Nagra Submission to Consultation Paper:

CONTENT PROTECTION SECURITY REQUIREMENTS

In support of

CROSS CARRIAGE MEASURE IN THE PAY TV MARKET

CONSULTATION PAPER

(As Issued on: 29th April 2011)

Issued: 25th May 2011

Nagravision Asia Pte Ltd.
8 Shenton Way #34-02
AXA Tower
Singapore 068811
SINGAPORE

26th May, 2011

Ms Eileen Ang
Head (Competition and Market Access)
Media Development Authority
(Attention: Ruth Wong)

Dear Ms Ang,

Re: Nagra Submission in response to MDA Consultation paper: CONTENT PROTECTION SECURITY REQUIREMENTS In support of the CROSS CARRIAGE MEASURE IN THE PAY TV MARKET

Thank you for the opportunity to submit our comments against the Consultation paper issued on 29th April, 2011 titled: "Content Protection Security Requirements in support of the Cross-Carriage measure in the Pay TV market".

Our response is contained in the attached document and outlines the Nagra Kudelski position on Security and Content Protection in the Pay TV environment with specific reference to the Consultation paper.

Kind regards

Paul Suters
Head of Solution Experts APAC
Nagravision Asia Pte Ltd.

TABLE OF CONTENTS

SUMMARY OF MAJOR POINTS

The following is a summary of the main points contained in this Nagra submission to the Consultation paper.

- Given that:
  - The Pay TV industry is undergoing a very rapid change to the delivery and consumption of content
  - The number and variety of consumption devices available to the consumer is growing rapidly

  the Pay TV Content Providers and delivery platforms must continue to rapidly evolve to ensure that their business models and delivery mechanisms maintain pace with the consumer demands
- The growing avenues for consumer content consumption is increasing delivery platform requirements and is escalating the complexity of business models
- As a result the Content Security must also rapidly evolve to ensure the protection of the stakeholders' most valuable asset – the content - and hence their revenue streams
- Regulations should not inhibit the evolution of these business models and consumer equipment by overly limiting the operator's ability to deliver and protect that content
- Each individual operator must be in a position to work with their own content security provider to ensure maximum protection with a maximum flexibility to rapidly progress with the consumer demands
- The Singapore Market has implemented the DVB/ETSI Standards, and these should continue to be built upon utilising Simulcrypt, Common Scrambling Algorithm (CSA1/2/3) and Common Interface (CI and CI+) and security provisions built around the DVB environment
- There are dangers in specifying security provisions that are based on markets which are essentially different to the Singapore market in both business models and in technical infrastructure. These dangers pose potentially arbitrary limits on the ability RQLs and SQLs to meet the evolution of customer expectations whilst maintaining a secure delivery and content consumption environment.

STATEMENT OF INTEREST

The Kudelski Group is a world leader in digital security and convergent media solutions for the delivery of digital and interactive content. Its technologies are used in a wide range of services and applications requiring access control and rights management to secure the revenue of content owners and service providers for digital television and interactive applications across broadcast, broadband and mobile delivery networks.

Nagra, a Kudelski Group company, is the leading provider of advanced security and multi-screen user experience solutions for the monetization of digital media. The company's comprehensive end-to-end portfolio offers content providers and DTV operators worldwide with state-of-the-art, secure, open, and integrated platforms and applications over broadcast, broadband and mobile platforms to enable compelling and personalized viewing experiences. Its services and content protection technologies are used by more than 120 leading pay-TV operators around the world securing content delivered to more than 144 million active smart cards and devices. Its advanced user experience solutions have been integrated into more than 160 million devices, enabling advanced user interfaces, video-on-demand, personal video recording, advanced advertising and a variety of enhanced television applications.

Nagra is very active in the Asia Pacific Region and maintains a close interest in the Singapore Market as we are currently providing Content Protection for one of the major content delivery platforms in this market.

COMMENTS

General Comments:
The MDA's Consultation Paper touches on many of the intricacies of the Content Protection requirements in the modern world. It illustrates the complex nature of protecting the many stakeholders in the content provision, distribution and consumption of the myriad of content available in the modern world.

It is also evident in the world today that the advent of piracy is increasing in both quantity and sophistication. There is a continuing and increasing requirement for the Content Protection Industry to stay ahead of the various piracy schemes.

It is also more and more apparent that the consumer, although they may oppose the concept of piracy and the "stealing of content", may actively participate in the consumption of pirated content if an illegitimate source is the only available source to them, for whatever the reason. It is therefore essential that whilst the Content Protection mechanisms are required to be tight and to dissuade the levels of piracy, the content protection must be transparent to those who are entitled to consume that content legitimately.

The media consumption environment is similarly evolving at an extremely fast rate. The public is provided with many choices for consumption of content and the content itself has now also evolved to maximise the facilities on the consumer devices. In fact, the definition of content has extended past the definition of just "video" and "audio", and now includes the multitudes of other data surrounding content: publicity images, DVD covers, Script and Cast information, professional and consumer reviews and recommendations and even into, schedule and catalogue information.

The various devices whereby content can be consumed has burgeoned in the last few years to include consumer computers, mobile phones, personal media players and the vast array of tablets etc. which are entering the market. The next "big thing" (whatever it is) is just around the corner, and will add to the consumer's choice of devices.

As a result, the Content Protection environment has been similarly evolving since its inception, and the levels of sophistication required today in the mass media world are beyond what could have been imagined only a few years ago. Content Protection now refers not only to the protection of the carriage medium (or "pipe") but also to the individual protection of each piece of content as it is consumed on individual devices.

In this region, the vast majority of content distribution systems are based around the DVB and ETSI standards and the consultation paper seems to

refer more to a US based environment which may not be so relevant to this market. It will be essential that any regulations which are implemented are relevant to the environment being used by the service providers.

The service providers (RQL and SQL in the MDA Consultation paper) are constantly appraising and updating their business models to ensure that their customers are provided with the greatest value service. As the customers increase their consumption of content or add to the devices that the content is consumed on, the Operators and hence their Security providers must evolve their systems to keep up with the customer demands and ensure that they have no reason to seek the consumption via illegal means. Simultaneously, each piece of content's entitlement provisions must remain secure so that only suitably permitted consumers are able to access the content.

In this rapidly evolving environment, the stakeholders must remain in control of their own secure destiny. All the stakeholders (content owners, rights holders, service providers and the consumers) are entitled to ensure that their rights are maintained with maximum value.

As a security provider, it is essential to maintain research and development specifically targeted to maintaining the technological advantage over "Pirates". This involves significant time and resource from both the individual operators and their security providers working together.

Specific Comments on Consultation paper:

Section 1.6:

It is Nagra's view that the certification of each service provider's network is the responsibility of that operator in conjunction with their security service provider (regardless of whether they are deemed an RQL or an SQL). In the event of an "Independent" certification, the responsibility is removed from both the RQL and the SQL leading to potential issues of shared or dissolving responsibility to rectify the issue.

It is further important that the "Rights Holder" (SQL) has the ability to ensure that their own security provisions meet the requirements of the Content Owner, but also ensure and receive certification from the RQL that their platform also conforms to those rights.

Over time, it is expected that the security requirements from the Rights Owners will continue to change and it will be difficult to maintain specific regulations consistent with the requirements of each individual Content Owner.

Section 2.7 and Section 2.8:

With reference to Headend Security, it is essential that one of the key features of the DVB Standards, Simulcrypt, is strongly recommended. This would

ensure co-operation between the various operators on the system, and ensure that no one content protection mechanism could be deployed.

In conjunction with the Common Interface (DVB-CI and DVB-CI+) and with the Common Scrambling Algorithm (DVB-CSA1/2/3), this would ensure that no provider is locked into a single provider of Content Protection in either the launch phase, or in an ongoing operational environment.

Section 4.4:
The most common encryption environment used in the DVB standards is the Common Scrambling Algorithm. The use of DVB-CSA, CSA(2) and CSA(3) should be included.

Section 4.6:
With respect to the revocation of entitlement privileges, it is certainly possible to attempt to revoke the entitlements of "pirate" equipment. However, there may potentially be an issue where an legitimate entitled device has suffered a security flaw.

Section 4.7 and 4.8:
An additional security and protection mechanism should be that the Content Protection Solution Providers shall provide to a neutral authority all the boot-loader keys, and descrambler keys to ensure that any security breach can be managed and controlled in all circumstances.

These issues are not simply related to set-top box receivers, but also devices enabled with common interface modules (CI and CI+), and conditional access modules (CAMs).

Section 5.4:
This entire section seems to be specific to set-top box receivers, however the same comments are true for any enabled devices perhaps using a DVB Common Interface (CI and CI+).

To limit the security requirements to the Cablelabs true2way Host Device License Agreement seems to discount the many appropriate and suitable security provisions in other regimes which have also been tested against the major Motion picture studios' requirements and been accepted.

It would be more appropriate for this section of the document to not refer to any specific standards which could inhibit the security solution providers and the operators from achieving the same results in different environments and in a non-proprietary manner.

CONCLUSION

Nagravision has a wide set of security solutions that can be used to fulfill the technical content security requirements as stated in the consultation paper. Some of these requirements are under control of the Conditional Access System, others are managed by the STB middleware and STB hardware capabilities. Nagravision fully supports MDA view that Pay TV content security does require strong security of the full end-to-end solution including the STB (secure bootloader, hardware root of trust, output control in both analogue and digital forms, etc.).

As the rapidly evolving environment requires rapidly evolving security and protection mechanisms, it is essential that the operators of various platforms have a flexible security platform to operate, and to secure their revenue whilst maintaining a flexibility to grow and expand the content offering to consumers.

In regards to the security provisions, the operators should not be constrained with arbitrary or inflexible standards.