing capabilities of attackers are now driving a new phase in Pay TV signal piracy as pairing keys and control words can be extracted from set-top box (STB) chipsets. These attacks defeat the current defenses against control word sharing and provide access to plaintext control words, enabling illegal access to premium content by non-subscribers. Solving the problem requires improved security in device chipsets, or System-on-Chips (SoCs), including strong hardware security cores.

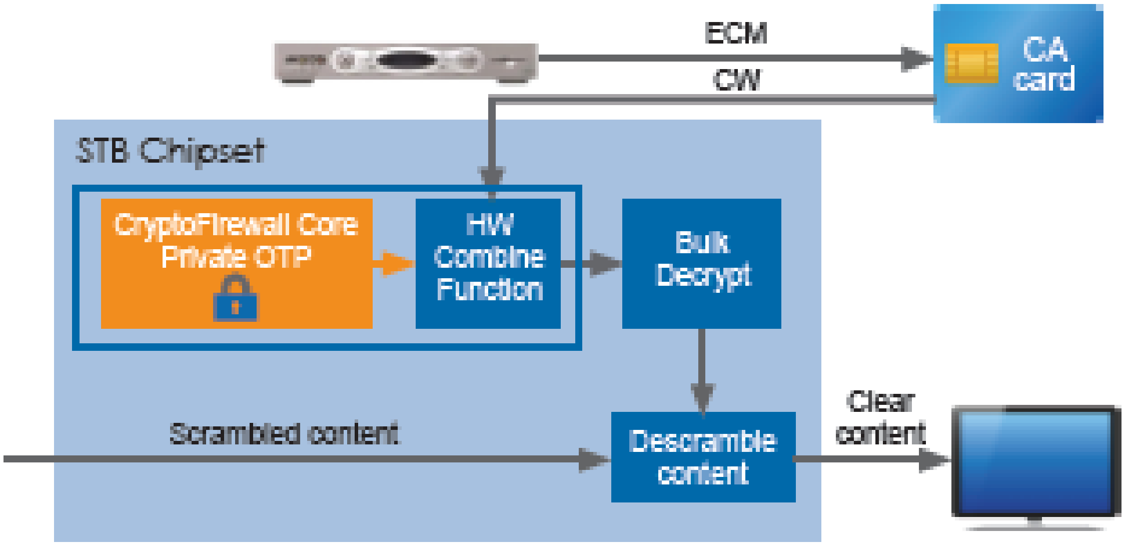
Sponsored Security Attacks by CA vendors:

Many of the attacks on the security of Paired Smart Cards were in fact sponsored by the CA vendors or their associates as this required the customers to continuously upgrade the CA version (Algorithms) and the Smart cards, at a huge cost. The Smart cards were vulnerable as the control words were transferred over an open interface between the smart card and the SoC. However the CA vendors had chosen not to change the methodology of embedding the smart card functions in the SoC till very recently.



Traditional control word encryption with a pairing key

This recent new measure is the **Crypto-Firewall security** wherein the video decryption functions are secured by a separate hardware core within the STB SoC. The Crypto-Firewall Maintains security even if the software and other cryptographic logic is compromised and provides complete key management with dedicated high-security root key storage. The crypto-firewall Supports all main distribution formats—satellite, cable, IPTV and OTT and integrates with leading CAS and DRM system providers and is available now from leading SoC manufacturers.



Secure content decryption with CryptoFirewall core

If an interchangeable CAS is an objective, it needs to be recognized that the risks of pairing key extraction (as well as other attacks) will reflect the weakest box. Such a box may not have a hardware secured security core**. In an interchangeable CAS environment, it will be a must to**

focus on providing a uniformly high level of security across STB models. This will imply giving a high priority to deploying STBs with strong hardware security, both in replacements as well as new deployments. This is specially important for new feature deployments (HD, 4K, 3D, etc.), to ensure that new, high-value features can use the better security. A possible solution for this will be a CryptoFirewall core which provides a separate hardware core within the SoC that manages keys independently from software and maintains security even if the remainder of the chipset is compromised. The CryptoFirewall core also offers complete key management, with a private bus for key delivery and extra logic for specific conditional access and DRM systems. Unlike traditional pairing key-based approaches, the CryptoFirewall core participates in the forming of the control word, effectively eliminating the vulnerability of control word interception from the smart card interface or software API and removing the need for pairing keys.

(Source: Cryptography.com/paytv)

Requirements of STBs in a Downloadable CAS Environment:

Complex & Multiple security Blocks

(a) Current Model: Currently all DTH operator's boxes are with one CAS with following SoC architecture. Here, CAS and SOC vendor deal with all security aspects and control STB accordingly.

In case of any security threat, CAS operator, SoC and Box vendor do all efforts eliminating ongoing piracy threats. Also in current model, CAS operator control the boot loader.

Pro:

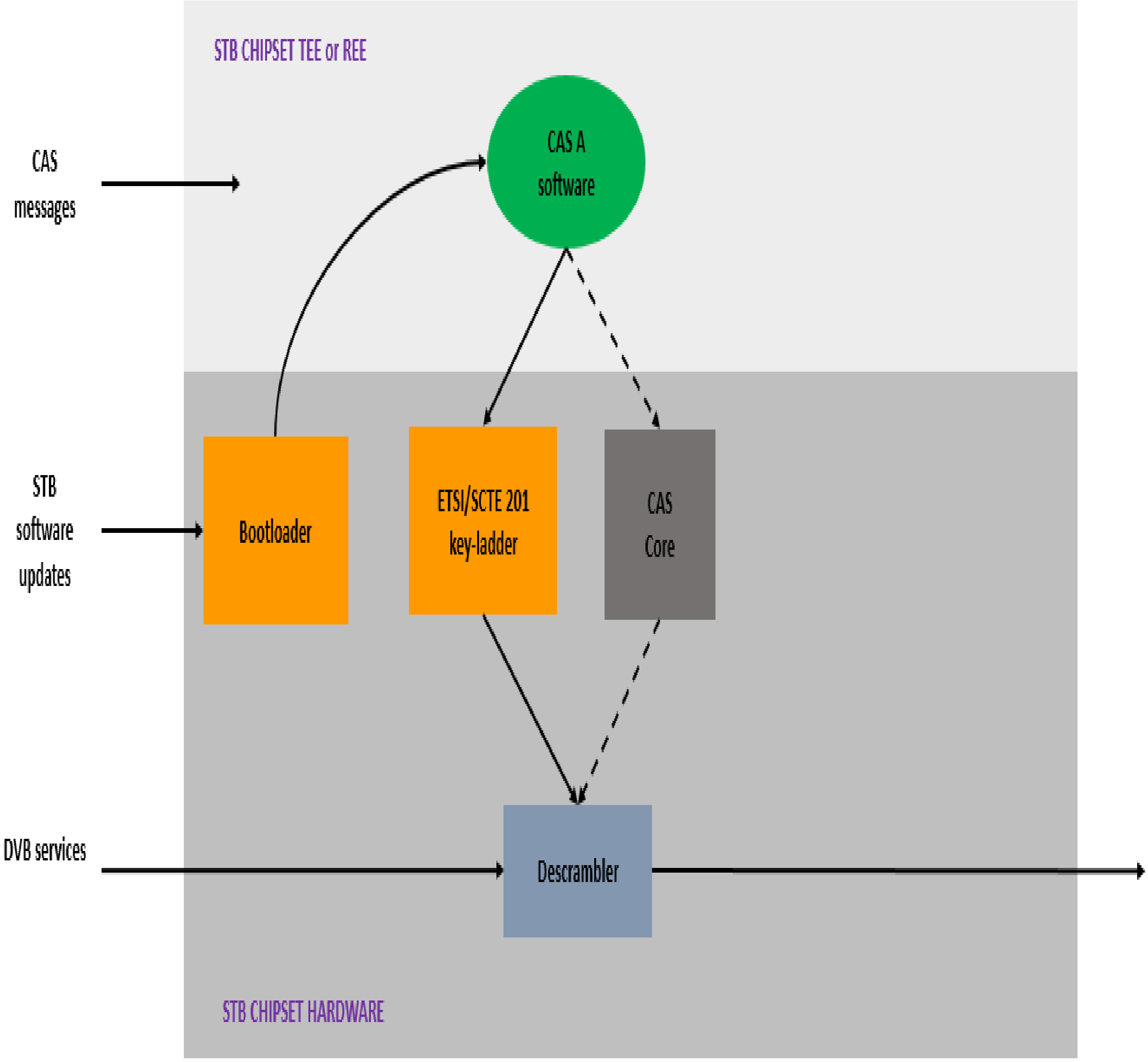
a. Most secure.
b. Only one CAS client license per SoC/BOX.
c. Low cost.

Cons:

a. No Interoperability within DTH operators.

Nevertheless, the low cost of STB, and higher security overcomes the disadvantage of non-interoperability.

Current DTH STB Model
(Only one CAS Client and their Core)



(b) In a Downloadable CAS Model (DCAS): **This new potential STB Model requires multiple CAS client licenses along with multiple security blocks to be enabled in advance on SoC for individuals CAS's Core.**

With new proposed model, common SoC is required to be very heavy and very high end to cater multiple CAS blocks and Key Ladders.

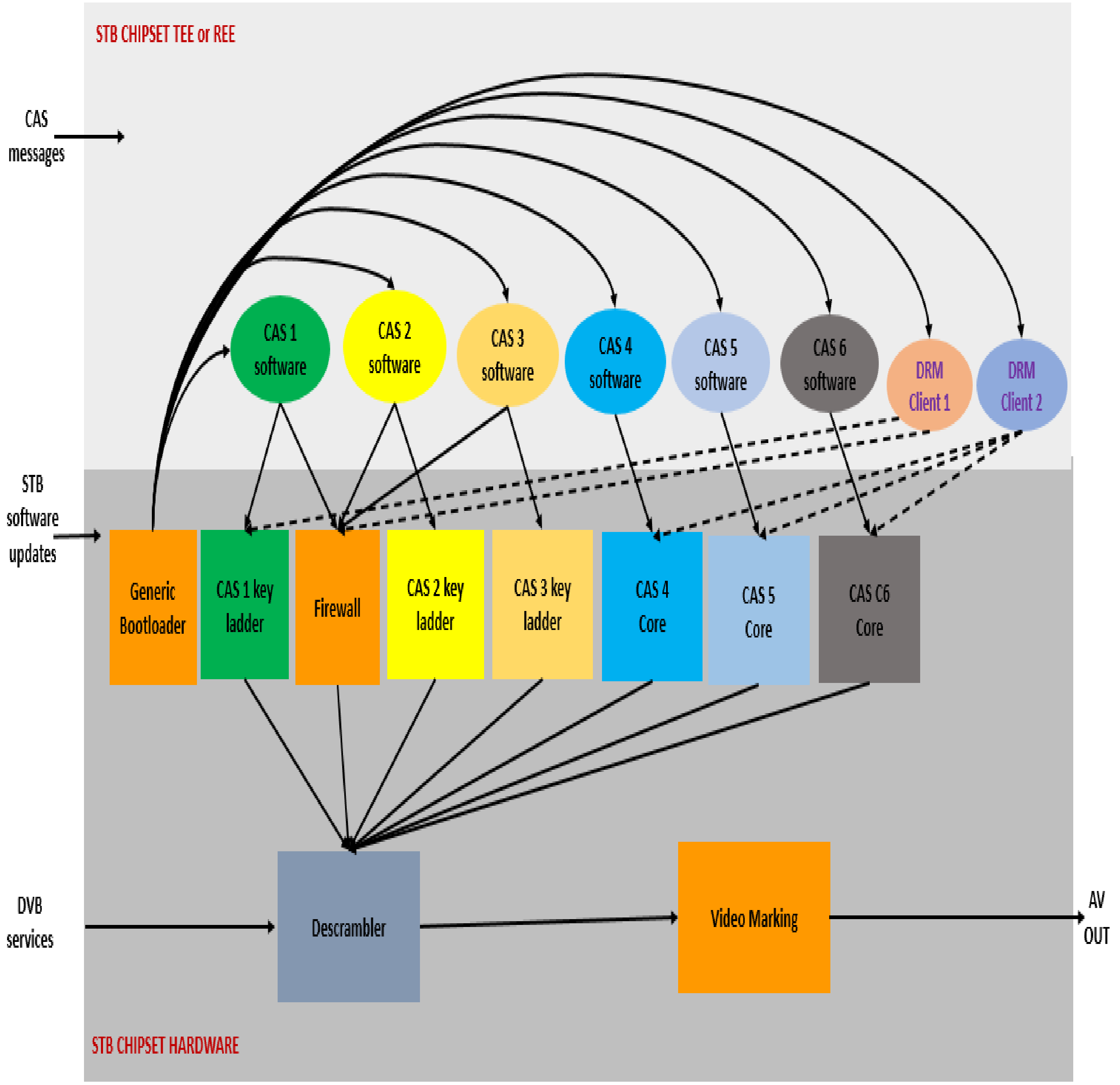
Pro:

a. Interoperability enabled.

Cons:

a. Boot loader will be very generic and no CAS operator will have control – Very high security threat.
b. SOC must be capable to cater all CAS Clients – to be certified by each CAS vendor.
c. SOC manufacturer has to pay certification cost to each CAS operators.
d. STB required to certify from each CAS vendor for their standard lib supports. STB vendors has to pay royalty to each CAS vendors.
e. STB vendors also has to get certification and NOC in advance from each DTH operators for their CAS, SMS and Middleware functionalities.
f. Similarly, when there any bug identify from any operator's signal then STB vendor need to fix the bug in accordance with respective CAS vendors and Middleware vendors. After bug fix, this STB again go to each DTH operators to test and certify. Chances are very high for new bug on third DTH operators and then this cycle keep on going for many months.
g. To support multiple CAS, SOC cost become very costly. This includes SoC cost itself (high end configuration chip) & Multiple CAS license fee.
h. In case of any security threat, it will be difficult to approach STB vendor or implement any bug fix without getting consent from all DTH operators. Hence OTA become very challengeable.
i. In case of piracy, broadcaster continue bleeding for very long period unless all DTH operator willing to upgrade box security.
j. One operator bug can be use with other operator's content and hence broadcaster forum continue in huge loss in terms of rampant piracy.
k. Piracy become easier because of very Generic boot loader.
l. Since some of DTH operators having return path and Hybrid box hence the same box must have DRM capability enabled from SoC as well as from STB vendor hence again cost will go higher side.

Common DTH STB Model
(Including all 6-CAS Clients and their Core)



Piracy Trends:

Today security is only dependent on the robustness of the STB: If the STB is secure, piracy can be prevented or blocked. If the STB is not secure, the smart card cannot block pirates who want to use it as basis for CW sharing piracy.

As we know, Smart cards were introduced in pay TV earlier for diverting attackers away from expensive STBs to devices that were cheaper and easier to replace. Pirates fetch the CWs they need for starting pirate operation from STBs.

Even though, currently Massive Piracy threat on STB where most of DTH operator's box compromised and hacked by hackers and extract Control Word from STB despite very tight security with securer boot loader environments.

Background to CW sharing piracy

CWs are the keys used to encrypt [or scramble] the actual content. In broadcast and multicast scenarios the signal goes simultaneously to all recipients who all need the same CW to decrypt [descramble] the content.

CW sharing piracy is to fetch CWs from a source of CWs, for example a hacked STB, upload them to a server, and arrange for pirate STBs to receive the CWs in real time from the server. The pirate STBs use the CWs to descramble the signal and provide unauthorized access to the service.

The CWs are typically delivered over the Internet. There are examples of CW delivery via satellite and mobile networks for areas with low Internet penetration. Pirates run the CW servers and make money by selling and upgrading pirate STBs. CW sharing piracy is now the dominant form of operator based piracy.

Pirates have risk reasons for attacking STBs

To get consumers to buy pirate STBs, pirates need to gain a reputation for reliable service. This means that pirates must secure steady sources of CWs. STBs have usually provided pirates with the easiest accessible CW sources so far. This as most operators have one or more generations of STBs that either receive CWs in the clear from the smart cards or are not well prepared for hacker attacks.

If pirates first can get CWs out of one STB, they can usually get CWs out of other STBs of the same type. So to block a STB CW source, the operator will normally have to replace one or more full generations of STBs. Operators are usually financially or logistically unable or unwilling to replace STBs especially if they were planned to last much longer or if the STB generation in question has been deployed in large volumes.

Consequently, if a pirate is able to obtain a source of CWs from operator STBs, then the basis is usually in place for running a reliable pirate operation for several years. This lowers risk and provides the pirate with a more solid basis for expanding the pirate operation.

Above is true scenario, even though every individual CAS implementing all kinds of efforts to protect the content unfortunately still rampant piracy continue just because of poor STB security or laps in hardware security time to time and hence piracy continue and broadcaster and operator continue in heavy loss.

Current focus to prevent operator piracy

The current security challenge is to improve the security level of the STBs. Today advanced STB SoCs support security aspects like:

a. Hardware protection techniques similar to those used in smart cards for protection of descramblers and CW management,
b. Dedicated security CPUs and hardware security cores/root-of-trust that protect key processing, rights processing and access decisions, and that are tightly integrated with CW management,
c. The option of splitting the CW into several CW contributions that are sent separately to the STB, processed by different functions and combined to form the CW eventually used for descrambling,

d. Marking of the outgoing content to assist blocking of unauthorized content redistribution,
e. Encryption of the outgoing content.

For SoCs that feature a hardware core/root-of-trust that can process rights and manage CWs, one can say that the smart card now has been moved inside the STB [SoC]. All these, required to enhance SoC capability with additional security in terms of Firewall or Core implementation from respective CAS operators.

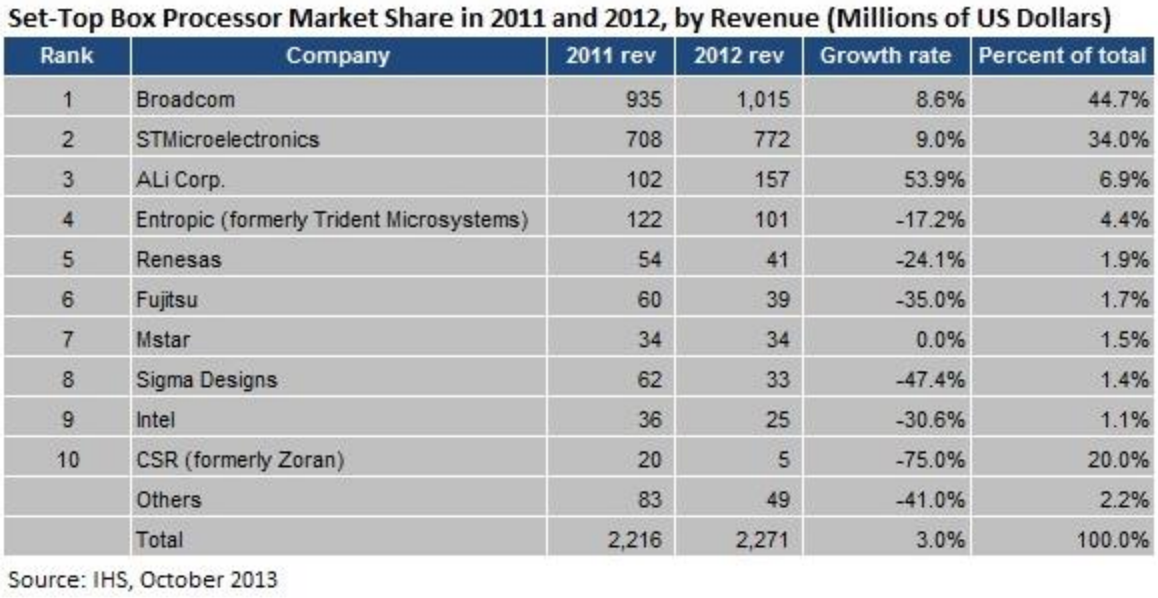
Q ii. What are the techno-commercial reasons for non-interoperability of STBs other than those mentioned above? Please provide reasons with full details.

Maintaining interoperable STBs across different operators would be a complex process. The following are the reasons:

(i) Chipsets frequently undergo upgradation or replacement

The Chipsets used in STBs undergo frequent changes, which have to be managed by the operator. Many of the Chipsets are phased out and new ones with better performance introduced due to the requirements of the operator, prices of Chipsets by new operators, changes in STB design or introduction of new features.

Each Chipset change requires the Operator to go through the entire cycle of porting of CA, certification by CA vendor, porting of middleware, field testing and hardening of STBs etc. **While this may be manageable in a single vendor requirement, the same cannot be managed in a multi-operator environment.**



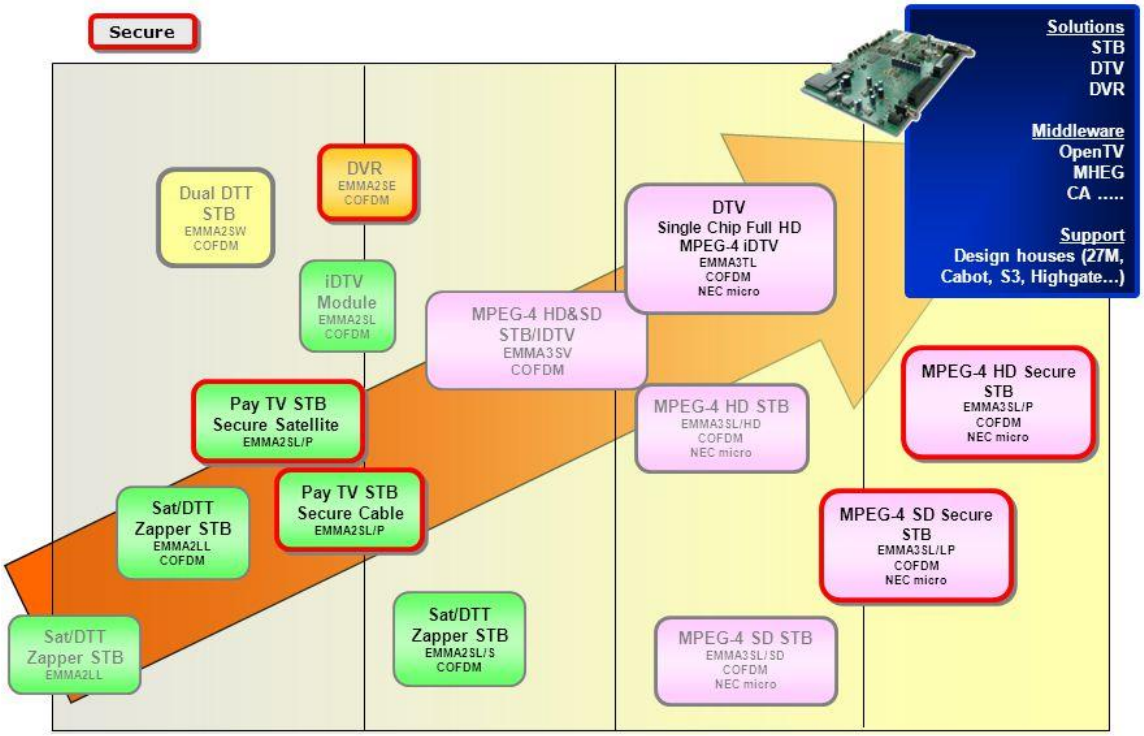
Set-Top Box Processor Market Share in 2011 and 2012, by Revenue (Millions of US Dollars)

Rank	Company	2011 rev	2012 rev	Growth rate	Percent of total
1	Broadcom	935	1,015	8.6%	44.7%
2	STMicroelectronics	708	772	9.0%	34.0%
3	ALi Corp.	102	157	53.9%	6.9%
4	Entropic (formerly Trident Microsystems)	122	101	-17.2%	4.4%
5	Renesas	54	41	-24.1%	1.9%
6	Fujitsu	60	39	-35.0%	1.7%
7	Mstar	34	34	0.0%	1.5%
8	Sigma Designs	62	33	-47.4%	1.4%
9	Intel	36	25	-30.6%	1.1%
10	CSR (formerly Zoran)	20	5	-75.0%	20.0%
	Others	83	49	-41.0%	2.2%
	Total	2,216	2,271	3.0%	100.0%

Source: IHS, October 2013

As an example, the table above shows Broadcom and STMicro as the top two vendors- having 44.7% and 34% market share respectively (total market share 78.7%). However, STMicro has now exited the STB business and Ali, Mstar have emerged the new vendors with new chipsets.

Hardware Reference Design (SoC + Tuner/Demod)

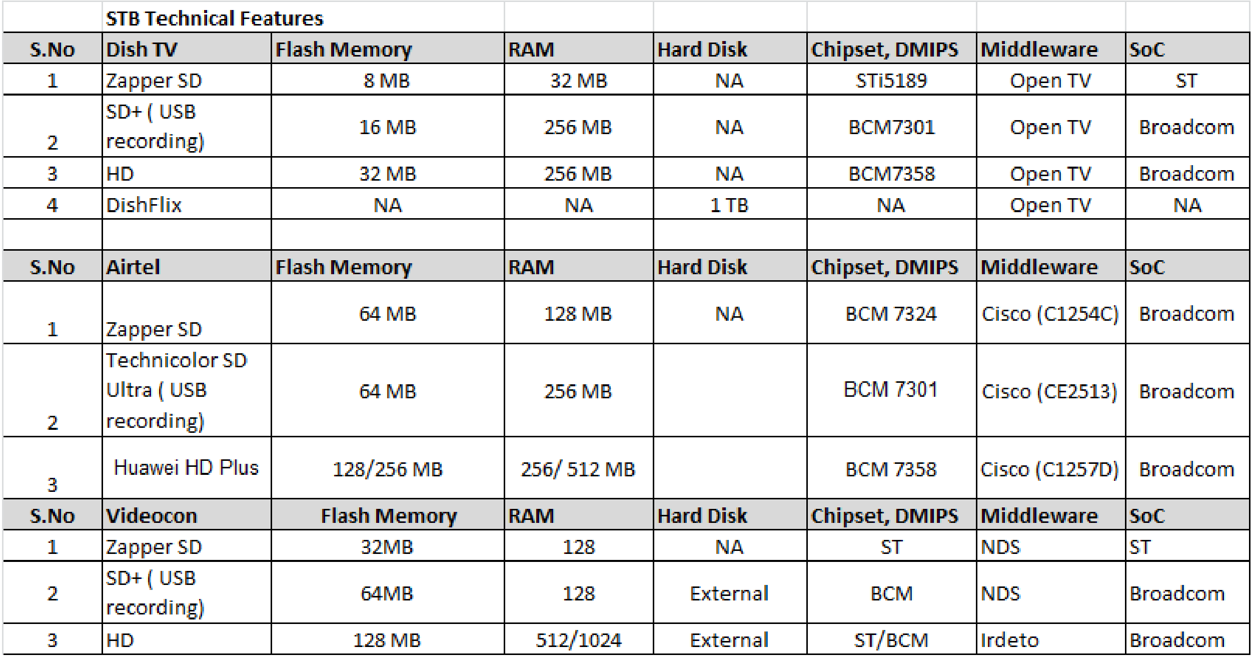

Secure
Dual DTT STB EMMA2SW COFDM
DVR EMMA2SE COFDM
iDTV Module EMMA2SL COFDM
Pay TV STB Secure Satellite EMMA2SL/P
Sat/DTT Zapper STB EMMA2LL COFDM
Pay TV STB Secure Cable EMMA2SL/P
Sat/DTT Zapper STB EMMA2LL
Sat/DTT Zapper STB EMMA2SL/S COFDM
MPEG-4 HD&SD STB/IDTV EMMA3SV COFDM
DTV Single Chip Full HD MPEG-4 iDTV EMMA3TL COFDM NEC micro
MPEG-4 HD STB EMMA3SL/HD COFDM NEC micro
MPEG-4 SD STB EMMA3SL/SD COFDM NEC micro
MPEG-4 HD Secure STB EMMA3SL/P COFDM NEC micro
MPEG-4 SD Secure STB EMMA3SL/LP COFDM NEC micro
Solutions
STB
DTV
DVR
Middleware
OpenTV
MHEG
CA .....
Support
Design houses (27M, Cabot, S3, Highgate...)

As new vendors of STBs enter with new chipsets, there is a complete cycle of testing and certification with each of the components of middleware, bootloader, CA system, Crypto-firewall supplier, Key-ladder supplier and STB vendor.

(ii) Multiple Levels of Complexity in STBs

STBs from various vendors have multiple STB types to cater to SD, SD with recording, HD, HD-PVR, UHD, Hybrid and connected STBs. These use different chipsets for each operator and are also use chipsets with different capabilities.

Enclosed is the sample data for some DTH Operators:



	STB Technical Features						
S.No	Dish TV	Flash Memory	RAM	Hard Disk	Chipset, DMIPS	Middleware	SoC
1	Zapper SD	8 MB	32 MB	NA	STi5189	Open TV	ST
2	SD+ (USB recording)	16 MB	256 MB	NA	BCM7301	Open TV	Broadcom
3	HD	32 MB	256 MB	NA	BCM7358	Open TV	Broadcom
4	DishFlix	NA	NA	1 TB	NA	Open TV	NA
S.No	Airtel	Flash Memory	RAM	Hard Disk	Chipset, DMIPS	Middleware	SoC
1	Zapper SD	64 MB	128 MB	NA	BCM 7324	Cisco (C1254C)	Broadcom
2	Technicolor SD Ultra (USB recording)	64 MB	256 MB		BCM 7301	Cisco (CE2513)	Broadcom
3	Huawei HD Plus	128/256 MB	256/ 512 MB		BCM 7358	Cisco (C1257D)	Broadcom
S.No	Videocon	Flash Memory	RAM	Hard Disk	Chipset, DMIPS	Middleware	SoC
1	Zapper SD	32MB	128	NA	ST	NDS	ST
2	SD+ (USB recording)	64MB	128	External	BCM	NDS	Broadcom
3	HD	128 MB	512/1024	External	ST/BCM	Irdeto	Broadcom

With multiple CA systems in operation, there will be a constant modification of firmware, SoC cores requiring certification cycles involving all vendors, if a common DCAS architecture is adopted. In practice, this will be too expansive to be practically manageable.

Comments on DCAS initiative in USA

Downloadable Conditional Access System or DCAS was a proposal advanced by CableLabs for secure software download of a specific Conditional Access client in to an STB or OCAP compatible device. The DCAS initiative also found support of the FCC and favorable regulatory view from the STELAR Reauthorization Act of 2014. FCC also appointed a Downloadable Security Technical Advisory Committee (DSTAC).The STELAR Act included a repeal of the set-top box security integration ban on cable operators, also known as the CableCARD mandate. (Under the CableCARD mandate, cable operators were not only required to supply CableCARDs to retail cable devices, such as TiVo DVRs, but they were also required to employ CableCARDs in all of their own set-tops, which increased cost and energy consumption, while adding no additional functionality or capability).

Subsequently the DCAS was implemented in some cable networks such as Charter Communications. However the DSTAC committee report which was released in 2015 did not view the implementations of DCAS as proposed in a favorable light.

The following are the extracts of the executive summary of recommendations:

(i) **"it would not be a step forward or economically viable** to require an environment in which a retail manufacturer would have to equip a device with RF tuners for cable and satellite, [and] varied semiconductor platforms, to support the dozen-plus proprietary CAS technologies that are currently in use."

(ii) "it is not reasonable to expect that all MVPDs will re-architect their networks in order to converge on a common solution."

(iii) Recognition "that the downloaded security components need to remain in the control of the MVPD

(iv) More and more retail devices are now based on Android, iOS, or other operating systems and are two way devices rather than being one way STB type devices.

Q iii. What are the plausible solutions for technical interoperability of STBs and their impact on the sector growth?

The technical interoperability of STBs, as elaborated in detail above is not likely to be in the interest of customers due to the high cost of implementation and maintenance of the system.

As the different operators use technologies such as H.264 or MPEG-2, DVB-S or DVB-S2 and different Middleware with widely varying memory footprint, only the highest level configured box i.e. H.265 DVB-S2 and with 1 GB RAM with a high DMips chipset is likely to be interoperable.

The prime concern will remain the threat of piracy where the leakage or extraction of the root key of any STB will compromise the entire system. Once the security is compromised, it will be logically possible to progressively hack all CA systems.

The cost of restoring such a system to equilibrium may be too high and the possibility of damage to the STBs due to large and heavy OTA software downloads will be unacceptable. A large number of STBs will turn to “Bricks” where they refuse to respond to any command. It is not possible for one or more DTH operators to set up repair shops to repair a STB which once belonging to a different operator has failed due to OTA process.

The sector growth will be impaired due to high cost STBs, cost of maintenance and issues in installation and commissioning of new STBs requiring one time download of entire software, if purchased from open market.

Q iv. Any other issue which you feel will be relevant for development of technical interoperability of the set top boxes.

It should be noted that while many of the examples cited in the consultation paper refer to interoperable CAS or DCAS in USA, these implementations initially targeted the Cable Networks, which are primarily 2-way in USA. This presents a conducible environment for two way communications during software upgrades and configuration, passing of keys and other functions.