Verimatrix Response

To

TRAI Consultation note on

Technical Interoperable Set Top Box

Table of Contents

1 Executive Summary 1-3
2 Verimatrix Response 2-5
3 Summary 3-7
4 Verimatrix Contact 4-8

1 Executive Summary

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 system. The key strategy is mitigate such threats are:

1. Upgrade and Update the security of the system on timely manner – Actively and Pro-actively
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 released by TRAI 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. Cardless) 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 MovieLabs™ security requirements for acquiring premium content (click here for detailed specification)

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.

Furthermore, Verimatrix is pleased to provide generic feedback on this consultation note/proposal.

The 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.

2 Verimatrix Response

1. System design enumerated in the TRAI's 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.

3 Summary

- 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 Cardless CA technologies as well in future.
- Points (I) – (XII) must be addressed before formalizing and mandating such protocol

4 Verimatrix Contact

For further information, please write to:

Naveen Kumar
Head Sales & Market Development SAARC Nations

Email: nkumar@verimatrix.com
Address: Level 15, Concorde Towers,
UB City, 1 Vittal Mallya Road,
Bengaluru - 560001, INDIA
Tel: +91 -80-6759 0404
Mobile: +91-9886729394

Kamari S. Swami
Presales, APAC

Email: kswami@verimatrix.com
Address: Level 15, Concorde Towers,
UB City, 1 Vittal Mallya Road,
Bengaluru - 560001, INDIA
Tel: +91 - 80-6759 0404
Mobile: +91-9999 00 6862