Consultation Paper on KYC of DTH Set Top Boxes

SmarDTV Global Response

AUGUST 14, 2019

SMARDTV GLOBAL
ZI Athélia IV, 147 avenue du Jujubier13600 La Ciotat - France+33 442 838 000
info@smardtv.com

SmarDTV Global, a French high technology company, is a leader for secured devices for Pay-TV industry. Our products and technologies provide worldwide operators with secure, flexible, high quality solutions to help them to enlarge service offering by introducing customized view experiences. With a global presence all over the world, we are close to our customers to deliver tailored proposals and support.

SmarDTV Global has cumulated a strong knowledge of Digital TV experience based on more than 20 years of product development. Our portfolio covers more than one hundred products including Digital TV Set-Top Boxes, Conditional Access Modules and Professional & Hospitality solutions. Largest operators have already selected our solutions and currently, we deliver our products in more than 130 countries.
SmarDTV Global deploys millions of secure devices around the world every year and is working with Tier One global worldwide operators.

Joining forces with Neotion in August 2018, a well-established company providing innovative solution for Digital Television market, SmarDTV Global reinforces its position in the Pay-TV industry.

SmarDTV Global and Neotion become a worldwide leader for the Conditional Access Module (CAM). They bring an extended product portfolio including CAM, Set-Top Box and OTT solutions and a reinforced expertise in delivering accurate solutions for the Pay-TV market over the world.

We prepared a brief answer in response to the consultation paper on KYC of DTH Settopboxes to address few technical queries raised in KYC Consultation note dated 19/07/2019

1) Is there a need for KYC or e-KYC of DTH Set Top Boxes to address the concern raised by MIB in their letter mentioned in paragraph 1.5 of this consultation paper? Give your answer with justification.

   SmarDTV: Yes, we consider as important that a proof of identity is given by the subscriber whenever a STB and associated subscriptions is purchased, essentially for protecting honest people that their identity and more importantly their bank details are not used illegally for subscription to Pay-TV services. Also, we understand the KYC as a process that would discourage and track malicious people adversely using identity of DTH subscriber or misusing connection for wider range of people benefit or transferring STB across locations.

2) If your answer to Q1 is in the affirmative, then what process is to be followed?

   SmarDTV: We think that the current process as described in Annexure-II is good.

3) Whether one-time KYC is enough at the time of installation or verification is required to be done on periodic basis to ensure its actual

location? If yes, what should be the periodicity of such verification?

SmarDTV: We think that one-time KYC to be established and on periodic basis subscriber's location and subscriptions to be ensured. Such kind of periodic verification can be done quarterly or half yearly time frame. This should can also be alerted during payment cycle.

4) Whether KYC of the existing DTH STBs is also required to be done along with the new DTH STBs? If yes, how much time should be given for verifying the existing STBs for DTH?
SmarDTV: Once KYC to be established for already deployed and new settop deployment. Hence forth verification of location movement can be monitored. Per Unit verification and authentication can take about 1 hr approximately.

5) Whether the location-based services (LBS) needs to be incorporated in the DTH set top boxes to track its location? Will there be any cost implication? Give your response with supporting data and justification.

   SmarDTV: We think that LBS makes sense for tracking the smuggling of DTH STB outside of India (geo-fencing). However, we do see the value of accurately ensure that the honest subscriber is using the STB as the exact location that was registered at the time of subscription.

Geo-fencing can be incorporated into set top boxes without having to increase the cost. The solution we would like to propose is to mandate the DTH STB to authenticate part of the signalling as broadcasted by Indian satellite.

The STB manufacturer will be asked to code in the application a check of the DVB `network_id` and `original_network_ID` and to only install display channels coming from Indian network identifiers.

For more information on DVB network identifiers, see http://www.dvbservices.com/identifiers/network_id.

This offers appropriate security:

- Changing the STB software to disable the checks is very difficult thanks to secure boot.
- To change the `network_id` of the signal processed by the STB, one must acquire, demodulate, modify and re-modulate the signal. This is doable but expensive and unlikely to be the basis of a popular hack.
- A neighbouring country or region could decide to re-use Indian's `network_id`. While nothing can prevent this, it would be very visible – this could be verified regularly by appropriate market intelligence.

A stronger check of the incoming signal can be enforced by signing of the Network Information Table (NIT) at the head-end side and requiring that a DTH STB verifies the authenticity of the NIT before it initiates the service installation.

One possibility is to have the NIT generator in the head-end associate a cryptographic signature to the `TS_delivery loop` of the NIT. The signature is calculated by use of a Private Key which counterpart Public Key is known by the STB Application.

The signature is conveyed in the NIT itself under a set of specific descriptors which are part of the first descriptor loop, as shown in the table below:

Fields	Comments
Network_information_section(){	NIT Actual
Table_id	0x64
Section_syntax_indicator	
Reserved_future_use	
Reserved	
Section_length	
Network_id	This should be included in the signed part.
Reserved	
Version_number	
Current_next_indicator	
Section_number	
Last_section_number	
Reserved_future_use	
Network_descriptors_length	
For (i=0;i<N;i++){	
Descriptor()	The descriptors carrying the signature hash must be inserted in that loop.
}	
Reserved_future_use	
TS_loop_length	
For (i=0;i<N;i++){	Part of the NIT to be signed.
TS_id	
ON_id	
Reserved_future_use	
Transport_descriptors_length	
For (j=0;j<N;j++){	
Descriptor()	
}	
}	

CRC_32	
}	

It is to be noted that the DTH STB can be provisioned by a variety of public keys and that the head-end may decide to use alternate private key whenever needs arise.

And lastly, new public keys can be provisioned to DTH STB over the air either as part of a software grade or by leveraging CAS mechanism for securely and trustfully addressing STBs with the updated public keys.

6) Any other issues

7) e relevant to KYC of DTH Set Top Boxes?