TRAI
Shri Sunil Kumar Singhal
Advisor (B&CS)
Telecom Regulatory Authority of India

Our ref:	**Your ref:**	**Date:**
THK	Sunil Kumar Singhal	22.08.2017

Conax comments to “Consultation Note on Solution Architecture for Technical Interoperable Set Top Box”

Conax AS
Storgata 33B
P.O.Box 425 Sentrum
NO-0103 Oslo Norway

T: +47 22 40 52 00
Org.nr.: NO 963 580 207
www.conax.com

Introduction

The consultation note describes an interoperable solution based on a standardized STB platform and operator-specific CA implemented by use of smart cards. In general, the initiative is good and the principle described in the document seems suitable for the purpose.

Conax, being a leading provider of content security solutions for the TV industry, will focus on the security aspects of the described architecture. The comments outlined below are kept on a high level, but we are prepared to discuss more details in a face-to-face setting if required.

It is important to emphasize that an adequate security analysis of such protocol is a significant undertaking. The present walkthrough from Conax is merely our immediate impressions after reading it.

General comments

General comments to the proposed architecture:

- The architecture describes a very simple "zapper" type STB with main feature being linear TV with basic EPG. There is no mention of more advanced features such as PVR or hybrid OTT services. In a mature TV service such advanced features are now becoming commonplace and an expected part of the service. While it will still be possible to implement these features on operator specific configurations, Conax feels that the scope of the architecture should be broadened to at least cover such common services as the PVR. Note that in our experience interoperability is more complex when catering for such services.

- The Conditional Access is implemented using a replaceable CA smart card. This is a good approach as it enables security segmentation using different CA solutions and different key structures on a per-operator basis, at the same time as a standardized STB can be shared amongst operators. As the critical parts of the CA system resides in a low cost device such as the smart card makes it feasible to swap the CA if needed to reinstate the security of a pirated operation.

- The architecture apparently describes a proper solution for the registration process based on the One-Time Password. Using a combination of the smart card, the STB and a mobile phone already registered in the operator head-end seems to cater for the control of which devices are used in the field. The security protocol is based around standard PKI cryptography with a central Trusted Authority as the source of a hierarchy of trusted certificates. This is considered best practice for establishing secure communication between large quantities of devices.

- The protection of the Control Word inside the STB is weak. While the control word is properly protected using a unique session key during the transport from the smart card to the STB, the protection and use of the control word inside the STB is not optimal. The architecture describes a solution whereby the CW is decrypted using hardware implementation of AES with a session key that is provided through a hardware path to the AES decryption module. The resulted plaintext CW is then stored in RAM, and the software of the STB is responsible for feeding it into the descramblers of the SOC. While this solution will work, the only protection against illegal redistribution of the control words is the protection of the software environment. If an attacker is able to modify the software of the STB, he will also be able to extract the control words for illegal sharing. This could result in serious piracy affecting any operator using the compromised model of the STB. By experience, practical attacks will after relatively short time expose a CW stored in RAM.

Instead of a pure software handling of the control words, Conax recommends utilizing hardware based key ladders in the SOC ensuring the control words are kept encrypted all the way into the descrambler modules. This can be done using a Manufacturer Key Ladder (specific to each SOC vendor) or a standardized key ladder such as ETSI Key Ladders. Managing the provisioning of keys to the CA vendors should be handled by an independent Trusted Authority.

An alternative approach is to specify a hardware path from the AES HW decryption directly to the key table of the descrambler module. Few, if any, CA schemes are set up today without a protected key table.

- Secure boot is specified to be done using the STB manufacturer's signature keys. This places the responsibility for keeping the software environment intact on the STB manufacturer. In Conax experience, not all STB manufacturers are worthy of this trust. Some STB manufacturers are even known to have close ties with the pirate community. Conax recommends that the secure boot on the top level is handled using the signature keys of the Trusted Authority.

- The description of the EMM handling in the architecture is unclear. It is clearly recommended to using group addressing to optimize EMM delivery efficiency - which is also industry best practice. However, in the architecture it is specified that the EMM shall be encrypted using the Periodic Key 'PK' which is uniquely generated for each smart card as part of the registration process. This would imply that all EMMs need to be sent unique for each smart cards, which does not scale sufficiently for large MSOs.

  A modern CAS is typically using both unique EMMs and group EMMs to optimize delivery of various types of commands and entitlements to the smart cards. The architecture should support setting up CA filters in the STB for both types of messages.

  The use of a Periodic Key established as part of the registration process to further enhance the security of the EMM delivery is a good idea, but it needs at the same time to cater for the need to optimize EMM delivery by using the same EMM for a group of smart cards.

- Problems may occur, where the change of CA doesn't recover the security. For such case the current specification falls somewhat short. The note does not specify responsibility for the overall security of the STB, nor for the certification of the STB before introduction into the market. The note also does not specify maintenance responsibility of the STB manufacturer if there is need to correct bugs in the field. Finally, carrying out anti-piracy efforts in an environment with very fragmented security responsibility has also been proven to be very difficult and costly. These aspects are indeed complex to establish, but in Conax' experience entirely necessary parts of any security specification. The cost pressure for STBs today leads to corner-cutting and cheating in both design, test and production. Only clear responsibilities and a proper certification can defy that. The specification should describe the clear responsibilities of all parties, at least covering certification, maintenance and anti-piracy.

Closing remarks

Specifying an architecture for an interoperable Set-Top-Box is a very challenging exercise, and the proposed architecture is a very good step in the right direction. There are however still some security and responsibility issues that should be addressed before this architecture is put into action.

Conax remains positive to the initiative of the Interoperable Set-Top-Box, and confirms that we are still willing and eager to work with TRAI on defining the best possible architecture to make this happen.

Yours Sincerely
Conax

Tor Helge Kristiansen
EVP Principal Architect

Trond Solberg
Director Client Security & Anti-Piracy