secure ▫ enable ▫ interact

Total pages:	10

Doc. Title:	Consultation Paper on Content Protection Security Requirements in support of the Cross-Carriage Measure in the Pay TV Market NDS Comments

Doc. No.:	MDA-TCN-001	**Classification:**	Unclassified
Revision:	1.00	**Restriction:**	Unrestricted
Date:	26 May 2011	**Recipient:**	Media Development Authority of Singapore

Owner:	Paul Jackson	**Reviewers/ Approvers:**	
Author:	Paul Jackson		

Address:	NDS Asia Pacific Ltd 5301 Central Plaza 18 Harbour Road Wanchai Hong Kong
Email:	pjackson@nds.com
Telephone:	+852 2201 9125

Contents

1 Summary of Major Points

NDS regrets that MDA wishes to impose mandatory minimum content protection requirements on current and future Receiving Qualified Licensees, as NDS understands that the minimum content protection requirements may vary considerably depending on the nature and availability through other means of specific content to be cross-carried.

Some local and regional content providers may have content protection requirements for certain content that is considerably more lenient than these, meaning that platforms that wish to carry this content alone will have to invest more than is strictly required by those content providers.

On the other hand, some content providers will undoubtedly have more stringent requirements than these for specific high value, time critical content, and demanding mandatory minimum requirements may tend to set an expectation among RQLs that all content should be made available to them if they meet these minimum criteria.

NDS would prefer that MDA offer these as a "reference" set of requirements, but that content providers and RQLs are free to negotiate more lenient and more stringent requirements for content on a case by case basis, as is the norm elsewhere.

The above comments are not repeated in Section 3 of this document, which contains only NDS's paragraph by paragraph comments and recommendations.

In Section 3 of this document, NDS recommends:

- clarification that content providers remain free to negotiate requirements with SQLs and RQLs for cross carriage of QC
- clarification whether the existing nationwide subscription television service licensees are or will be required to comply with these Requirements, or will be granted "grandfather rights" which exempt them from doing so
- addition of references to DVB / ETSI standards, since one of the existing nationwide subscription television service licensees uses DVB Cable distribution technology, specifically:
    - DVB Common Scrambling Algorithm should be a permissible CPDS content encryption algorithm, and it should be permissible to record and use QC thus protected (which is not DQC) both internally and externally to the set-top box receiver (or IDTV)
    - DVB Content Protection and Copy Management should be a permissible digital output protection mechanism

- self or joint certification for RQLs, with a mechanism to allow content providers to be involved to the extent they wish
- a three year review cycle is too long for rapidly changing technology and threats and an annual review is more appropriate
- developments in piracy and anti-piracy measures that may require changes to the Requirements are best not discussed in public
- certain details of content protection threats and measures, especially in future reviews, may need to be conducted under enforceable non-disclosure agreements with appropriate penalties for improper disclosure
- given these comments alone, the implementation date of 30 June 2011 seems to be too aggressive to be achievable
- the process for collection of comments needs to be revised for the regular and ad-hoc reviews of these Requirements so that parties may request confidential treatment for any proportion of their comments on security concerns without this resulting in rejection of any or all of those comments.

2 Statement of Interest

NDS Group Ltd. creates technologies and applications that enable pay-TV operators to securely deliver digital content to TV STBs (set-top boxes), DVRs (digital video recorders), PCs, mobiles and other multimedia devices.

NDS is a prospective technology, service and application provider to existing and future content providers and pay TV operators in Singapore, including the current nationwide subscription television service licensees likely to be designated Receiving Qualified Licensees (RQLs) and retail service providers (RSPs) on the NIMS platform.

Over 80 of the world's leading pay-TV platforms rely on NDS solutions to protect and enhance their businesses.

VideoGuard® is the world's market-leading conditional access (CA) and digital rights management (DRM) technology, currently deployed on 150 million active devices, and safeguarding pay-TV service revenues exceeding $50 billion.

NDS middleware, including MediaHighway® which enables a host of advanced services for subscribers, has been deployed on 180 million devices.

NDS DVR technology, centred around XTV™, leads the global industry with 38 million units deployed. (Deployment figures as of 31st March 2011).

Headquartered in the UK, NDS is committed to investing in research and development with over 75% of its employees dedicated to pioneering work at development centres in China, France, India, Israel, Korea, the UK and the US.

NDS has within the last year established a Singapore subsidiary, NDS SE Asia Pte Ltd and currently employs well over one third of its total worldwide staff in the Asia Pacific region, with that proportion rising.

NDS has implemented a host of initiatives aimed at reducing its carbon footprint and helping digital TV subscribers reduce energy consumption.

NDS Group Ltd. is a private company owned by the Permira Funds and News Corporation.

Please see www.nds.com for more information on NDS.

3 Comments

Page 2, paragraph 1.6, third sentence

NDS suggests that this sentence is reordered for clarity as follows:

For the avoidance of doubt, SQLs and RQLs continue to be free to negotiate the requirements for carriage of QC, subject to their meeting the minimum requirements set out in the MMCC, since different Content Providers ("CPs") may have different security requirements for carriage of QC.

Pages 2-3, paragraph 1.6, final sentence

It is unclear from this whether the two nationwide subscription television service licensees likely to be designated RQLs have already deployed content protection systems and anti-piracy measures are or will be required to comply with these Requirements, or will be granted "grandfather rights" which exempt them from doing so.

Page 13, paragraph 3.5.7, second sentence

NDS suggests that this sentence is rephrased as follows, as currently it is contradictory:

However, the RQL should not 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). Moreover, the RQL should not neglect to undertake any activity agreed with the SQL that is necessary to preserve such forensic watermarking.

Page 15, paragraph 4.4, first sentence

NDS suggests that this sentence is expanded as follows to include specific reference to the DVB Common Scrambling Algorithm, as used in DVB Cable systems, given that one of the two nationwide subscription television service licensees likely to be designated RQLs currently uses such technology:

The RQL's CPDS should implement the 128-bit Advanced Encryption Standard ("AES") or the DVB Common Scrambling Algorithm 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. The RQL should demonstrate with third-party analysis that its chosen encryption algorithm achieves similar or better security.

Page 17, paragraph 5.1, last sentence

The phrase "decrypted DQC" repeats the term decrypted. Either omit "decrypted" or use "decrypted QC".

Pages 19-21, paragraph 5.5.9, penultimate bullet

Recognising that not all content protection solutions are proprietary and US-originated, specific authorisation should at least be given for the use of DVB Content Protection and Copy Management, which is an open standard.

NDS suggests adding the following bullet:

- The RQL's set-top box receivers may output DQC, and pass DQC to any output in digital form where such output is protected by DVB-CPCM and the Authorised Domain (the set of DVB-CPCM compliant devices which are permitted to consume or store content from that DVB-CPCM protected output) is configured in accordance with the rules set for the specific QC by the relevant CP and securely communicated via the SQL to the RQL and by the RQL to the set-top box (for example, using the CPDS security).

Page 23, paragraph 5.5.16, first bullet, final sentence

As per its comment on paragraph 4.4, to allow for DVB Cable, NDS suggests appending the following additional sentence:

Alternatively, when internally storing QC which has not been decrypted, the QC shall be stored as content encrypted according to the native scrambling algorithm of the CPDS, which may include the DVB Common Scrambling Algorithm.

Page 23, paragraph 5.5.18 (a) and page 24, after paragraph 5.5.23

NDS recommends that MDA describes the approval mechanism and indicative timetable for amendments to add approved technologies mentioned in 5.5.18 (a).

NDS's DVR technology is deployed in over 38 million DVRs worldwide, including pay TV platforms such as DirecTV (US), BSkyB (UK), Sky Italia, Foxtel (Australia), Viasat (Sweden), Sky New Zealand, Astro (Malaysia), Bharti Airtel and Tata Sky (India). All of those DVRs are permitted to record content that is provided by MPAA member content providers – provided that content has been authorised for the individual DVR / subscriber – without any security concerns.

NDS would thus expect to be able to secure approval by MDA within a reasonably short time for an amendment to add its DVR technology and related content protection solutions for ancillary devices within a DVB-CPCM-like Authorised Domain (see comment on 5.5.9), if at some stage these are required.

Page 25, paragraph 5.5.24, clause (a)

As per its comments on paragraph 4.4 and 5.5.16, to allow for DVB Cable, NDS suggests expanding this clause as follows:

(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, or alternatively, when passing QC which has not been decrypted, the QC shall be conveyed and stored as content encrypted according to the native scrambling algorithm of the CPDS, which may include the DVB Common Scrambling Algorithm.

Page 30, paragraphs 6.1 and 6.2

Independent certification is likely to be time consuming and very expensive – particularly since the precise Requirements proposed are unique to Singapore. The Singapore pay TV market, however much it grows, is not going to offer a sufficiently sustainable level of business to any third party that would enable it to benefit from, and pass on the benefit of, meaningful economies of scale for such a certification process.

Self-certification may be appropriate, especially for the existing nationwide subscription television licensees; however, in order to ensure a level playing field, joint certification by the RQL and SQL may be preferable.

Since fundamentally the content providers must be comfortable with the content protection security measures, processes and procedures applied to their content, they should be allowed to be involved in the certification as well, to the extent they wish to be.

Page 30, paragraph 6.3

For fast changing pay TV technology, a regular review cycle of three years is too long. An annual review – however brief it may be – seems more appropriate.

Although the draft Requirements are in the public domain, developments in piracy and anti-piracy measures that may require changes to the Requirements are best not discussed in public. If a previously unnoticed or insignificant vulnerability is exploited or becomes a more significant threat, it is not wise to publicise it while it may still be exploited. Moreover, there should be provision for some more detailed parts of future versions of the Requirements to be protected at very least by enforceable non-disclosure agreements with appropriate penalties for improper disclosure.

Page 30, paragraph 6.4

Given some of the significant technological concerns expressed in this response alone, the implementation date of 30 June 2011 seems to be too aggressive to be achievable.

Page 31, paragraph 7.4, last sentence

While this may be acceptable when dealing with this Consultation Paper, it does not make sense in the context of security reviews, as explained in the second paragraph in the comment above on paragraph 6.3.

If such a restriction were to remain for future reviews of the Requirements, then entirely valid security concerns that a party may not want to disclose publicly would be rejected, unless that party could pad out the response with enough additional comments to ensure that the "confidential" concerns did not form a substantial part of its response.

4 Conclusion

NDS would be pleased to clarify, elaborate on or explain any of these points to MDA and hopes that MDA will take these recommendations into account before issuing its final directive on the matter.

Please do not hesitate to contact the author of this document for further details or discussion on any of its contents.