Gospell Feedback

For India TRAI

"Consultation Paper On Interoperability of Set Top Box"

GOSPELL
TECHNOLOGY SERVES PEOPLE

GOSPELL Digital Technology Co., Ltd

Abbreviation

Abbreviations and Symbols	Description
CA	Conditional Access
CAID	Conditional Access ID, terminal ID
CAM	Conditional-access module
CAS	Conditional Access System
CI	Common Interface
CPE	Customer-premises equipment
CW	Control Word
DTH	Direct-to-Home
DTV	Digital television
DRM	Digital rights management
ECI	Embedded Common Interface
EMM	Entitlement Management Message
EPG	Electronic programming guide
ESCK	Encrypted Secret Chipset Key
IPTV	Internet Protocol television
LNB	Low Noise Block
NIM	Network Interface Module
SDK	Software development kit
SoC	System-on-Chip
STB	Set-Top Box
OTA	Over-the-Air
OTP	One Time Programmable

Table of Contents

Q1.

Question: In view of the implications of non-interoperability, is it desirable to have interoperability of STBs? Please provide reasoning for your comment.

Gospell Feedback:

We believe that the interoperability of STBs is necessary, and it is the development trend of the industry (whether it is a DTV or IPTV STB). In the long run, it can save capital investment and reduce e-waste. However, increasing the interoperability design may result in more complex set-top box hardware and increased cost. From a business perspective, only if it still has “surplus” after the favorable factors brought about by interoperability and such cost increasement offset each other, interoperable STB will be valuable.

Q2.

Question: Looking at the similar structure of STB in cable and DTH segment, with difference only in the channel modulation and frequency range, would it be desirable to have universal interoperability i.e. same STB to be usable on both DTH or Cable platform? Or should there be a policy/regulation to implement interoperability only within a platform, i.e. within the DTH network and within the Cable TV segment? Please provide your comment with detailed justifications.

Gospell Feedback:

At present, some NIM modules support the simultaneous reception of DTH and Cable signals (the driver can change the demodulation mode by some settings), but it is not popular because of cost. Moreover, because the DTH signal may require the set top box to provide the LNB feed output, this feed must also be added to the set top box used in the Cable network for compatibility. This will lead to a further increase in the cost of the set-top box. It is feasible if this is acceptable after evaluation of the cost increasement.

Q3.

Question: Should interoperable STBs be made available through open market only to exploit benefits of commoditization of the device? Please elaborate.

Gospell Feedback:

There are pros and cons for STB entering the open market. This involves not only technology and products, but also the after-sales service and the benefit of operators.

First, because of resource constraint, STB cannot be compatible with all network (signal reception, CAS, EPG, etc.) requirement. Therefore, if subscribers purchase STB from the open market, they must first update the software of the STB to the version of the network which they bought services from before STB can be used, which results in a lot of cumbersome upgrade and customization steps from the time the subscriber purchases the STB to the actual availability, thereby it makes the user experience of using the product poor and subscriber refuses to use. The original model, although lacking interoperability, STB is immediately available for subscribers after they buy the box home.

Second, when the STB becomes an open-market product, besides the service quality of the operator (including the number and quality of the program source) and the price, the factors considered by the subscriber when selecting the operator and the product will also include the cost and availability of the STB, etc. We originally hoped that the price of STBs for different operator networks would be similar, so that operators need to attract more subscribers by improving product quality and service level, and lowering price. At present, there are many operators who still is able to win lots of subscribers because the cost of the STB is low, although the quality of the program, network quality and service are relatively behindhand due to the limitation of construction cost. If it will cause cost increasement and disappearance of differentiation by STB interoperability design, these operators will gradually lose their living space. Therefore, it is also possible to form a market monopoly, which will harm the interest of consumers.

Q4.

Question: Do you think that introducing STB interoperability is necessary with a view to reduce environmental impact caused by e-waste generated by non-interoperability of STBs?

Gospell Feedback:

If the STB becomes a product in the pure consumer market, then it may also be like mobile phone. Subscribers may purchase new STB because of some new features, more processing capability, and even stylish appearance, thus making the original STB becomes electronic waste. Therefore, the problem must be viewed from two aspects.

Q5.

Question: Is non-interoperability of STBs proving to be a hindrance in perfect competition in distribution of broadcasting services? Give your comments with justification.

Gospell Feedback:

Yes, if the choice of the STB is rich enough to offset the impact of the STB cost increasement by STB interoperability. We believe that the final option is at the subscriber (if both custom STB and "universal" STB are allowed to exist on the market simultaneously).

Q6.

Question: How interoperability of STBs can be implemented in Indian markets in view of the discussion in Chapter III? Are there any software based solution(s) that can enable interoperability without compromising content security? If yes, please provide details.

Gospell Feedback:

We believe that all the STB interoperability solution in the CA/DRM proposed in Chapter 3 have certain problems. The cost of CI (including CI based on USB interface) is too high, and the cost of CAM module is not affordable to subscriber. ECI may be the most advanced solution, but the STB SoC that currently supports ECI is not very popular. The popularity of this technology also requires the following stages:

1) Each mainstream STB chip vendor recognizes and integrates ECI, and develops the corresponding low layer SDK;
2) All major CAS suppliers complete the CA function migration verification according to the ECI specification;
3) The construction of the ECI Trust Authority (TA) and the improvement of the system specifications;
4) Each set-top box manufacturer completes the development and mass production of CPE.

Even if we begin to do it now, it will take at least 2 to 3 years. We believe that the Indian market cannot wait for such a long time.

Software-based solution are more realistic.

We know that the key factor that causes CAS incompatibility is the difference between its algorithm and key for encrypting content and managing information. For a normal secure set-top box, these two major keys can be protected with software using white box technology. In addition, for the encryption and storage of the CA client data, the key security can also be realized by the white box technology, and the data is saved in the set top box Flash, so that it frees the smart card to form the pure software CA terminal. If the government authority can stipulate the uniform regulation on the storage method of the CA client data, the management and update of the white box key library of each CA provider, and the management and maintenance of the CAID, then at least at the application level of content decryption for the common security set-top box, it is possible to implement CA replacement by white box update method, thereby achieving interoperability (when changing CA, replace CA corresponding client CA software and white box in the SoC; and manage CAID in unified manner).

For advanced security STB, we believe that the decryption of management information (EMM) can still be achieved by white box technology, while for CW encryption, due to the need to descramble in Key Ladder mode, and ESCK is programmed in OTP space of SoC, so that it is not possible to achieve interoperability. However, if a new generation of advanced security SoC can permit ESCK multiple rewrite while other mechanisms remain

same, update key and CA by software are technically feasible. At this time, the encryption algorithm generated by ESCK can also be integrated into the CA client. When the CA needs to be replaced, after the CA client software is updated by the OTA, it runs its CAS ESCK generation algorithm, calculates the ESCK and writes it to SoC, then the CA client deletes the ESCK generation algorithm in software to ensure the security of its core key. This model can be achieved with a little improvement in the design of a new generation of advanced security SoC but a strong organization is needed to facilitate it.

Q7.

Question: Please comment on the timelines for the development of ecosystem to deploy interoperable STBs for your recommended/suggested solution.

Gospell Feedback:

The software of the CA client for common security STB can be completed within 6 months. The software of the advanced security STB CA client, if supported by the SoC vendor, is expected to be completed within 18~24 months.

Q8.

Question: Do you agree that software-based solutions to provide interoperability of STBs would be more efficient, reduce cost of STB, adaptable and easy to implement than the hardware-based solutions? If so, do you agree ETSI GS ECI 001 (01-06) standards can be adopted as an option for STB interoperability? Give your comments with reasons and justifications.

Gospell Feedback:

As mentioned earlier, we believe that the popularity of ECI standards may take some time; the most critical of these is that SoC vendors design chips and modify their SDKs according to ECI standards (this is a huge amount of work). In addition, the application of ECI will also lead to cost increasement of STB (virtual machine is very memory intensive), which is relatively unfavorable for the popularity of STBs in the cost-sensitive Indian market. Therefore, our company does not recommend the use of ECI (but if the authority forces the implementation, our company will also cooperate with product development).

We think the most suitable solution is in the reply of Q6.

Q9.

Question: Given that most of the STB interoperability solutions become feasible through a common agency defined as Trusted Authority, please suggest the structure of the Trusted Authority. Should the trusted authority be an Industry led body or a statutory agency to carry out the mandate? Provide detailed comments/ suggestion on the certification procedure?

Gospell Feedback:

We feel that this authority is more suitable as an industry entity. We have already expressed support for the software downloadable CAS solution in our reply for Q6. For this scenario, we recommend that the basic steps can be as follows.

1.Authority should establish a cloud service-based information management platform to manage the information of various stakeholders and related problems. Stakeholders include operators, CAS providers, SoC providers, set-top box manufacturers, and more.

2.The authority provides unified requirement for BootLoader and set-top box software upgrade, CA client software upgrade, terminal CAID rule, CA client data storage requirement, and CA client dynamic update requirement (including CA client online upgrade stream encapsulation format).

3.On the authority platform, record and maintain the information, including deployed network for each CAS vendor system, the deployed version in each network and internal serial number of the key system used in each CAS vendor; record and maintain the information, including STB manufacturers which can provide such STB product in the current market, its STB product model, the type of SoC, hardware configuration, etc.; record and maintain the CAS vendor's test record and final test report for the installation of its CAS client for each STB model; record and maintain CA terminal software for each STB type and each network, released by each CAS vendor (including white box, CA client, etc.).

4.Before the STB manufacturers finalize their hardware and software architecture, they need to obtain the verification of each CAS manufacturer that is active in the Indian market through authority. Since the systems deployed by different CAS vendors at different operators may use different versions and key systems, the same CAS may also require the STB to perform multiple CA library authentication for different versions of different operators. In order to reduce the workload of the CA library integration verification for the manufacturers, CAS vendors can provide their CAS client software uniformly for a series of STB chip platforms. These client software can be shared between different STB models and manufacturers (The premise is that they use the same SOC platform and are suitable for a certain CAS version of the CAS vendor.).

5.Authority evaluates the hardware specification and software framework architecture of a certain STB model of the STB manufacturer (including whether the design framework allows dynamic update of the CA client, etc.); the application information submitted by the STB manufacturer should include the SoC platform information (processor type, operating system, compilation environment, etc.). If the interoperability design requirements are met, the various CA clients (including the white box and the CA terminal runtime library) issued

by the CAS vendor for the platform can be obtained from the authority server.

6.Each operator should broadcast the CA client stream of each mainstream STB SoC platform for all CASs installed on its head-end at its main frequency. The CA client library included in these streams needs to be confirmed by the authority authentication uniformly. In addition, each operator's SMS should have an interface with the authority server; through this interface, the authority can delete an STB CAID from the operator's SMS (when the subscriber abandons the operator), or add a new CAID to SMS (when the subscriber switches to this operator). In addition, through this interface, the operator can inform the authority of the CAS provider and version in its system, as well as the main frequency, so that the authority can inform the subscriber in some way (for example, through the mobile communication network, see later).

7.If a STB sold in an open market is purchased by a subscriber for the first time, the store salesperson needs to write program for the STB according to the subscriber's needs. This program ensures that the operator and CAS system client selected by the subscriber are included. Note that the program mirror needs to be obtained from the authority website. The steps are: select the city, select the digital TV operator, select the CAS vendor and version recommended by the operator, and then download the program to the STB (USB upgrade is recommended). Then the salesperson fills in the STB card number (authority unified code), operator and CAS to authority website. The website informs the operator's SMS system of the STB information, so that the STB purchaser becomes a legitimate subscriber of the operator. The subscriber takes the STB home and accesses the operator's signal to obtain the activation and authorization command sent by the operator's SMS system through the selected CAS system, if he paid to the operator, and then can enjoy the services provided by the operator.

8.When changing the operator: The subscriber accesses the signal of the new operator and controls the STB to lock its main frequency point. The set-top box first downloads and installs the client library of the CAS running by the new operator; after installation, the new CA library will clear the data of the original CA library and initialize its own data. The subscriber then contacts the new operator, applies for activation, then pays the fee and obtains product authorization.

9.In order to make the above steps more automated and intelligent, authority can develop an APP that includes the function of controlling the CA switch of STB. The APP can obtain the STB serial number (and SoC platform) by scanning the QR code, and then communicate with the authority server to select the CAS recommended by the operator and the operator. After the selection is made, the authority can inform the subscriber whether the set-top box supports the selected operator through the APP. If it is supported, it can inform the main frequency that the set-top box needs to lock and search. Moreover, the APP can use the authority server to delete the subscriber's set-top box from the SMS system of the original operator and add to the SMS system of the new operator. This helps subscribers achieve flexible switching.

Q10.

Question: What precaution should be taken at planning stage to smoothly adopt solution for interoperability of STBs in Indian market? Do you envisage a need for trial run/pilot deployment? If so, kindly provide detailed comments.

Gospell Feedback:

See Q9's feedback. The key points are:

1) Specify the set-top box software framework, including white-box and card-free implementation of the CA client, set-top box serial number, card number encoding and storage specification, etc.
2) Interface between authority and various stakeholders (including after-sales service mechanism in the retail market, especially set-top box software control).
3) Determine the authority's operation management mode, funding solutions and other issues.

Q11.

Question: Interoperability is expected to commoditize STBs. Do you agree that introducing white label STB will create more competitions and enhance service offerings from operator? As such, in your opinion what cost reductions do you foresee by implementation of interoperability of STBs?

Gospell Feedback:

When Subscribers are unsatisfied after purchasing the services of a operator, they can apply to another operator by changing the software instead of changing the box, so it can definitely promote the operator to improve service and the cost-effectiveness of the product. The answer to the first question is yes.

In addition, when the set-top box becomes a common product, the storage, distribution, and after-sales service of the STB can be relatively centralized to be completed by the logistics industry or professional service providers, which does not need the operators to do these things themselves. In this way, each operator can greatly reduce the number and investment of after-sales service team, which can greatly reduce operation and maintenance cost, and can also improve service quality. At the same time, this can also promote the construction of a more intelligent after-sales service platform combined with mobile communication, thereby making the industry's overall service level higher and technology more advanced.

Q12.

Question: Is there any way by which interoperability of set-top box can be implemented for existing set top boxes also? Give your suggestions with justification including technical and commercial methodology?

Gospell Feedback:

This is possible but this requires a hardware up-gradation on all the existing deployments to the requirement of ECI. This certainly will be a logistics challenge as every box hardware has to be upgraded. Our suggestion shall be to allow new hardware on the common platform with interoperability and the phasing out of existing solutions can be done in a phased manner. Further details explained in Q6 & Q9.

Q13.

Question: Any other issues which you may like to raise related to interoperability of STBs

Gospell Feedback:
Most of the concerns have already been raised in the previous questions.