Comments on TRAI Consultation Note on Technical Architecture for Interoperable STB

IESA Digital Broadcast Core group consists of stake holders from all the segments of Broadcast value Chain. Our members have gone through the TRAI Inter-operability document and given their comments. The responses from IESA Broadcast Core group members are not uniform. The opinions varied widely depending on the broadcast stakeholder's position. Hence we are providing the feedbacks from all the stakeholders of IESA Broadcast core group below:

Summary:

Most of the members welcomed the move that has the potential to reduce E-Waste. STB manufacturers would follow operator's preference. SOC companies are awaiting consultation with CAS companies to ascertain feasibility of the concept, however SOC solutions only on CAS without addressing middleware diversity would not achieve inter operability. The availability of plethora of STB platforms does not allow inter operability just through CAS without standardizing the platform designs. CAS companies have provided detailed analysis of the concept. The concept note is based on Smart Card Based STB, while the market is moving rapidly towards card-less Conditional Access Systems, the concept note only addresses legacy systems and not emerging technologies. The concept still has the Control Word Sharing vulnerability. The concept note has not addressed Hack recovery aspect of the System, which is one of major concern for any unified security approach. The view of System Integrators are that the concept note is technically feasible, but in the present form it does not address problems of real networks, where systems have been deployed after various tweaks, it does not address the migration path of present deployment to new system. The Operators are concerned about increased cost of operation and security vulnerability in the proposed concept.

A. **STB Manufacturers** are of the view that if Operators accept it and CAS companies agrees on the approach, then they will have no other option but to follow.

B. **SOC companies** view is that at this stage details need to be looked into by CAS vendors for the CAS flow and especially the addition of a Trusted Authority (TA) that will assign authentication codes to OEM's and Operators.

   From SOC Company's perspective, they would need to look at supporting multiple CAS systems on selected chip families that will be used in India. Currently, few of the SOC's do support this, though it is limited to tie-ups with CAS companies and Operators who request this for specific designs. However, interoperability among them has not been yet studied by them.

   In addition of this, there is a immediate need to have detailed discussions with different CAS companies, Middleware vendors, Operators and OEMs for identifying feasibility of the architecture of such a system. These discussions must include the following

   - CAS companies need to resolve their issues with proposal, especially about security of the Control Word in the proposal.

- Currently Middleware is tightly tied to silicon architecture, and is not easily decoupled. For interoperability it is not clear how will this be ported across silicon vendors.
- STB architecture in terms of hardware specifications to satisfy basic Zappers/ PVR/ Hybrid /Android differs largely between silicon vendors. How interoperability would be achieved among them has not been addressed.

C. CAS Companies view

With the rapid shift by content providers, aggregators and end consumers to stream and consume premium services this opens the door to additional ways for un-authorized users to consume the high value content. It is evident with ever evolving techniques to circumvent stringent security measures implemented in various Conditional Access systems. The key strategies in mitigating such threats are:

1. Upgrade and Update the security of the system on timely manner – Actively & Proactively

2. Evolve to latest advancements in technologies based on the practical threat perception and value of the content

3. Introduce robust measures to trace back illegal content distribution sources

It is therefore only natural for pay-TV Conditional Access System providers to create an end to-end eco-system of trusted entities and thus maintaining close and secure integration of the CA components. However, this has led to creation of non-interoperable set-top-boxes.

From positive perspective, such non-inter-operability is ramification of greater benefits achieved by maintaining closed and secure end-to-end eco-system of trusted entities. Consultation note to achieve inter-operability among set-top-boxes strives to propose a protocol that can serve as common denominator for all Conditional Access System providers through using removable Smart Card based approach. It is a noted fact that market synergies are moving towards adopting SC less (a.k.a. Card-less) Conditional Access systems and key benefits with this fundamental shift are:

1. Better security through generational advancement in secure SOC technologies i.e. Trusted Execution Environment (TEE) capable chipsets

2. Reduced cost and e-waste that has been one of the key drivers for this initiative

3. Compliances to and mandate from Movie Labs™ security requirements for acquiring premium content.

Adoption to SC based system would defeat the above three core benefits and would impede the achievement of final goal of this initiative. With ongoing rapid developments in the field of SOC advancements w.r.t. security and functionalities, adopting SC would result in promoting legacy technologies that would not serve its purpose for very long in the field.

Points enumerated in section-2 of this document optimistically conveys grand total of the market synergies, upcoming technologies and security requirements from the content owners/aggregators across the world. Thus the feedback is towards achieving a comprehensive, robust and inter-operable set-top-box. System design enumerated in the consultation note meets the security requirements for low-resolution SD content only. In order to further raise and meet security requirements for protecting HD content, following must be factored in the proposal:

a. SOC (HW) based/anchored implementation of proposed protocol for protection of Content Keys and all data exchanged between SC<>STB.

b. If above is not feasible then the SW implementation of proposed protocol must be implemented in the TEE/SEE of the SOC with direct access to TEE/SEE exclusive descrambling registers from TEE.

c. Enhance the proposal to include provisions to enforce Secure Video Path (SVP) through TEE/SEE of the SOC.

Further, following topics that needs to be addressed beforehand formalizing and mandating the proposal:

I. There is no definition of a platform independent framework to address all filter scenarios of the different CA manufacturer's i.e. detailed design specification for "CA MESSAGE FILTER" block in Fig. 6 should be added in the proposal after addressing all CA manufacturer's needs.

II. "CA MESSAGE FILTER" block in Fig. 6 shall be platform independent such that each subsequent STB is supported seamlessly with one SC.

III. "CW Decrypt" block in Fig. 6 shall be defined in detail such that:

a. Requirement as mentioned in point 1(a) of this document is met

b. "CW Decrypt" block is platform independent

c. "CW Decrypt" block is CA independent.

d. "CW Decrypt" block is SOC independent so that multiple SOC is supported with one SC.

IV. Platform hardening rules (hardening of OS, drivers and other REE components) – which are (and may always be) CA vendor specific.

V. Process, ownership and control of secure boot loader of the STB and relevant signing keys.

VI. Process, ownership, integration and control of black box programming at chip manufacturer's and set top box manufacturers facility.

VII. Ownership, testing, validation and control of overall security implementation in STB. VIII. Countermeasures against various type known piracy threats like – STB cloning/emulation, EMM blocking, STB tempering etc.

IX. Process of generation, degree of randomization and ownership for private root keys.

X. Detailed definition of "Advanced crypto system; this layer of abstraction" and how it will interface with operator specific SC's.

XI. Detailed design on cycling of root certificates of set-top-boxes in case of compromise/hack.

XII. Blocking/black-listing of specific set-top-box model in the event of piracy.

The proposed architecture is not suitable to meet security requirements for protecting high value/premium content (HD, UHD, 4K) content and is only suitable for SD/low valued content.

Suggestion in 1(a), 1(b) and 1(c) of Section 2 must be implemented in order to raise the

- suitability of the proposed design to meet security requirements for premium content. It shall be mandatory for each STB/SOC manufacturer to have periodic security audit of

- their implementation through reputable, independent and trusted authority (TA) selected third party auditor. The protocol must allow CA vendors to implement independent, additional and proprietary

- (non-inter-operable) "SC less" CA technology alongside the proposed protocol. The protocol shall be extendable to support similar interoperability for Card-less CA technologies as well in future.

- Points (I) – (XII) must be addressed before formalizing and mandating such protocol

D. System Integrators View

1. Overall framework in the concept note for interoperability looks fine and technically quite feasible to implement and deploy

2. The framework does not address on how to bring already deployed STBs on to this framework. Without addressing this issue, every operation will have duplication of all activities and consequent cost.

3. In case deployed boxes are not getting moved onto the framework then the approach for migration needs to be defined.

4. Most of the operators in India have tweaked the TS (Transport Stream) from DVB standards in their implementation and deployment. However the concept Note Framework does not address flexibility in prevailing standards and in some cases, non-adherence to the standard/recommendations during implementation. This would be major hurdle of implementation of the concept in practice.

5. Introduction of a new entity like Trusted Authority will add overhead and may become a single point bottleneck.

6. In this Concept note framework how the revocation will be handled when there is an identification of hacking has not been addressed at all.

7. Framework does not address provisioning of Soft CAS.

8. Framework does not address leveraging of DRM approach for a connected box

9. There is no analysis on the cost implications for a transformation to this Framework

E. Operator's view

Following is operator's point of view purely from a business perspective.

1. If the system is implemented it has to be prospective considering the cost of sunk investment, Managing both legacy and new system would increase total cost of operation.

2. Operators have taken a lot of pain and time in selecting the CAS and Middleware, based on their business plans they have invested for the future and in some cases investors have also invested based on the same .What happens to such plans when the new system us implemented and all the basis for investment changes in midstream.

3. The country has been digitalised at great pain and cost to Operators, this concept if implemented would increase both for operators.

4. Who would be this trusted authority, who will have all the keys with them and what are the rules and regulations by which it will be governed.

5. What happens if this single system is HACKED on which the whole business of the operators are dependant. Can the entire industry take such a risk on a single entity? Who will be responsible if there is a Hack and who will compensate the Operators for loss of business.

6. The risk of having interoperability lends itself to larger risk (Operators by and large have subsidised STB to consumers), in this case someone with deep pockets can take over the whole industry by offering free STB' s etc.

7. There will also be several issues in terms of technology integration for all the CASes and sharing of keys together with cost of bandwidth or transponder cost etc., who will pick up this cost.

F. Scientific Society comments

1. Secure channel establishment is considered for confidentiality only. It is suggested to consider secured communication between Smart Card and STB.

2. Smart Card Data definition should be standardized.
    a. Mechanism of key storing and its retrieval mechanism need to be standardized
    b. Security aspect of smart card data and key store is not available.

3. Generation of nonce is not clear (True Random Number?)

4. Generation of UK(user key) is not there in the document

5. How the scheme would work for Card-less Set Top Box (Soft CAS based STB)

6. HACK Recovery is not considered in the document.

Ankan Biswas
Convener
Digital Broadcast Core Group

IESA™
INDIA ELECTRONICS & SEMICONDUCTOR ASSOCIATION
Taking India to ESDM Leadership