M5

SABC
Vuka Sizwe!

16 May 2008

Themba Phiri
Department of Communications
Private Bag X860
Pretoria
0001

Dear Themba

STB CONTROL

As you are aware, there has in recent months been intense debate about the possibility of including conditional access in the minimum specifications for the DTT Set-Top Box. The SABC has been one of the proponents of the argument that the basic STB should be capable of having some form of conditional access. It has been our view that this need not be a conditional access system along the lines of the traditional, costly systems used for pay-TV but that some form of hybrid solution using only a software-based solution may suffice.

This continues to be our view.

While we acknowledge the fact that there has been vociferous opposition to conditional access by other broadcasters, we are of the view that stakeholders are speaking at cross-purposes on this issue.

We therefore wish to make a proposal on how this matter might be resolved in the Broadcasting Digital Migration Policy and final STB specification. In essence, we believe that there is general agreement on many of the core issues related to conditional access. We believe that reformulating the issue as one of STB control and making clear that there is no intention to limit viewers' access to free-to-air television, should help ensure the support of different stakeholders and enable the Department to move forward on this matter.

1. Importance of STB control

There are various public-interest reasons why some form of control of the STB is important. It should be noted that this STB control can be achieved through certain hardware specifications, security requirements and the inclusion of STB control

software. The encryption of services is not required. This would therefore not be a conditional access system in the traditional sense of the term.
We believe the public-interest reasons for STB control should have the support of all stakeholders. These public-interest reasons are:

To prevent subsidised STBs leaving SA

- There is a real risk that STBs could be shipped out of South Africa and used in other territories. This has happened in other jurisdictions. If the South African STBs are subsidized, this would effectively mean that government funds would be wasted. This should obviously be avoided and can be prevented by configuring the STB so that it is able to validate authenticated network messages and parameters and only operates in their presence.
- For the method to remain secure in the long term the use of asymmetric cryptography is essential. In this way discovery of keys held in the STBs would not allow hackers to generate legitimate messages. It must not be possible to change these keys within the STB, or at least the cost must be greater than manufacturing a new STB. However, it may not be necessary for these keys to be kept secret for the system to remain secure, as there is no requirement to encrypt broadcast services using secret keys. Ideally the keys and the unique address would be programmed into the chipset at the time of chipset manufacture. Alternative but less secure means might allow for the information to be programmed during STB manufacture. It is not possible to programme this unique data at a later stage, since the means to target any message carrying unique data is dependent on the address and means of validation being present in the STB.

To be able to turn off stolen STBs

- The value of stolen STBs can be minimized by ensuring that particular STBs, if reported stolen, can be disabled. It is therefore necessary for the STB to be able to process messages that turn the STB on and off. As above, the STB must be able to validate the authenticity of these messages. In addition, as it can never be certain that the STB will receive a switch-off message, the system should require that the STB receives periodic addressed switch-on messages. The effective duration of these messages should be variable and may in typical operation be set to be around 1 – 3 months. An efficient means of addressing is also required and the address of the STB must be stored in a secure way (along with the key data mentioned above), otherwise this might be modified and messages destined for one STB might be processed by another. The STB address will best be stored within the STB chipset but it might be possible to achieve sufficient security if the address is stored within the secure boot sector of the memory referred to below.

To secure software download capability

- The STBs will require software download capability and it is important that this is done securely, in order to prevent illegal software being loaded into the STB which might be used to circumvent the mechanisms described above. A secure loader can be implemented in many ways: the most important features are the validation of the software, again requiring the use of asymmetric cryptography, and a requirement that the loader software cannot be modified. Furthermore, the loader must be designed to be efficient and operating in the presence of errors, so for example the design should not require that the whole image is resent in the case of a few errors. The operation of a secure loader requires a secure boot process, which is described below. As the loader is an essential component of the STB and required for reliable operation it must not be possible to corrupt the loader software. Accordingly, the loader software should be stored in such a way that it cannot be modified by the application software.

- All of the above requirements could be circumvented if the STB can be made to start up using alternative software. Most STB chipsets incorporate hardware that allows for the boot-up (start-up) software to be validated before any software is run in the STB. The use of these chipsets requires data to be stored at the time of STB manufacture. Software based validation methods are not as secure as the chip set based methods and are not recommended for high volume production.

To target messages to STBs and groups of STBs

- It is one of government's expectations that DTT could be used for the delivery of e-government messages. It is also the SABC's strong belief that DTT should allow for messaging so that TV licence fee reminders can be sent. The SABC expects that this will result in substantially improved licence fee collections. This would require the inclusion of a unique address in the STB. The application software may later be changed or may make use of group addresses that are programmed using the unique address. For example, one group might be customers with subsidized STBs and another might be customers in a given region. As the unique address is the same as that required for the functions described above, this requirement has no impact on the STB manufacturing process. However, application software to make use of this address will be required and ideally the system will make use of the MHEG application environment to enable a wide range of interesting and useful messages to be displayed.

It should be apparent that no encryption of services is required to meet any of these four public-service objectives

In the light of these requirements for STB control, the SABC makes the following specific recommendations:

Recommendations

1. The policy should specifically state that there will be no encryption of free-to-air services on the DTT platform. In our view this should go a long way to assuage the fears of other broadcasters on the matter of conditional access.

2. In light of this, it is the SABC's further recommendation that any references to "Conditional Access" in the STB specification should be changed to "STB control".

3. Finally, the STB specification should include the following requirements :

    - a secure bootstrap loader,
    - unique serial number (SA DTT ID), and keys
    - secure download function
    - secure hardware layout

It should be noted that if there is no encryption of services, the ability to restrict the entrance of non-conformant STBs into the South African market will be weakened. However, the use of other mechanisms such as strong regulation, a well-organised conformance regime and import tariffs can act to protect the domestic market, although these are not easily achieved. In our view, the risks associated with the conformance issues are mitigated by the advantages secured by getting the agreement of all stakeholders on the matter of STB control.

The SABC thanks you for the opportunity to share our views on this important matter. We are available for future discussions on this matter.

Yours sincerely

Yusuf Nabee
DTT PROJECT LEADER

SOUTH AFRICAN CONSULATE GENERAL DUBAI