MEDIA DEVELOPMENT AUTHORITY OF SINGAPORE

CONTENT PROTECTION SECURITY REQUIREMENTS

in support of the

CROSS-CARRIAGE MEASURE IN THE PAY TV MARKET

CONSULTATION PAPER

ISSUED ON: 29 April 2011

1. Introduction

1.1 On 12 March 2010, the Media Development Authority ("MDA") introduced the cross-carriage measure ("Measure") to address MDA's concerns over the nature of competition developing in the Singapore pay TV market and, in particular, the very high degree of content fragmentation which had resulted in increased inconvenience and attendant costs for consumers and created significant barriers to entry for new entrants. The Measure imposes an obligation on Supplying Qualified Licensees (or "SQLs") (as defined in the Media Market Conduct Code ("MMCC")) to make available channels or programming content which are Qualified Content[1] ("QC") (as defined in the MMCC), for carriage by Receiving Qualified Licensees (or "RQLs") (as defined in the MMCC). The Third Consultation on the Measure was conducted from 23 March 2011 to 19 April 2011, and set out (amongst other things) the proposed amendments to the MMCC to facilitate implementation of the Measure.

[1] "Qualified Content" means:

(i) any channel or programming content (whether in a linear or non-linear format), including any basic function in support of such channel or programming content that is specified in Part I of Appendix 1 in the proposed MMCC , where such channel or programming content is:

(A) subject to sub-paragraph (ii), produced or commissioned by a Regulated Person and where, on or after 30th June 2011 the Regulated Person transmits the same on its Subscription Television Service in Singapore and refuses to allow the channel or programming content to be acquired or otherwise obtained from it for transmission on any other Relevant Platform in Singapore by:

(I) any other Regulated Person; or

(II) where the Regulated Person that produced or commissioned the channel or programming content belongs to a Group, any other Regulated Person outside the Group; or

(B) acquired or otherwise obtained on or after the Effective Date by a Regulated Person for transmission on its Subscription Television Service in Singapore under an arrangement, whether explicit or implicit, which prevents or restricts or is likely to prevent or restrict the channel or programming content from being acquired or otherwise obtained from it for transmission on any other Relevant Platform in Singapore by:

(I) any other Regulated Person; or

(II) where the Regulated Person that acquired or otherwise obtained the channel or programming content belongs to a Group, any other Regulated Person outside the Group; and

(ii) any bundled channels or bundled programming content comprising, in whole or in part, any channel or programming content that is referred to in sub-paragraph (i) of this definition.

For the avoidance of doubt, any channel or programming content is not Qualified Content by virtue only of the incorporation of any value added service that is specified in Part II of Appendix 1 of the proposed MMCC in the channel or programming content.

For the purposes of sub-paragraph (i)(B) of this definition, for the avoidance of doubt, whilst any channel or programming content that is acquired or otherwise obtained is not Qualified Content if it was acquired or otherwise obtained under or pursuant to an arrangement referred to in that sub-paragraph before the Effective Date, it is Qualified Content if and from the time such arrangement is extended, renewed, or otherwise re-contracted for on or after the Effective Date.

1.2 Under the proposed amendments to the MMCC at paragraph 2.7.2A(d), the RQL is obliged to ensure that it has a content protection system for each of its Relevant Platforms[2] which would reasonably prevent the security of all Qualified Content made available to it by any SQL from being compromised[3]. Part III of Appendix 1 in the MMCC further sets out the content protection security principles which the RQL must ensure their content protection system for each of its Relevant Platform adhere to.

Scope and objectives

1.3 This document sets out the guidelines ("Proposed Guidelines") on minimal content security requirements which may be adopted by RQLs so as to facilitate compliance with their obligations in the MMCC.

1.4 MDA's key considerations in developing the Proposed Guidelines are to identify reasonable security requirements that are considered acceptable by the pay TV industry, including content and channel providers, and at the same time ensure that these security requirements donot result in the unnecessary preclusion of pay TV retailers from becoming RQLs due to inordinate security implementation costs.

1.5 The Proposed Guidelines are intended to be platform agnostic, which means the Proposed Guidelines are intended to be applicable to all the Relevant Platforms.

1.6 Under Part III of Appendix 1 of the MMCC, RQLs would be required to certify its compliance with the principles set out in Part III of Appendix 1 of the MMCC. MDA seeks comments on whether the certification process should be one of self-certification by the RQL, joint-certification by the RQL and the SQL, or independent certification. For avoidance of doubt, SQLs and RQLs continue to be free to negotiate the requirements for carriage of QC, since different Content Providers ("CPs") may have different security requirements subject to their meeting the minimum requirements set out in the MMCC. As mentioned in the Second Consultation and Third Consultation paper***s***, MDA understands that SingNet Pte Ltd ***("***mio TV***")*** and StarHub Cable Vision Limited ("SCV"), the two nationwide subscription television service licensees likely to be designated RQLs have already deployed content

[2] "Relevant Platform" means:

(i) a hybrid fibre-coaxial network; or

(ii) a managed network using Asymmetric Digital Subscriber Line technology; or

(iii) a managed network over optical fibre- (also known as Next Generation Nationwide Broadband Network, "NGNBN").

[3] Paragraph 2.7.2A (d), MMCC.

protection systems and anti-piracy measures which MDA understands are acceptable to international content providers.

Structure of Document

1.7 The remainder of this document is laid out as follows:

- Section 2 provides an overview of the end-to-end content protection security requirements for transmitting content.
- Section 3 focuses on minimum security requirements at the network operator headend.
- Section 4 describes minimum security requirements for the content protection delivery system.
- Section 5 considers minimum set-top box content protection security requirements.

Supplementary materials used in the development of the Proposed Guidelines are included in the Annexes:

- Annex A provides a list of the reference documents used to develop the minimum security requirements.
- Annex B provides a glossary of technical terms used in this document.

1.8 MDA welcomes comments from interested parties on the Proposed Guidelines. The four-week consultation period will close on 26 May 2011.

2. END-TO-END CONTENT PROTECTION SECURITY OVERVIEW

2.1 The Proposed Guidelines on content protection security requirements outlined in this document are intended to provide end-to-end protection of QC from the point at which it enters the RQL's headend broadcast operation, all the way to the point at which it reaches the subscriber's home, where it may be securely recorded or output over a digital interconnect to the subscriber's television set. Figure 2.1 below illustrates the end-to-end cross-carriage video program distribution system.

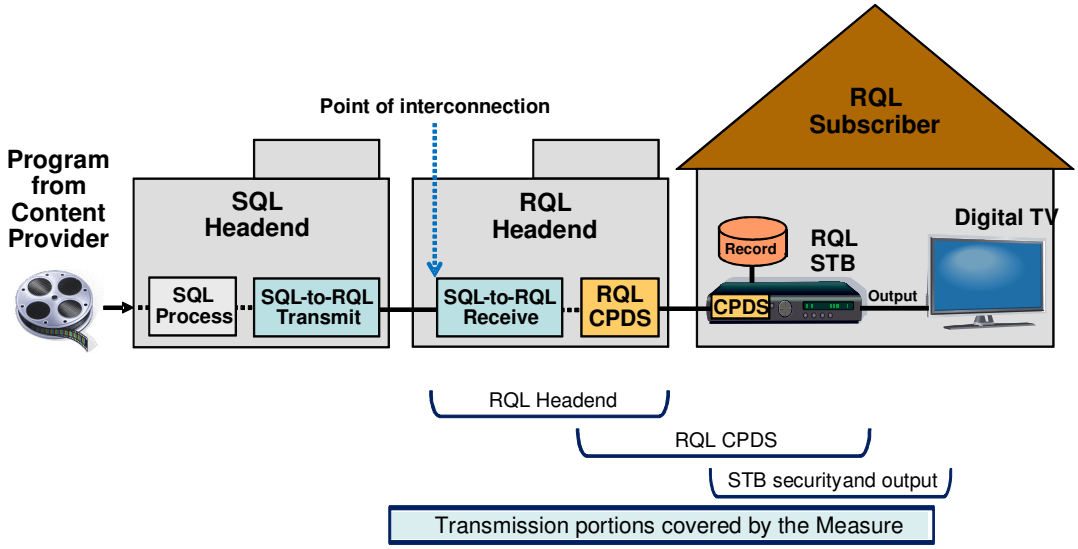

Figure 2.1: Illustration of the End-to-End Cross-Carriage Video Program Distribution System

2.2 The first stage of the system covers the delivery of programming from the content provider to the SQL. The security requirements for this first stage are not covered by the Measure.

2.3 This QC then passes through various form of SQL processing that may include reformatting, encoding and encryption to put it into a digital form used for secure transmission from the SQL transmitter to the RQL receiver inside the RQL's broadcasting headend. Once the QC enters the RQL's headend, the RQL must protect the QC, based on the Content Protection Security Requirements set out in the MMCC.

2.4 MDA is proposing that the delivery process and the technical specification of QC from SQL to RQL be left to commercial negotiation.

2.5 Whilst the above refers to linear content, MDA holds the preliminary position that the same approach is appropriate for VOD content. The SQL should make available to the

RQL whatever format the CP supplies the VOD content to the SQL in. Most VOD content is encoded by the CP or VOD content aggregator into a digital encoded file that can be securely delivered to the system operator over private networks or the Internet. The system operator can directly load the encoded content files onto its VOD servers and begin delivering to the subscribers' premises. This eliminates the need to encode the content from digital video tapes and conduct quality control review of the encoded files. If the RQL is not able to support the SQL's VOD file format specifications, then the SQL could transcode the VOD content file into the RQL's preferred format or source from the CP an additional VOD content file in the RQL's preferred format. In either case, under paragraph 2.7.1(i) of the MMCC, the SQL shall bear the cost of transcoding or sourcing the VOD file will be covered by the SQL, unless the SQL is able to agree otherwise with the RQL.

2.6 Protection of QC by the RQL can be split into three main parts:

- **Headend security**: In the RQL's headend, the RQL must follow certain network operator headend security requirements, to ensure that QC received from an SQL is adequately protected from physical or digital theft.

- **Content protection delivery system ("CPDS") security**: The RQL must provide adequate CPDS security to protect QC while it travels across the RQL's distribution network from the RQL headend to RQL subscribers' premises. The CPDS should ensure that QC is only accessible in useable form by set-top box receivers[4] that are authorised by the RQL.

- **Set-top box security**: The RQL must provide adequate set-top box security to protect QC against unauthorised access once QC has been decrypted by an authorised set-top box.

Headend security

2.7 Whilst the QC is present in the RQL's headend, the RQL must ensure that the network operator headend security requirements meet the standards set out in Part III of Appendix 1of the MMCC. Section 3 outlines the measures RQLs should adopt to facilitate compliance with paragraph 2(a) of Part III of Appendix 1 of the MMCC. As unencrypted, or "in the clear", content is generally present at some stage within operator's headend facilities, CPs are likely to be particularly sensitive to the minimum security requirements at this stage of the transmission network.

2.8 The measures outlined in Section 3 have been adapted from the security best practices documents produced by the Motion Picture Association of America

[4] Including integrated receivers such as those built into TV sets.

("MPAA"), the trade association of the major US motion picture studios. The section specifies the best practice guidelines for creating a control environment that ensures that the proper organization, processes and procedures are in place to securely protect QC. The section also describes best practices for physical site security to protect QC against physical theft, as well as best practices for digital network security to protect QC against digital theft.

Content Protection Delivery System ("CPDS") security

2.9 The CPDS used by the RQL must meet the standards set out in Part III of Appendix 1 of the MMCC. Section 4 outlines the measures the RQL should adopt to facilitate compliance with paragraph 2(b) of Part III of Appendix 1 of the MMCC. The RQL's selection and use of a CPDS is a critical part of protecting QC while it is delivered across the RQL's distribution network from the RQL's headend to RQL subscribers' premises. The CPDS ensures that QC is only accessible by set-top box receivers that are authorized by the RQL. These measures have been developed based on the specifications and characteristics of commercially-available CPDSs being used by major retail service providers ("RSPs") in Singapore, the United States and Europe.

2.10 MDA has used the term CPDS to apply to both RSPs using conditional access security ("CAS") systems for protecting and controlling access to high-value pay TV content, and also to RSPs using digital rights management ("DRM") technologies.[5] The same requirements will apply to both types of system.

Set-top box security

2.11 Once the QC is decrypted of its CPDS-protection in the RQL's authorized set-top box receiver, it must be further protected against unauthorized output or recording as described in the set-top box content protection security requirements set out in Part III of Appendix 1 of the MMCC. Section 5 sets out the compliance rules the RQL should adopt to facilitate compliance with paragraph 2(c) of Part III of Appendix 1 of the MMCC. These compliance rules include the set of analogue and digital video outputs that can be used on the set-top box for outputting decrypted qualified content ("DQC") and the set of secure recording technologies that can be used by the set-top box for making protected recordings of DQC. Section 5 also describes the Robustness Rules associated with the design and manufacture of set-top boxes that will ensure that hackers are effectively frustrated from gaining access to DQC or any of the keys or secrets that could be used to expose and gain access to DQC. The

[5] These recommendations do not preclude the RQL's use of a DRM software-based player application running on a general purpose user-programmable computing device (e.g. a PC) to deliver QC to its subscribers as an alternative to a set-top box receiver. However, such a DRM software solution would need to meet the content protection security requirements outlined in this document.

Compliance and Robustness Rules in Section 5 are adapted from the Robustness Rules defined in the US cable industry's CableLabs tru2way Host Device License Agreement [A2].

3. NETWORK OPERATOR HEADEND SECURITY REQUIREMENTS

3.1 The RQL and the SQL would have agreed on the form of secure delivery mechanism for transporting QC, such as a network broadcast feed, digital files, and/or videotapes from the SQL's headend facility to the RQL's headend facility. As described in Section 2, this will be the responsibility of the SQL under paragraph 2.7.1(i) of the MMCC. Once the QC has arrived at the RQL's headend, the RQL's management team must have in place a control environment that documents and implements both physical and digital security policies, procedures, and controls to reasonably prevent the security of all QC made available to it by the SQL from being compromised.

3.2 The remainder of this section sets out a list of the security measures that an RQL should implement in its headend facility for creating an effective control environment, for managing physical site security, and for maintaining adequate digital network security, that will prevent theft of QC from the RQL's headend operation. As previously mentioned, these network operator headend security requirements were developed based on the security best practice documents produced by MPAA, the trade association of the major US motion picture studios [A13, A14].

CONTROL ENVIRONMENT

3.3 This section describes the measures which the RQL should adopt to create and implement a management control environment that defines security policies, procedures, and controls for the secure handling of QC.

Organization maturity

3.3.1 The RQL executive management team should implement controls and processes that enable the organization to identify security threats, develop formal action plans, establish roles and responsibilities, and budget for the implementation of security control. This should include implementing an annual content security risk assessment across the organization and key workflow areas, which identifies potential security risks and areas for improvements and a budgeting process for the maintenance of the security installations (e.g., CCTV, alarm system), as well as consideration of new security tools and initiatives.

Policies and procedures

3.3.2 The RQL should document and implement formal policies, procedures, and guidelines to minimize the possibility of inappropriate handling of QC assets and execution of implemented control. These policies should include employee digital recording device usage restrictions, IT system employee usage policies, and controls on the storage and movement of QC assets.

Incident response

3.3.3 The RQL should implement an incident response and escalation procedure that is followed by the organization in order to respond and minimize the impact of an incident, as well as procedures to report to the SQL. Incidents should be recorded, investigated, resolved, and communicated to the SQL. The SQL may, in turn, inform the CP in accordance with their commercial agreement.

Process management

3.3.4 The RQL should document and implement a formal workflow for the processing and management of QC in its facility, including checkpoints and segregation of duties. The workflow should be monitored to ensure controls continue to operate as implemented. The RQL should perform an annual audit of its monitoring controls and authorization checkpoints, which should be conducted by personnel who are independent of the production and/or control processes.

Recruitment and personnel

3.3.5 The RQL's process for recruiting and hiring personnel should include controls to mitigate the risk of hiring personnel that would pose a significant threat to QC assets. Controls should comprise performing professional references and criminal background checks, use of confidentiality agreements with new employees, and the definition, communication, and use of disciplinary measures for employee violations of company policies.

Training and education

3.3.6 The RQL should develop and provide security and anti-piracy training and awareness programs to relevant full-time and temporary employees upon hiring, as well as on a periodic basis. The training should include an overview of content handling and facility security policies, and may also include discussion of the impact of piracy on the company and the industry, as well as on individuals.

Vendor management

3.3.7 The RQL should develop and follow a vendor screening process that ensures vendors emulate the organization's internal policies, procedures, and standards as they relate to the protection of QC assets. RQLs should also not grant access to sensitive production areas, where QC assets are located, to common facility vendors (e.g., cleaning crew, seasonal temps) unless accompanied by RQL staff.

PHYSICAL SECURITY

3.4 This section describes the measures which the RQL should adopt for the physical security of its headend facility to protect against the physical theft of QC while present in the facility.

Facility access

3.4.1 The RQL should implement access controls at its headend facility in order to prevent unauthorized access of individuals that could lead to theft of QC, including physical entry protocols for employees and visitors, as well as means of identifying internal personnel, temps, and visitors. The RQL should utilise security guards and implement a key-card system to control and monitor all entry points into the headend facility. The RQL should also implement a visitor protocol that includes the use of a visitors' log, easily-identified visitor badges, and visitor escorts when visitors are in the facility.

Facility security

3.4.2 The RQL should implement security controls at the facility in order to secure the perimeter, including the use of fences/walls and alarm systems, as well as the implementation of emergency protocols to securely protect QC assets from theft. Based on the location and layout of the RQL headend facility, management should implement a strong perimeter security environment that should include security fencing, cameras, limited vehicle and pedestrian entry points, a centralized alarm system, loading docks, and security cages containing QC assets**.**

Facility monitoring

3.4.3 The RQL should implement a closed-circuit TV ("CCTV") system to monitor the headend facility. Processes should be implemented to review CCTV footage and key-card access logs. CCTV footage and key-card access logs should be retained, based on the RQL's log retention/rotation policy. Searches should be performed on individuals, packages, and vehicles entering and exiting the facility, when and where

applicable. CCTV recordings and key-card access logs should be retained for at least 90 days.

Inventory and asset management

3.4.4 The RQL should implement a media asset management procedure to provide detailed tracking of physical QC and blank media assets (e.g. blank DVDs). Inventory counts should be performed on a periodic basis, and blank media is tracked and counted periodically. Asset tracking logs should be retained for at least 90 days.

Physical asset security

3.4.5 QC assets, blank media/raw stock, and production systems should be stored in secure locations in the RQL headend with access restricted to appropriate personnel. In addition, scrap/disposal assets should be stored in a secure location before destruction, and all disposals/destructions should be logged.

Shipping and receiving

3.4.6 The RQL should implement a process to receive and ship physical QC assets in and out of the facility, including techniques used to track asset shipping and receiving details. This process should include implementing a truck driver's log to record each shipment. Such logs should be retained for at least 90 days. Delivery staff, such as truck drivers should not be allowed to enter the facility unless accompanied by RQL staff.

DIGITAL SECURITY

3.5 This section describes the measures the RQL should adopt for the digital security of its headend facility to protect against the digital theft of QC digital assets while present in the facility.

Infrastructure security

3.5.1 The RQL should implement sufficient security controls at the infrastructure or network layers of the facility's internal content network. This includes network servers, routers, switches, and other network devices used within the RQL's headend facility. The RQL should segment the internal content network from other networks in the facility (e.g., office network) and apply MAC-address security at the switch level to restrict non-production systems (e.g., laptops) and remote access from the public Internet to the internal content network. The RQL should also implement state-of-the-art firewalls with an access control list ("ACL") to prevent unauthorized access to the internal content network. The RQL should also prohibit the use of

wireless devices on the internal content network as well as prohibit Internet access on systems (e.g., desktops and servers) that process or store QC.

System security

3.5.2 The RQL should block and/or monitor the use of input/output devices on production systems where digital QC is stored or processed. Anti-virus software should be implemented on any systems on the internal content network that are vulnerable to being infected with viruses and/or malicious codes coming from outside the facility.

Infrastructure authentication and authorization

3.5.3 The RQL should implement authentication mechanisms to restrict access to the internal content network. Administration access rights should be restricted to appropriate personnel in charge of the internal content network security. This pertains to network devices, as well as the operating system on production workstations and servers. This should include assigning system administration rights on network devices (e.g., servers, routers, switches, firewalls) and production system operating systems to personnel responsible for managing the network and production devices and enforcing the use of unique usernames and strong passwords to access production systems/networks.

Infrastructure monitoring

3.5.4 The RQL should implement processes for the logging and monitoring of activities performed on the internal content network, including routers, switches, and other network devices. These logs should be retained for at least 90 days.

Content authorization

3.5.5 The RQL should implement a process to manage user access rights to the QC, including the processes to manage QC access requests, access changes, and access terminations, as well as controls to limit administration rights. This pertains to QC storage devices (e.g., storage area networks, network attached storage, and QC servers).

Content security and watermarking

3.5.6 The RQL should use advanced content security techniques on all QC assets, including the use of encryption of stored QC files, where applicable.

3.5.7 The SQL's application of an RQL-specific forensic watermark[6] to track and determine potential sources of piracy of QC supplied to each RQL should be at the option and responsibility of the SQL. However, the RQL should not undertake, or neglect to undertake, any activity which would strip, obscure or interfere with such forensic watermarking (for example, during the RQL's processing of QC within its headend facility).

3.5.8 There may be instances where an SQL has agreed with a CP to apply a transactional forensic watermark to track and determine potential sources of piracy of each instance of QC accessed by each SQL subscriber. In the case where an SQL has agreed and is complying with such a transactional watermarking obligation for QC (for example, transactional watermarking applied in the subscriber's set-top box during viewing of an early-window, high definition VOD movie), then the RQL will also be obligated to apply transactional forensic watermarking for such QC accessed by each of its subscribers.

Content tracking

3.5.9 The RQL should track all activities performed with QC (e.g., access, copy, movements) on content storage devices through the use of object audit logging and/or a digital content management system. These tracking logs should be retained for at least 90 days, with log access being restricted to personnel responsible for storage device administration.

Content transfer security

3.5.10 The RQL should implement secure transfer tools, secure authentication protocols, and dedicated content transfer devices when QC is transferred into or out of the RQL headend facility. These dedicated transfer devices should not be in the internal content network, and should only be used by authorized personnel.

Content transfer authorization

3.5.11 The RQL should implement a process to manage user access rights on content transfer tools, including the processes to request and grant access and assign system privileges, as well as controls to limit administration rights. The access rights to

[6] For example, an SQL could uniquely watermark the video program file/stream being delivered to each RQL so if there was a piracy leak, the SQL could extract the forensic watermark from the discovered, pirated content in order to trace the leakage back to a specific RQL. Watermarking can be "covert" (invisible/inaudible) or can be "overt" (visibly marked in the video). In the case of the Measure, an SQL would need to use a covert watermark since the RQL would object if the SQL was delivering programming with the SQL's overt watermark in the program.

transfer tools should be restricted based on job function. The assignment of transfer tool administration rights should be limited to appropriate personal.

Content transfer tracking

3.5.12 The RQL should use electronic transfer tools that have logging capabilities enabled to monitor all transfer activities performed with digital QC. The RQL should maintain QC transfer logs for at least 90 days.

Summary

3.6 In summary, the measures set out in this section for network operator headend security are designed to protect QC within the RQL's headend facility. The RQL's management team must have in place a control environment that documents and implements both physical and digital security policies, procedures, and controls for protecting the QC assets.

3.7 These headend security requirements were adapted from the security best practices documents produced by the MPAA.

4. CONTENT PROTECTION DELIVERY SYSTEM SECURITY REQUIREMENTS

4.1 The RQL's CPDS plays a critical role in protecting digital QC while it is carried across the RQL's network so it can be received, decrypted, and then made accessible in usable form by a set-top box that has been authorized by the RQL.

4.2 In the Proposed Guidelines, the term CPDS will apply to both RSPs using CAS systems for protecting and controlling access to high-value pay TV content and also to RSPs using DRM technologies.[7] The same requirements apply to both types of system.

4.3 The remainder of this section sets out a list of the security measures which an RQL should adopt in relation to its CPDS in order to protect against the unauthorized access to and use of QC.

CPDS content encryption algorithm

4.4 The RQL's CPDS should implement the 128-bit Advanced Encryption Standard ("AES") encryption algorithm for securely protecting QC, or alternatively, a publicly-reviewed encryption algorithm (for example, the Triple Data Encryption Standard ("Triple DES")) with similar or better security (which the RQL demonstrated with third-party analysis).

4.5 The RQL's CPDS should manage and securely deliver the subscribers' access and usage rights, along with the keys, secrets and/or DRM license required to decrypt the protected QC. The system should also convey the copy control rights information associated with QC, as well as provide a mechanism for managing the protected analogue and digital video outputs and the secure recording of CPDS-decrypted QC.

CPDS revocation and renewability

4.6 In addition to its ability to revoke security components which have been compromised, the RQL's CPDS must have the ability to revoke compromised devices when pirate set-top boxes appear in the market.

4.7 Furthermore, the RQL's CPDS must implement a means for economically renewing the secrets and security of the CPDS in the case of a successful compromise of the system. This renewal typically takes the form of replacing the smartcard, which holds the secrets of the CPDS. Where a smartcard is used, additional secrets may be held in the

[7] These recommendations do not preclude the RQL's use of a DRM software-based player application running on a general purpose user-programmable computing device (e.g. a PC) to deliver QC to its subscribers as an alternative to a set-top box receiver. However, such a DRM software solution would need to meet all of the content protection security requirements outlined in this document.

set-top box, but these secrets should not include information regarding the customer entitlements or keys/algorithms required to process such entitlements.

4.8 In a two-way connected CPDS without removable security hardware, it is also possible to implement a software-renewable CPDS by using a hardware root of trust in the set-top box.

CPDS compromise monitoring, response, and renewal process

4.9 The RQL must implement a CPDS piracy monitoring process, for example monitoring street markets and internet sales of pirate smartcards, set-top boxes, or circumvention software, to determine when a compromise of the CPDS has occurred. The CPDS must support software countermeasures and second-line defences that can be deployed to re-secure the system in the case of a successful compromise. In addition, the CPDS vendor should supply new hardware or software security elements to the RQL to facilitate renewal of the security elements to begin within 6 months of confirming the compromise, and should be completely finished with the CPDS renewal within 12 months.

CPDS security element uniqueness

4.10 The security elements used by the RQL's CPDS should be unique to that operator. These elements should include at least an element of hardware modification that introduces an element of device uniqueness to the deployed cryptography. Alternatively, software techniques (such as those used in DRM solutions) may be deployed in combination with a hardware root of trust that provide for sufficient software diversity and device uniqueness to ensure that the transport of software or secrets between a pirated system and another from the same CPDS vendor will not result in piracy of the second system.

Summary

4.11 In summary, the measures set out in this section for Content Protection Delivery System security are designed to protect QC as it is carried across the RQL's network so it can be received, decrypted, and then made accessible in usable form by a set-top box that has been authorized by the RQL.

4.12 These content protection delivery system security requirements have been developed based on the specifications and characteristics of commercially available conditional access systems being used by major RSPs in Singapore, the United States, and Europe.

5 SET TOP BOX CONTENT PROTECTION SECURITY REQUIREMENTS

5.1 In order to meet the content protection security requirements at the set-top box level as mandated by the MMCC, MDA holds the preliminary view that the RQL's set-top box receiver should decrypt the CPDS-protected QC and then securely manage the output and recording of such content using protected digital output and secure recording technologies that that are acceptable to content owners. The output and recording of decrypted DQC is based on the copy control usage rights conveyed via the CPDS.

5.2 Section 5.5 sets out compliance rules the RQL should adopt to facilitate compliance with paragraph 2(c) of Part III of Appendix 1 of the MMCC. These compliance rules include the set of approved analogue and digital video outputs that can be used on the set-top box for outputting DQC and the set of secure recording technologies that can be used by the set-top box for making protected recordings of DQC.

5.3 Section 5.6 describes the Robustness Rules associated with the design and manufacture of set-top boxes that are intended to ensure that hackers are effectively frustrated from gaining access to DQC or to any of the keys or secrets that could be used to expose and gain access to DQC or circumvent the content protection.

5.4 The set-top box content protection security requirements set out in this section are adapted from the Compliance and Robustness Rules, defined in the United States cable industry's CableLabs tru2way Host Device License Agreement, which are generally supported by the major US motion picture studios.

5.5 Compliance rules for protected outputs and secure recording

5.5.1 The RQL's set-top box receivers, at the time of manufacture, must comply with the compliance rules set forth in this section and be constructed so as to resist attempts at circumvention of these requirements as specified in Section 5.6, Robustness Rules for Design and Manufacture of Set-Top Box Receivers.

Outputs from the set-top box

General

5.5.2 MDA takes the preliminary view that in order to meet the set-top box content protection security standard under paragraph 2(c)(i) of Part III of Appendix 1 of the MMCC, the RQL's set-top box receivers should not output DQC, or pass DQC received through the RQL's service to any output, except as set out in this Section 5.50, or otherwise allowed by the receiver's middleware application. For the purposes of

these compliance rules, an output shall be deemed to include, but not be limited to, any transmissions to any internal copying, recording, or storage device, but shall not include internal non-persistent or transitory transmissions that otherwise satisfy these Compliance and Robustness Rules.

Standard definition analogue outputs

5.5.3 RQL's set-top box receivers may only pass DQC received through the RQL's service, in analogue form, if such receiver can generate the appropriate specifications for the Automatic Gain Control and Colorstripe copy control systems [A17] and the appropriate copy control and redistribution control signalling (also known as and carried in the Widescreen Signaling ("WSS") data) for standard definition analogue video outputs.

5.5.4 In particular, the RQL's set-top box receivers with any standard definition analogue outputs shall only output DQC received through the RQL's service, or pass DQC received through the RQL's service, as permitted by the below.[8]

5.5.5 In any transmission through a PAL RF, Composite, Y,R-Y,B-Y, or RGB format analogue output (including an S-video output and including transmissions to any internal copying, recording or storage device) of a signal, the RQL's set-top box receiver shall generate the appropriate copy control and redistribution control signalling in response to the copy control information conveyed by the CPDS (i.e. trigger bits for Automatic Gain Control and Colorstripe copy control systems, as referenced below). The technologies that satisfy this condition include the following:

(1) For PAL analogue outputs (including RF, Composite or S-Video), the specifications for the Automatic Gain Control and Colorstripe copy control systems and with copy control and redistribution control signalling mapped to the appropriate respective data fields of Line 23 complying with ETSI EN 300 294 [A8];

(2) For 576i (interlace scan), YUV or Y, R-Y, B-Y outputs, the appropriate specifications for the Automatic Gain Control copy control system and copy control and redistribution control signalling, as identified in the Specifications in (1);

(3) For 576p progressive scan outputs, the appropriate specification for the Automatic Gain Control copy control system, as identified in the specifications in (1) and copy control and redistribution control signalling mapped to the appropriate respective data fields of Line 43 complying with IEC 62375 [A12]; and

[8] We note that not all of the cases will be applicable to all types of technical platform which may be operated by RQLs in Singapore.

(4) Except as provided for under VGA below for standard definition analogue outputs not specified above, or as provided for in the section on high definition analogue outputs, below, RQL's set-top box receivers shall not transmit DQC through such analogue outputs until such time as these Compliance Rules are amended to permit the same.

5.5.6 An RQL's set-top box receiver may output DQC, or pass DQC through an analogue VGA interface to a monitor, in standard definition analogue Form, in RQL's set-top box receivers manufactured prior to December 31, 2005. As used herein, "VGA" is a Video Graphics Array display system, typically implemented as a computer video output that is 640 x 480 pixels.

High definition analogue outputs

5.5.7 RQL's set-top box receivers with high definition analogue component video outputs may only pass DQC received through the RQL's service, in high definition analogue form through such outputs, if such receiver can generate the appropriate analogue copy control and redistribution control signalling mapped to the appropriate respective data fields and vertical lines complying with CEA-805-D [A3].

5.5.8 RQL's set-top box receivers with high definition analogue component video outputs may only pass DQC received through the RQL's service, in high definition analogue form through such outputs under one of the following circumstances:

- Over 1080i60 or 720p60 analogue component video output if marked with copy control signalling defined in CEA-805-D [A3];
- Over 1080i50 or 720p50 analogue component video outputs, but only if the SQL has approval from the CP to output the QC over such output; or
- Over 1080i50 or 720p50 analogue component video outputs, if such HD Qualified Content is first processed into a constrained image.

Digital outputs

5.5.9 The RQL's set-top box receivers with any digital outputs shall only output DQC received through the RQL's service, or pass DQC received through the RQL's service, as permitted by the following.[9]

- The RQL's set-top box receivers may output DQC, and pass DQC to an output, in digital form over IEEE 1394 interfaces, where such output is protected by DTCP [A1]. The RQL's set-top box receivers must support DTCP "Full Authentication," and may additionally support DTCP "Restricted Authentication". When so

[9] We note that not all of the cases will be applicable to all types of technical platforms which may be operated by RQLs in Singapore.

outputting or passing such DQC to a DTCP-1394 output, the DTCP Source Function shall correctly map the copy control information ("CCI") to the DTCP Encryption Mode Indicator ("EMI"), DTCP Analogue Protection System ("APS") signalling, DTCP Image Constraint Token ("ICT"), and DTCP Encryption Plus Non-assertion ("EPN") signalling in accordance with the DTCP Specification. (Please note that capitalized terms used in this paragraph, but not otherwise defined in these Compliance Rules, shall have the meaning set forth in the DTCP Specification [A6] or the DTCP Adopter Agreement [A5].)

- The RQL's set-top box receivers may output DQC received through the RQL's service, and pass DQC received through the RQL's service to an output, in digital form over DVI, HDMI, or DisplayPort interfaces, and where the output always has HDCP active and on. When so outputting or passing such DQC to a DVI, HDMI, or DisplayPort output, the HDCP Source Function shall pass DQC received through the RQL's service to such output in digital form only when it has securely verified that the HDCP Source Function has signalled that it is engaged and able to deliver protected content, which means (i) HDCP protection is operational and always active on all DVI, HDMI, or DisplayPort outputs; and (ii) there is no HDCP device on such output whose Key Selection Vector is in a SRM. Capitalized terms used in this paragraph, but not otherwise defined in these Compliance Rules, shall have the meaning set forth in the HDCP Specification [A10] or the HDCP License Agreement [A9].

- The RQL's set-top box receivers may output DQC received through the RQL's service, and pass DQC received through the RQL's service to an output, in digital form using HDCP 2.0 Specifications [A11], as defined above (including the approved interfaces identified therein), where the output always has HDCP active and on. When so outputting or passing such DQC to such outputs the HDCP Source Function shall pass DQC received through the RQL's service to such output in digital form only when it has securely verified that the HDCP Source Function has signalled that it is engaged and able to deliver protected content, which means (i) HDCP protection is operational and always active on all such outputs; and (ii) there is no HDCP device on such output whose key selection vector is in a system renewability message ("SRM"). Capitalized terms used in this paragraph, but not otherwise defined in these Compliance Rules, shall have the meaning set forth in the HDCP 2.0 Specifications [A11] or the HDCP License Agreement [A9].

- The RQL's set-top box receivers may output DQC, and pass DQC to an output in digital form where such output is protected by DTCP-IP. When so outputting or passing such DQC to a DTCP-IP output, the DTCP Source Function shall map the CCI conveyed by the CPDS to the DTCP Encryption Mode Indicator ("EMI"), DTCP APS signalling, DTCP ICT, and DTCP EPN signalling in accordance with the DTCP

Specification. Capitalized terms used in this paragraph, but not otherwise defined in these Compliance Rules, shall have the meaning set forth in the DTCP Specification or the DTCP Adopter Agreement.)

- The RQL's set-top box receivers may output DQC, and pass DQC to an output in digital form where such output and content is protected by IP Rights Management ("IPRM") system in accordance with the Motorola IPRM System Submission of New Digital Outputs and Content Protection Technologies; Revision 2.7 dated November 10, 2006 [A15], as amended, and the applicable license terms governing the implementation of IPRM, as provided by Motorola, such terms including compliance with the Compliance and Robustness Rules herein.

- The RQL's set-top box receivers may output content received through the RQL's service, which has no rights being asserted by the content owner, through digital outputs other than the outputs listed above.

System renewability messages

5.5.10 When outputting or passing DQC through any output, RQL's set-top box receivers shall process and carry all valid SRMs delivered through the RQL's content delivery system. In the case of DTCP, the RQL's set-top box receivers shall process and pass the DTCP SRM to the DTCP Source Function. Likewise, in the case of HDCP, the RQL's set-top box receivers shall process and pass the HDCP SRM to the HDCP Source Function.

Copy Control Watermark Non-Interference

5.5.11 Commencing 18 months after the existence of a Consensus Watermark, the RQL should, when selecting among technological implementations for product features for its set-top box receivers designed after such date, take commercially reasonable care (taking into consideration the technical characteristics, costs of implementation, commercial terms and conditions, and impact on DQC and the effectiveness or visibility of the Consensus Watermark) that its set-top box receivers do not strip, obscure or interfere with such Consensus Watermark in QC that has been decrypted; (ii) shall not source and deploy set-top box receivers for the primary purpose of stripping, obscuring or interfering with such Consensus Watermark in QC that has been decrypted; and (iii) shall not knowingly market or distribute or knowingly cooperate in marketing or distributing set-top box receivers for the primary purpose of stripping, obscuring or interfering with such Consensus Watermark in QC that has been decrypted.

5.5.12 If the RQL complies with the foregoing provisions of this section, an RQL should be able to incorporate legitimate features (e.g. zooming, scaling, cropping, picture-in-

picture, compression, recompression, image overlays, overlap of windows in a graphical user interface, audio mixing and equalization, video mixing and keying, down-sampling, up-sampling, and line doubling, or conversion between widely-used formats for the transport, processing and display of audio-visual signals or data, such as between analogue and digital formats and between PAL and NTSC or RGB and Y, Pb, Pr formats, as well as other features, as may be added to the foregoing list from time to time by the MDA by amendment to these Compliance Rules) in their RQL's set-top box receivers, without compromising the set-top box content protection security standards set out in the MMCC. Such features should not be prohibited by law, and not be deemed to strip, interfere with or obscure the Consensus Watermark in DQC.

Copying, recording, and storage of controlled content

General

5.5.13 In order to meet the set-top box content protection security standard under paragraph 2(c)(ii) of Part III of Appendix 1 of the MMCC, the RQL's set-top box receivers (including, without limitation, such RQL set-top box receivers with inherent or integrated copying, recording or storage capability) should not copy, record, or store DQC, except as set out in this section.[10]

Mere Buffer for Display

5.5.14 RQL's set-top box receivers may store DQC temporarily for the sole purpose of enabling the immediate display of DQC, provided that (a) such storage does not persist after the DQC has been displayed, and (b) the data is not stored in a way that supports copying, recording, or storage of such data for other purposes.

Copy No More

5.5.15 The RQL's set-top box receivers shall not copy, record or store DQC that is designated in the copy control information as having been copied but not to be copied further ("copy no more"), except as permitted in the *Mere Buffer for Display* and *Copy One Generation* sections, above and below.

Copy Never

5.5.16 The RQL's set-top box receivers, including, without limitation, such RQL set-top box receivers with integrated recording capability such as a so-called "personal video recorder," shall not copy DQC that is designated in the copy control information

[10] We note that not all of the features will be applicable to all types of technical platforms which may be operated by RQLs in Singapore.

conveyed by the CPDS as never to be copied ("copy never") except as permitted in the *Mere Buffer for Display* section above, or by the following:

- Such RQL set-top box receivers may internally store such DQC, including for the purpose of pausing the program, when instructed by the copy control information conveyed by the CPDS if the stored content is securely bound to the set-top box receiver doing the recording so that it is not removable at that point and is not itself subject to further temporary or other recording within the set-top box receiver before it is rendered unusable; provided such set-top box receiver is made in compliance with the Robustness Rules to avoid circumvention of such restrictions. When internally storing such DQC, including for the purpose of implementing a pause function, as allowed in this section, the DQC shall be stored in a manner which is encrypted in a manner that provides no less security than 128-bit AES or 112-bit 3DES.

5.5.17 The RQL's set-top box receivers shall be designed and manufactured to be able, when required by the copy control information conveyed by the CPDS, to obliterate the stored DQC or render unusable the stored DQC after a stated period of time, on a frame-by-frame, minute-by-minute, megabyte-by-megabyte basis.

Copy One Generation

5.5.18 The RQL's set-top box receivers may make a copy of DQC that is designated in copy control information conveyed by the CPDS as permissible to be copied for one generation ("Copy One Generation"), as provided in the *Mere Buffer to Display* or *Copy Never* sections or provided that the copy (a) is scrambled, encrypted or uniquely bound to that set-top box receiver, in each case using a form of copy protection that is identified by an amendment to this section, if any, and (b) is remarked as not to be further copied ("copy no more") in a manner that is set forth in this section or the *User Accessible Bus* section, and will be effective to prevent such further copies being made by devices capable of receiving a transmission of such remarked data through the outputs identified in the *Digital Outputs* section above. In the absence of either such amendment to this section, no copy of such DQC other than as permitted in the *Mere Buffer to Display, Copy Never* or the *User Accessible Bus* sections may be made.

5.5.19 An RQL's set-top box receiver that makes a copy of DQC marked in its copy control information as "Copy One Generation" in accordance with this section may move such content to a single removable recording medium, or to a single external recording device, only when:

(a) the external recording device indicates that it is authorized to perform this Move function in accordance with the requirements of this section, and to copy such DQC in accordance with the requirements of this section;

(b) such DQC is marked for transmission by the originating set-top box receiver as "Copy One Generation";

(c) the DQC is output over a protected output, in accordance with Section 5.5;

(d) before the Move function is completed, the originating set-top box receiver recording is rendered non-useable and the moved DQC is marked "Copy No More";

(e) the device to which the removable recording medium is moved is unable or rendered unable to output the DQC except through outputs authorized by these Compliance Rules; and

(f) the copy is stored (i) using a secure encryption protocol which uniquely associates such copy with a single device so that it cannot be played on another device or, if stored to removable media, so that no further usable copies may be made thereof or (ii) otherwise using methods referenced above.

5.5.20 Multiple moves consistent with these requirements are not prohibited.

5.5.21 In accordance with the above, the RQL's set-top box receivers may make a copy of DQC that is designated as Copy One Generation using VCPS in accordance with the Vidi System Description Version 1.0 dated March 2004 [A19] and the license terms governing the implementation of VCPS as provided in version 1.2 of the Video Content Protection System Agreement, dated September 1, 2004 [A18].

5.5.22 In accordance with the above, the RQL's set-top box receivers may make a copy of DQC that is designated as Copy One Generation providing such copy is protected using CPDO [A7] in accordance with the EnCentrus Content Protected Digital Output Port System Description; Revision 1.2 dated January 2006 and the current license terms[11] governing the implementation of CPDO as provided in the CPDO License Agreement [A4] dated December 20, 2005 or later, such terms, including compliance with the Compliance and Robustness Rules herein.

5.5.23 In accordance with the above, the RQL's set-top box receivers may make a copy of DQC that is designated as Copy One Generation, providing such copy is protected using RPSP. The RQL's set- top box receivers may also make a copy of DQC that is signalled to have redistribution control asserted providing such copy is protected using RPSP. Such copies produced using RPSP shall be made in accordance with the Recording Protection System for Portable extension Technical Specification [A16].

User accessible bus

5.5.24 An RQL's set-top box receiver may use a user-accessible digital interface to store DQC on a storage device, if:

(a) the DQC is encrypted across the interface, and in storage, with an encryption algorithm that provides no less security than 128-bit AES or 112-bit 3DES;

(b) the DQC is uniquely cryptographically associated with (i) the original set-top box receiver, or (ii) the storage device itself, such that DQC is unusable to any other product or device;

(c) the interface and storage device, or the system architecture, provides protection from a "disk cloning attack";

(d) no key information is stored on the storage device unless encrypted with security no less than 128-bit AES or 112-bit 3DES encryption; and

(e) the move, storage and copying of DQC otherwise meets the criteria set forth in the Robustness Rules and these Compliance Rules.

5.6 Robustness rules for design and manufacture of set-top box receivers

5.6.1 Under paragraph 2(c)(iii) of Part III of Appendix 1 of the MMCC, RQLs have to ensure that the set-top box receivers should be robust to effectively frustrate attempts to gain access to decrypted QC or the keys to gain access to such QC. To facilitate compliance, the RQL's set-top box receivers should be designed and manufactured according to the Robustness Rules set forth in this section.

Construction

General

5.6.2 The RQL's set-top box receivers, as shipped, should meet the Compliance Rules defined in Section 5.5, and should be designed and manufactured in a manner to effectively frustrate attempts to modify such set-top box receivers to defeat the Compliance Rules or content protection security functions.

Defeating functions

5.6.3 The RQL's set-top box receivers should not include the following in each case by which the content protection technologies, analogue protection systems, reprotection, CGMS-A/RCI/APS signalling, output restrictions, recording limitations, or other mandatory provisions of the Compliance Rules can be defeated or by which DQC can be exposed to unauthorized access, copying, redistribution, or modification of usage rights:

(a) switches, buttons, jumpers, specific traces that can be cut or place the set-top box receiver in a test mode, or software equivalents of any of the foregoing; or

(b) active JTAG ports, emulator interfaces or test points to probe security functions; and

(c) service menus or functions (including remote-control functions);.

Keeping of secrets

5.6.4 The RQL's set-top box receivers should be designed and manufactured in a manner to effectively frustrate attempts to discover or reveal (a) the unique number, of a specified bit length, assigned to each set-top box receiver, or the numbers used in the process for encryption or decryption of DQC (collectively, "Keys"), and (b) the methods and cryptographic algorithms used to generate such Keys.

Documents and robustness certification checklist

5.6.5 Before deploying any set-top box receivers for commercial use, the RQL must confirm that its set-top box vendor has performed tests and analyses to assure compliance with these Robustness Rules. The RQL and its set-top box receiver vendor are strongly advised to review carefully the Compliance Rules and these Robustness Rules so as to evaluate thoroughly both its testing procedures and the compliance of its set-top box receivers.

Controlled content paths

5.6.6 DQC should not be available on outputs other than those specified in the Compliance Rules, and, within such RQL's set-top boxes, DQC should not be present on any user-accessible buses (as defined below) in non-encrypted form (compressed or uncompressed). Similarly unencrypted Keys used to support any QC encryption and/or decryption in the RQL's set-top box receiver data should not be present on any user-accessible buses. Notwithstanding the foregoing, compressed audio data can be output in the clear via a digital connector.

5.6.7 The RQL's set-top box receivers should not allow DQC on any internal interface unless secured from unauthorized interception to the level of protection specified in Section 5.6.90.

5.6.8 The RQL's set-top box receivers should not allow Keys used to support any content encryption and/or decryption to be present on any user-accessible bus or on any internal interface unless encrypted and secured from unauthorized interception to the level of protection specified in Section 5.6.9.

Methods of making functions robust

5.6.9 The RQL's set-top box receivers should use at least the following techniques to make robust the functions and protections specified in this document:

(a) **Distributed functions:** the portions of the RQL's set-top box receivers that perform authentication and decryption and the MPEG (or similar) decoder should be designed and manufactured in a manner associated and otherwise integrated with each other such that DQC in any usable form flowing between these portions of the RQL's set-top box receiver shall be secure to the level of protection described in (e) below from being intercepted or copied.

(b) **Software**: any portion of the RQL's set-top box receiver that implements a part of the content protection functions in software should include all of the characteristics set forth in Sections 5.6.2 to 5.6.5. For the purposes of these Robustness Rules, "software" should mean the implementation of the content protection functions requires an RQL's set-top box receivers to be compliant through any computer program code consisting of instructions or data, other than such instructions or data that are included in Hardware. Such implementations shall:

(i) Comply with the *Keeping of Secrets* portion (Section 5.6.4) by any reasonable method including but not limited to encryption, execution of a portion of the implementation in ring zero or supervisor mode, and/or embodiment in a secure physical implementation; and in every case of implementation in software, using effective techniques of obfuscation to disguise and hamper attempts to discover the approaches used;

(ii) Be designed to perform self-checking of the integrity of its component parts such that unauthorized modifications will be expected to result in a failure of the implementation to provide the authorized authentication and/or decryption function. For the purpose of this provision, a "modification" includes any change in, or disturbance or invasion of features or characteristics, or interruption of processing, relevant to Sections 5.6.2 to 5.6.5. This provision requires at a minimum the use of code with a cyclic redundancy check that is further encrypted with a private key or a secure hashing algorithm;

(iii) Meet the level of protection outlined in (e) below.

(c) **Hardware**: any portion of the RQL's set-top box receiver that implements a part of the Specifications in hardware should include all of the characteristics set forth in Sections 5.6.2 – 5.6.5. For the purposes of these Robustness Rules, "hardware" should mean a physical device, including a component, that implements any of the content protection functions requires that RQL's set-top box receivers be compliant, and that does not include instructions or data other than such instructions or data

that are permanently embedded in such device or component; or includes instructions or data that are not permanently embedded in such device or component where such instructions or data have been customized for such set-top box receivers, and such instructions or data are not accessible to the end user through the RQL's set-top box receiver. Such implementations should:

(i) Comply with *Keeping of Secrets* portion (Section 5.6.4) by any reasonable method including but not limited to: embedding Keys, Key generation methods and the cryptographic algorithms in silicon circuitry or firmware that cannot reasonably be read, or the techniques described above for software;

(ii) Be designed such that attempts to re-program, remove or replace hardware elements in a way that would compromise the security or content protection functions or in the RQL's set-top box receiver would pose a serious risk of damaging such set-top box receiver so that it would no longer be able to receive, decrypt or decode DQC. By way of example, a component which is soldered rather than socketed may be appropriate for this means;

(iii) Meet the level of protection outlined in (e) below.

(d) **Hybrid**: the interfaces between hardware and software portions of the RQL's set-top box receivers should be designed so that they provide a similar level of protection which would be provided by a purely hardware or purely software implementation, as described above.

(e) **Level of protection**: the core encryption functions of the content protection requirements (maintaining the confidentiality of Keys, Key generation methods and the cryptographic algorithms, conformance to the Compliance Rules and preventing Controlled Content that has been unencrypted from copying or unauthorized viewing) should be implemented at a minimum, in a way that they:

(i) Cannot be reasonably foreseen to be defeated or circumvented merely by using general purpose tools or equipment that are widely available at a reasonable price, such as screw drivers, jumpers, clips and soldering irons ("widely available tools"), or using specialized electronic tools or specialized software tools that are widely available at a reasonable price, such as EEPROM readers and writers, debuggers or de-compilers or similar software development tools ("specialized tools"), other than devices or technologies whether hardware or software that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies required ("circumvention devices"); and

(ii) Can only with difficulty be defeated or circumvented using professional tools or equipment (excluding circumvention devices and professional tools or equipment that are made available only on the basis of a non-disclosure agreement), such as logic analysers, chip disassembly systems, or in-circuit emulators or other tools, equipment, methods or techniques not included in the definition of widely available tools and specialized tools in subsection (i) above.

(f) **Advance of technology**: Technological advancements take place at a rapid pace. The RQL has a continuing obligation to ensure that the set-top box content protection security meet the standards set out in the MMCC at all times. If and when necessary, the RQL must cease distribution of set-top boxes which no longer meets the security standards set out in the MMCC and make available new or updated set-top boxes which meet the requisite security standards.

5.7 Summary

5.7.1 In summary, the minimum requirements set out in this section for set-top box content protection security are designed to protect QC within the customer's premises. MDA holds the preliminary view that the RQL's set-top box receiver must decrypt the CPDS-protected QC and then securely manage the output and recording of such content using protected digital outputs and secure recording technologies that are acceptable to content owners. The output and recording of DQC is based on the copy control usage rights conveyed via the CPDS.

5.7.2 The set-top box content protection security requirements set out in this section are based on the Compliance and Robustness Rules defined in the United States cable industry's CableLabs tru2way Host Device License Agreement, which are generally supported by the major U.S. motion picture studios.

6 IMPLEMENTATION AND REVIEW OF PROPOSED GUIDELINES

Compliance Process

6.1 As mentioned in Section 1, MDA proposes to implement the Proposed Guidelines through a certification process, and seeks comments on whether the process should be one of self-certification by the RQL, joint-certification by the RQL and the SQL or independent certification.

6.2 In determining the appropriate certification process, MDA will be guided by the principles that the process should be cost efficient, effective for the intended purpose and easy to implement.

Evolution of Minimum Standards

6.3 MDA proposes to review the Proposed Guidelines every three years as part of the triennial review of the MMCC, or whenever there is sufficient evidence of market development or major technological changes that warrants an interim review.

Implementation Detail

6.4 MDA proposes to implement the Proposed Guidelines by 30 June 2011.

7 REQUEST FOR COMMENTS

7.1 MDA invites the submission of written comments regarding the Proposed Guidelines in the following format:

a) Cover page (including the information specified in paragraph 7.3);
b) Table of contents;
c) Summary of major points;
d) Statement of interest;
e) Comments; and
f) Conclusion.

7.2 Supporting material may be placed in an annex. All comments should be clearly and concisely written, and should provide a reasoned explanation for any proposed revision to the Proposed Guidelines. To the fullest extent possible, parties should identify the specific section on which they are commenting.

7.3 All comments should be made on or before 5pm, 26 May 2011. All comments must be submitted in softcopy (in Microsoft Word format compatible with Microsoft Office Version 2003). Parties submitting comments should include their personal or company particulars, and their correspondence address, contact numbers and email addresses on the cover page of their comments. All comments should be addressed to:

Ms Eileen Ang
Head (Competition and Market Access)
Media Development Authority of Singapore
(Attention: Ruth Wong)
Email: ruth_wong@mda.gov.sg

7.4 MDA reserves the right to make public all or parts of any written comment and to disclose the identity of the source. Commenting parties may request confidential treatment for any part of the comment that the commenting party believes to be proprietary, confidential or commercially sensitive. Any such information should be clearly marked and placed in a separate annex. If MDA grants the request for confidential treatment, it will consider, but it will not publicly disclose, the information. If MDA rejects the request for confidential treatment, it will return the information to the commenting party and will not consider the information as part of its review. As far as possible, commenting parties should limit any request for confidential treatment of information submitted. MDA will not accept any comment that requests for confidential treatment of all or a substantial part of the comment.

Annex A: References

A1	"5C Digital Transmission Content Protection Release 1.0", as amended by the Digital Transmission Licensing Administrator, LLC (DTLA)
A2	CableLabs' tru2way Host Device License Agreement, July 1, 2010
A3	CEA-805-D (November 2008): "Data Services on the Component Video Interfaces"
A4	Content Protected Digital Output License Agreement, December 20, 2005
A5	Digital Transmission Content Protection Adopter Agreement
A6	Digital Transmission Content Protection Specification
A7	EnCentrus Content Protected Digital Output Port System Description, Revision 1.2, January 2006
A8	ETSI EN 300 294 V1.4.1 (2003-04): "Television systems; 625-line television Wide Screen Signalling (WSS)"
A9	High-Bandwidth Digital Content Protection License Agreement
A10	High-Bandwidth Digital Content Protection Specification
A11	"High-Bandwidth Digital Content Protection System, Rev. 2.0 Interface Independent Adaptation" as amended by the Digital Content Protection, LLC (DCP)
A12	IEC 62375 International Standard "Video systems (625/50 progressive) – Video and accompanied data using the vertical blanking interval – Analogue interface"
A13	Motion Picture Association of America Digital Services Content Security Best Practices Version 1.0
A14	Motion Picture Association of America Distribution Content Security Best Practices Version 1.0
A15	Motorola IPRM System Submission of New Digital Outputs and Content Protection Technologies; Revision 2.7
A16	Recording Protection System for Portable extension Technical Specification, Revision 0.92, November 2009
A17	"Specifications of the Macrovision Copy Protection Process for STB/IRD Products" Revision 7.1.S1, October 1, 1999
A18	Video Content Protection System Agreement, September 1, 2004
A19	Vidi System Description Version 1.0, March 2004

Annex B: Glossary of Terms

3DES – 112-bit, triple data encryption standard.

576i (interlace scan) – standard-definition interlaced video usually used in traditionally PAL and SECAM countries.

576p progressive scan outputs – standard progressive video display resolution.

AES – advanced encryption standard, a symmetric-key encryption standard adopted by the U.S. government. The standard comprises three block ciphers: AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analysed extensively and are now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES).

APS – analogue protection system, also known as Copyguard, is a DVD copy prevention system originally developed by Macrovision.

Automatic Gain Control – an adaptive system found in many electronic devices. The average output signal level is fed back to adjust the gain to an appropriate level for a range of input signal levels.

CA – conditional access, the protection of content by requiring certain criteria to be met before granting access to the content.

CAS – conditional access system, a technology used to control access to digital television services to authorized users by encrypting the transmitted programming.

CCI – copy control information, the use of data that is provided within or in addition to media that is used to enable or disable the ability of devices to make copies of media.

CCTV – closed-circuit TV, the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.

CEA-805-D – standard that specifies how data are carried out on analogue component video interfaces and addresses the signal format and data structure of information when carried.

CGMS-A – analogue Copy Generation Management System.

Colorstripe – part of Macrovision's Analogue Copy Protection (ACP) for DVD-Video.

Consensus Watermark – a copy control watermark that has been developed on a multi-industry basis pursuant to a broad consensus in an open, fair, voluntary process, and that has been adopted and is being used by major content providers.

Constrained Image – an image having the visual equivalent of no more than 520,000 pixels per frame (e.g. an image with resolution of 960 pixels by 540 pixels for a 16:9 aspect ratio). A constrained image may be attained by reducing resolution, for example, by discarding, dithering, or averaging pixels to obtain the specified value. A constrained image can be displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image. By way of example, a constrained image may be stretched or doubled, and displayed full-screen, on a 1000-line monitor.

CPDO – the secure digital recording method as specified by EnCentrus Systems, Inc. in its document entitled *EnCentrus Content Protected Digital Output Port System Description*; Revision 1.2 dated January 2006.

CPDS – content protection delivery system, a term used to encompass conditional access security (CAS) systems and digital rights management (DRM) systems.

DQC – decrypted qualified content, a term describing qualified content which is not encrypted in any way.

DRM – digital rights management, a term for access control technologies that can be used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices.

DTCP – method of encryption, decryption, key exchange and renewability that is described in the specification entitled "5C Digital Transmission Content Protection Release 1.0", as amended by the Digital Transmission Licensing Administrator, LLC (DTLA) from time to time.

DVI – digital visual interface, a connection that can transfer a digital video signal from a source component directly to a video display that also has a DVI connection without an analogue conversion.

Displayport – a digital display interface standard put forth by the Video Electronics Standard Association (VESA). It defines a royalty-free, digital audio/video interconnect intended to be used primarily between a computer and its display, or a computer and a home-theatre system.

EEPROM – electrically erasable programmable read-only memory, a type of memory used in computers and other electronic devices to store small amounts of data that must be saved when power is removed, e.g., calibration tables or device configuration.

EMI – encryption mode indicator, allows for a method and system for transferring information.

EPN – encryption plus non-assertion, technology that allows users to make as many copies of their content as they would like.

ETSI EN 300 294 – specifies the wide screen signalling information, the coding and the way of incorporating the coded information into a 625-line system

HDCP – method of authentication, encryption, decryption, and renewability that is described in the specifications entitled "High-Bandwidth Digital Content Protection System" as amended by the Digital Content Protection, LLC (DCP) from time to time.

High definition analogue form – a format or output that is not digital, and has a resolution higher than Standard Definition Analogue Form or Output.

HDMI – high-definition multimedia interface, a compact audio/visual interface for transmitting uncompressed digital data, and an alternative to consumer analogue standards.

ICT – image constraint token, a protocol flag that can cause down-sampling of high-definition video content on Blu-ray and HD DVD to slightly-better-than-DVD quality video.

IEC 62375 – standard for video systems, video and accompanied data using the vertical blanking interval – analogue interface

Internal interface – any internal interconnection not defined as a user-accessible bus and includes, but is not limited to, any signal on a chip bonding pad, JTAG, or other testing point (any place signals move onto and off of a silicon die).

IPRM – IP rights management, in accordance with the Motorola IPRM System Submission of New Digital Outputs and Content Protection Technologies, as amended.

IPTV – Internet protocol television, a process of providing television services through the use of Internet protocol networks.

JTAG – Joint test action group, a type of port initially devised for testing printed circuit boards using boundary scan but more generally can be used as a means of interface with chips.

MAC address – a unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification, and used in the Media Access Control protocol sub-layer.

MPAA – Motion Picture Association of America, a non-profit trade association formed to advance the interests of the movie studios. Its members consist of seven major studios: the Walt Disney Company, Sony Pictures, Metro-Goldwyn-Mayer, Paramount Pictures, Twentieth Century Fox, Universal Studios, and Warner Bros.

MPEG – Moving picture experts group, an asymmetric compression standard for audio and video compression and transmission.

NGNBN – the Next Generation Nationwide Broadband Network, Singapore's next-generation fibre network.

PAL RF – phase alternate line radio frequency, an analogue television encoding system used in broadcast television systems in large parts of the world

RCI – redistribution control information, as defined in CEA-805-D (November 2008): "Data Services on the Component Video Interfaces".

Reprotection – the application of an approved, protection technology, when required, to DQC received from the RQL's service that is to be output from the RQL's STB receiver, and the integrity of the system and methods by which such application is assured.

RGB – an additive colour model based on red (R), green (G), and blue (B) light; RGB is used by computers, televisions, and film recorders to display colours; mixing equal amounts of red, green, blue light will produce white light.

RPSP – the secure digital recording method as specified by Samsung Electronics Co. Ltd, in its document entitled *Recording Protection System for Portable extension Technical Specification*; Revision 0.92 dated November 2009.

SRM – system renewability message data, which is transmitted to set-top boxes, or other devices, using a transport protocol such as an Internet protocol-type data stream.

S-video – Separate Video, an analogue video signal that carries video data as two separate signals: luma (luminance) and chroma (colour).

tru2way – a brand name for interactive digital cable services delivered over the cable video network.

User-accessible bus – a bus which is designed for end-user upgrades or access such as SmartCard, PCMCIA, Cardbus or PCI that has sockets or is otherwise user accessible, but not memory buses, CPU buses and similar portions of a STB receiver's internal architecture.

VGA – Video Graphics Array system, typically implemented as a computer video output that is 640x480 pixels.

VOD – video-on-demand, an interactive TV technology that allows subscribers to view programming in real time or download programs and view them at a later stage.

Y, R-Y, B-Y – the formula used to convert RGB into the various signals used for TV/video. This designation is also found on video equipment to represent analogue component video inputs and outputs, although they are also designated as Y, Pb and Pr (YPbPr). The Y represents the luma (brightness), and B-Y and R-Y represent colour difference signals. For

TV/video storage and transmission, RGB signals are converted to either YUV (NTSC/PAL composite video), YPbPr (component analogue) or YCbCr (component digital).

YUV – the colour encoding system used for analogue television worldwide (NTSC, PAL and SECAM). The YUV colour space (colour model) differs from RGB, which is what the camera captures and what human eye can interpret.

VCPS – Video Content Protection System for recording encrypted content on DVD+RW and DVD+R optical digital media protected by VCPS technology.