SDMI Portable Device Specification

Part 1

Version 1.0

Contents

1 INTRODUCTION 4

2 ANTITRUST STATEMENT ON THE SECURE DIGITAL MUSIC INITIATIVE 5

3 DEFINITIONS 6

3.1 LCM (Licensed Compliant Module) 6
3.2 PD (Portable Device) 6
3.3 Version 1.0 PD 6
3.4 PM (Portable Media) 6
3.5 SDMI-Compliant 6
3.6 Content 6
3.7 SDMI Protected Content 6
3.8 SDMI Validated Content 7
3.9 Unknown Content 7
3.10 Authentication (or Authenticate, Authenticated) 7
3.11 SAC (Secure Authenticated Channel) 7
3.12 Protected 7
3.13 SDMI Domain 8
3.14 Local SDMI Environment 8
3.15 Metadata 8
3.16 Check-Out 8
3.17 Check-In 8
3.18 Copy 8
3.19 Move 8
3.20 Usage Rules 9

4 REFERENCE MODEL 10

4.1 Application Layer 10
4.2 Licensed Compliant Module (LCM) Layer 10
4.3 The PD Layer 11
4.4 Architecture Description 12
4.5 Content Flow and Usage Rule Diagram 12

5 SDMI IMPLEMENTATION REQUIREMENTS 14

5.1 Portable Devices (PD) 14
5.2 LCM 16
5.3 SDMI Compliant Applications 18
5.4 Portable Media (PM) 20
5.5 Security 20
5.6 Content provided via EMD 20
5.7 Move and Check-In/Check-Out 20

6 SCREENING 21

6.1 Phase 1 21
6.2 Phase 2 (Informative Text, See Appendix A) 21

7 SDMI COMPLIANCE 23

7.1 Trademark 23
7.2 Authentication 23

8 APPENDIX A — TRANSITION AND SCREENING 24

8.1 Overview of the Call 24
8.2 [Reserved] 25
8.3 Scope 25
8.4 Required Additional Information 26
8.5 Information for Proposers 27
8.6 Implementation Proposals 28

9 APPENDIX B — SDMI QUERY DATA SET EXAMPLE 29

10 APPENDIX C — ROBUSTNESS REQUIREMENTS 30

10.1 General 30
10.2 Methods Of Making Functions Robust 31
10.3 Required Levels Of Robustness 32
10.4 New Circumstances 33
10.5 Examination/Inspection 33

11 APPENDIX D — LIST OF FIGURES 35

1 Introduction

This specification sets forth the requirements for first generation devices that are anticipated to be delivered by the December 1999 holiday season. As a result of the desire to finalize requirements for first generation devices by June 30, 1999, this specification describes devices that are limited in capability. Such devices will play protected SDMI music.

This document is Part 1 of the global SDMI Portable Device (PD)[1] specification. Subsequent parts will describe second generation and beyond Portable Devices, and a generalized framework for SDMI components. It is expected that subsequent versions will provide additional functionality.

[1] Capitalized terms not otherwise defined herein shall have the meanings set forth in Section 3.

2 Antitrust Statement on the Secure Digital Music Initiative

Two points of antitrust law govern the SDMI process:

First, many of the companies participating in this process are competitors of other participants. SDMI is not intended to be, and cannot take the form of, an agreement that limits competition.

Second, the antitrust laws permit, indeed under appropriate circumstances encourage, the creation of neutral standards that benefit the affected industry and consumers.

The SDMI specification is such a standard. Record companies have identified the lack of an open and interoperable standard for security as the single greatest impediment to the growth of legitimate markets for electronic distribution of copyrighted music. Likewise, technology companies developing computer software, hardware and consumer electronics devices that will handle new forms of digital music have realized that an important part of these devices is the presence (or absence) of adequate security for electronic music. The SDMI specification will reflect both the legitimate needs of the record labels for security of digital music and the technical constraints and realistic needs of technology companies. By supporting a wide variety of agreements between rights owners and consumers, such a Specification will enable multiple new and flexible business models to emerge in the marketplace.

Technology companies can reasonably conclude that an SDMI-Compliant product will meet the security needs of record companies and that consumers purchasing such devices will have broad, legitimate access to music. Moreover, the SDMI process has the potential for facilitating broad interoperability between compliant software and electronic devices. Both results create value for consumers.

The end result of the process, however, will be a specification, not an agreement. Each music company, and indeed each participant, will make its own decision as to the degree of security it finds acceptable in light of marketplace conditions and each technology company will decide whether and the extent to which it incorporates the SDMI specification in its designs.

3 Definitions

Unless otherwise noted, references to SDMI-Compliant components refer to compliance with this Version 1.0 specification.

3.1 LCM (Licensed Compliant Module)

An SDMI-Compliant module that interfaces between SDMI-Compliant applications and SDMI-Compliant devices, media and components.

3.2 PD (Portable Device)

A device that stores on internal or Portable Media (PM) SDMI Protected Content received from an LCM residing on a client platform. A PD does not include an LCM.

3.3 Version 1.0 PD

An SDMI-Compliant PD that has limited functions and is intended primarily to perform playback of SDMI Protected Content through an analog output.

3.4 PM (Portable Media)

SDMI-Compliant portable media that may be used to store SDMI Protected Content.

3.5 SDMI-Compliant

A device, application or any other implementation that conforms to the requirements of this specification including the Robustness Requirements attached hereto as Appendix C.

3.6 Content

Digital audio and, if present, related data (e.g., text, graphics, video, Metadata, etc.).

3.7 SDMI Protected Content

Content made accessible only in accordance with the requirements as set forth in this specification. Within the SDMI Domain, such Content shall be accessed only by SDMI-Compliant devices or components. Such Content may be for distribution or for local use:

3.7.1 SDMI Protected Content for Distribution

Content that has the following attributes:

- It is Protected;
- It is authorized for distribution by the Content owner or Usage Rules;

- It has rules embedded, associated and/or attached in a Protected manner;
- It may be watermarked;
- It may be accompanied by a non-encrypted header;
- In the case of electronically distributed Content, it is traceable back to the unique distributor (e.g., by a digital signature, watermark or other means to be specified by SDMI).

3.7.2 SDMI Protected Content for Local Use

Content that has the following attributes:

- It is Protected such that it is not accessible outside the Local SDMI Environment.
- It is not authorized for distribution by the Content owner or Usage Rules.
- It has rules embedded, associated and/or attached in a Protected Manner.
- It may be watermarked.
- It may be accompanied by a non-encrypted header.

3.8 SDMI Validated Content

Content that has successfully passed through an SDMI Compliant Phase 1 Screen as described in this specification but which has not yet become SDMI Protected Content. Content that has been transferred outside the SDMI Domain is no longer SDMI Validated Content.

3.9 Unknown Content

Content that has not yet been screened by an SDMI Compliant Phase 1 Screen as described in this specification.

3.10 Authentication (or Authenticate, Authenticated)

For purposes of this specification, a cryptographic process ensuring that only components which are currently SDMI-Compliant (i.e., not revoked, see Section 7.2[2]) can interoperate either:

- Explicitly by an active cryptographic process typically involving challenge/response protocols against a private key, or
- Implicitly by a cryptographic process, such that the interoperation of SDMI-Compliant non-revoked components is achieved indirectly by the result of another cryptographic process, such as key derivation.

3.11 SAC (Secure Authenticated Channel)

Protected and Authenticated communication between two or more SDMI-Compliant components.

3.12 Protected

State in which unauthorized access is restricted by technical means (e.g., encryption or scrambling).

[2] All section references in this document are references to other sections of this specification.

3.13 SDMI Domain

The environment in which all SDMI rules and behaviors shall be obeyed. This includes, but is not limited to, SDMI-Compliant:

- Screening components;
- Applications, trusted delegates, interfaces, PDs, PMs and LCMs;
- SDMI Usage Rules interpreters (see Figure 3);
- Tools for preparing SDMI Protected Content.

3.14 Local SDMI Environment

A subset of the SDMI Domain from which no Content may be copied, exported or moved, except for:

- SDMI Validated Content,
- SDMI Content Protected for Local Use as provided for by the Content's Usage Rules.

In the case that the Content is Copied/Moved onto a PM, the Content shall be Protected in accordance with the rules set forth in Section 5.4.1 of this specification.

3.15 Metadata

A structured description of Content elements, their relationship, form, related usage rules, obligations and/or options. Metadata may be embedded in or otherwise associated with Content in a Protected manner.

3.16 Check-Out

The process by which the ability to render SDMI Protected Content for Local Use is copied via the LCM to a single other location within the Local SDMI Environment and the number of permitted copies is decremented by one.

3.17 Check-In

The process by which the ability to render SDMI Protected Content for Local Use is restored via the LCM to its original location within the Local SDMI Environment and the number of allowed copies is incremented by one. The Checked-Out copy shall then be rendered unusable.

3.18 Copy

The process of replicating Content from one location to another.

3.19 Move

A "Move" is deemed to occur when SDMI Protected Content for Distribution is copied to its destination, and the original is made permanently un-usable in an atomic operation.

3.20 Usage Rules

Rules expressed by Content providers that govern the Content's use in the SDMI Domain. For example, Usage Rules include rules governing Copy (including number of copies/generations of copies permitted), Move, Check-in/Check-out (including number of useable copies), export from the SDMI Domain, and combinations thereof. Usage Rules shall be embedded, attached and/or associated with its Content in a Protected manner. Usage Rules include default rules (see Sections 5.3.2 and 5.1.2.2.2).

4 Reference Model

Figure 1 provides a view of the functional layers of the reference model for this specification. The actual manner of implementation of these requirements is not described in this specification and is instead left to the discretion of individual implementers. The reference model consists of three layers:

4.1 Application Layer

The application layer is where all SDMI-Compliant electronic music distribution applications, software players, home library software applications, CD extractors and other applications reside.

In this reference model, digital rights management and Phase 1 (see Section 6) and Phase 2 screening (see Appendix A) occur in the application layer but an application may use any trusted delegate (including, but not limited to, an LCM) for any task prescribed for applications within this specification. (SDMI restrictions on inter-application communication are provided in Section 5.3.)

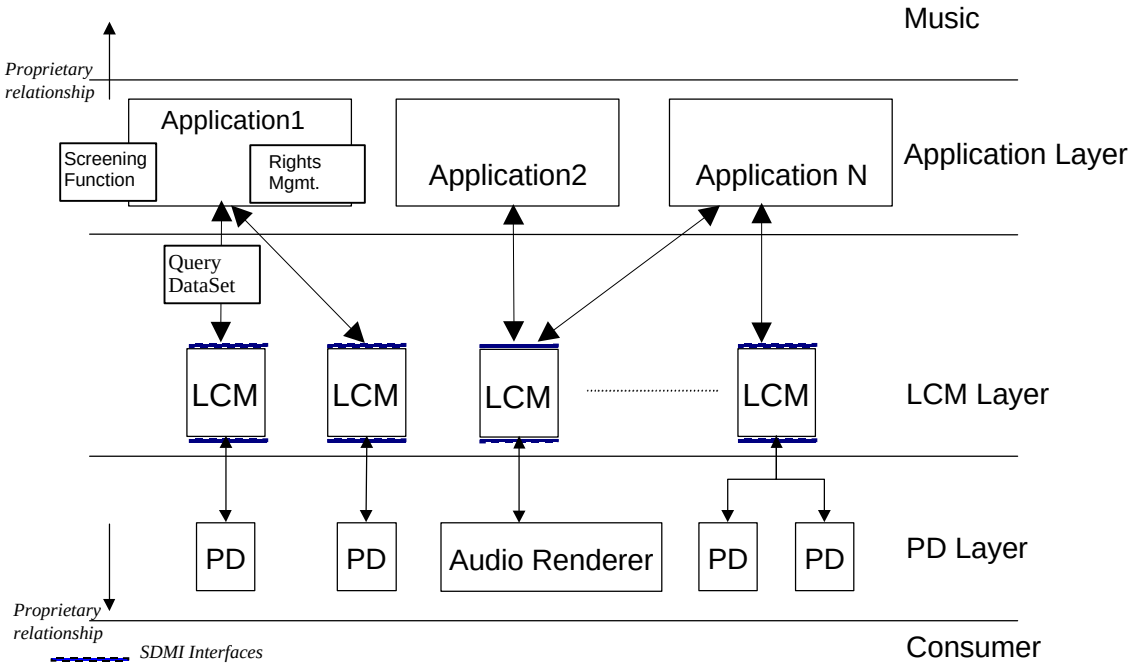


Figure 1: Reference Model Functional Layers[3]

4.2 Licensed Compliant Module (LCM) Layer

The LCM is the module that transfers Content from SDMI-Compliant applications to PDs and PMs (hereafter, "PD" unless otherwise specified) that use one or more formats. In the case where there is

[3] In the event of any conflict between the textual provisions of the specification and the diagrams included herein, the provisions set forth in the text shall control.

a PD format that the application cannot interpret, the LCM may serve the role of a trusted translator, so that SDMI applications are not required to communicate directly with all PD formats.

As depicted in Figure 1, it is anticipated that an application may communicate with multiple LCMs. A single LCM may also communicate with multiple applications. One important function of an LCM is to provide an abstracted device interface to SDMI applications for PDs/PMs. (For illustration, as viewed from the application layer, the LCM is in effect a *virtual portable device.)*

4.3 The PD Layer

The PD layer receives only Protected Content from the LCM-PD interface (i.e., a SAC), including transfer of Content to the PD from a PM. The PD layer constitutes the playback component of the PD reference model as depicted below in Figure 2, which allows for multiple PD formats. Section 5.1 of this specification describes the requirements applicable to the PD layer.

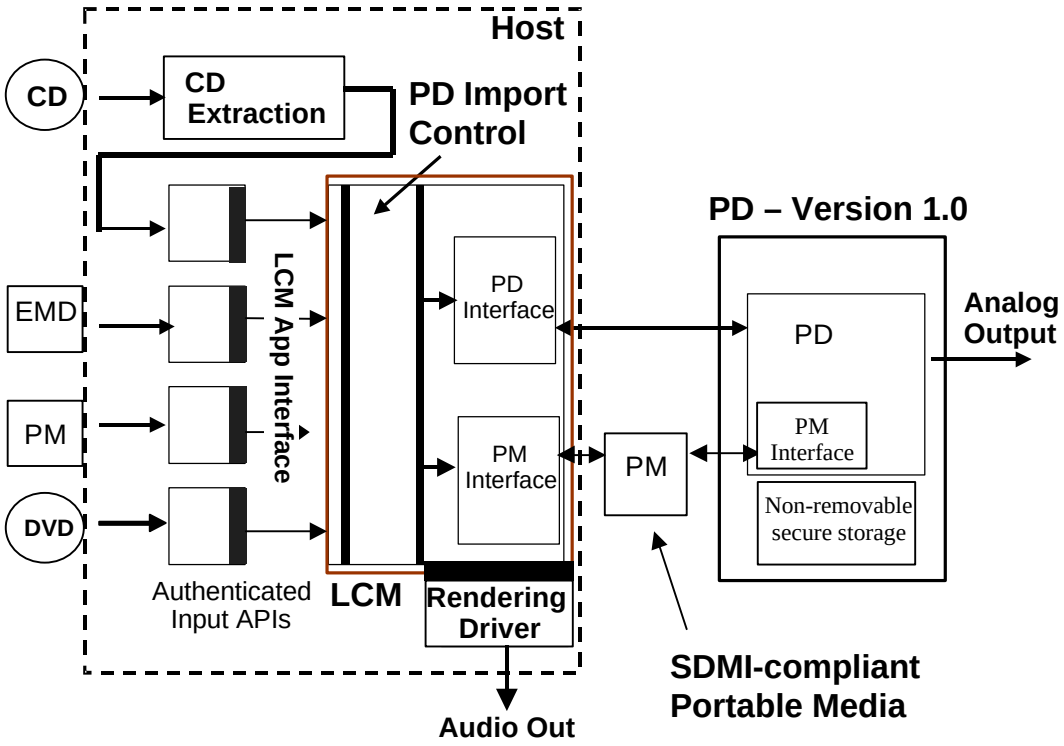


Figure 2: Version 1.0 Functional Reference Model[4]

[4] Note: In this example the terms CD and DVD are used for purpose of illustration and the term CD refers to Redbook CD. In addition, not all features are illustrated nor are all those shown required to be implemented by a particular PD/LCM.

4.4 Architecture Description

The reference model in Figures 1 and 2 represents a PD that communicates with a client platform via a proprietary (device specific) secure interface or via SDMI-Compliant PM. The client platform supports an LCM. An LCM may be embedded in a music management application. The LCM supports one or both of the following two device-side interfaces: one for communication with SDMI-Compliant PM to be used in the PD and another for direct communication with the PD.

Version 1.0 PDs may perform analog playback of SDMI Protected Content. For this functionality, the PD shall support at least one codec and shall interface with an LCM that is responsible for Content management (e.g., key management, content decryption, etc.). The functionality and requirements for these PD components are described in Section 5.1.

The LCM provides the means by which SDMI-Compliant applications interface with SDMI-Compliant Version 1.0 PDs. The LCM contains a PD import module that is responsible for all communication between the application and the LCM domain, including supporting application queries about PD or PM capabilities. The interface between the application and the LCM shall be Authenticated and for some types of applications, as defined in this specification, this communication shall also be Protected.

This specification provides application builders with requirements for developing applications that are SDMI-Compliant. This specification requires a SAC to all LCMs for all such applications. Application builders may provide transcoding, transcryption (translation from one encryption method to another) and music management in their applications. This is subject to the requirements of this specification, including Usage Rule management. This specification supports, in a completely modular way, CD extracting, existing electronic music distribution (EMD) applications, future SDMI EMD applications as well as SDMI-Compliant transcoding and formatting[5] applications. It also supports output from the LCM to SDMI-Compliant PDs/PMs for audio rendering.

4.5 Content Flow and Usage Rule Diagram

This reference diagram illustrates *one possible example implementation* of an SDMI application as described in this specification. Arrows indicate allowed content pathways. Boxes represent specific functions and are not necessarily individual components in a particular implementation. SDMI-Compliant applications may perform any of the behaviors shown, provided they conform to this specification.

[5] Note: "Formatting" does not imply a standardized file format.

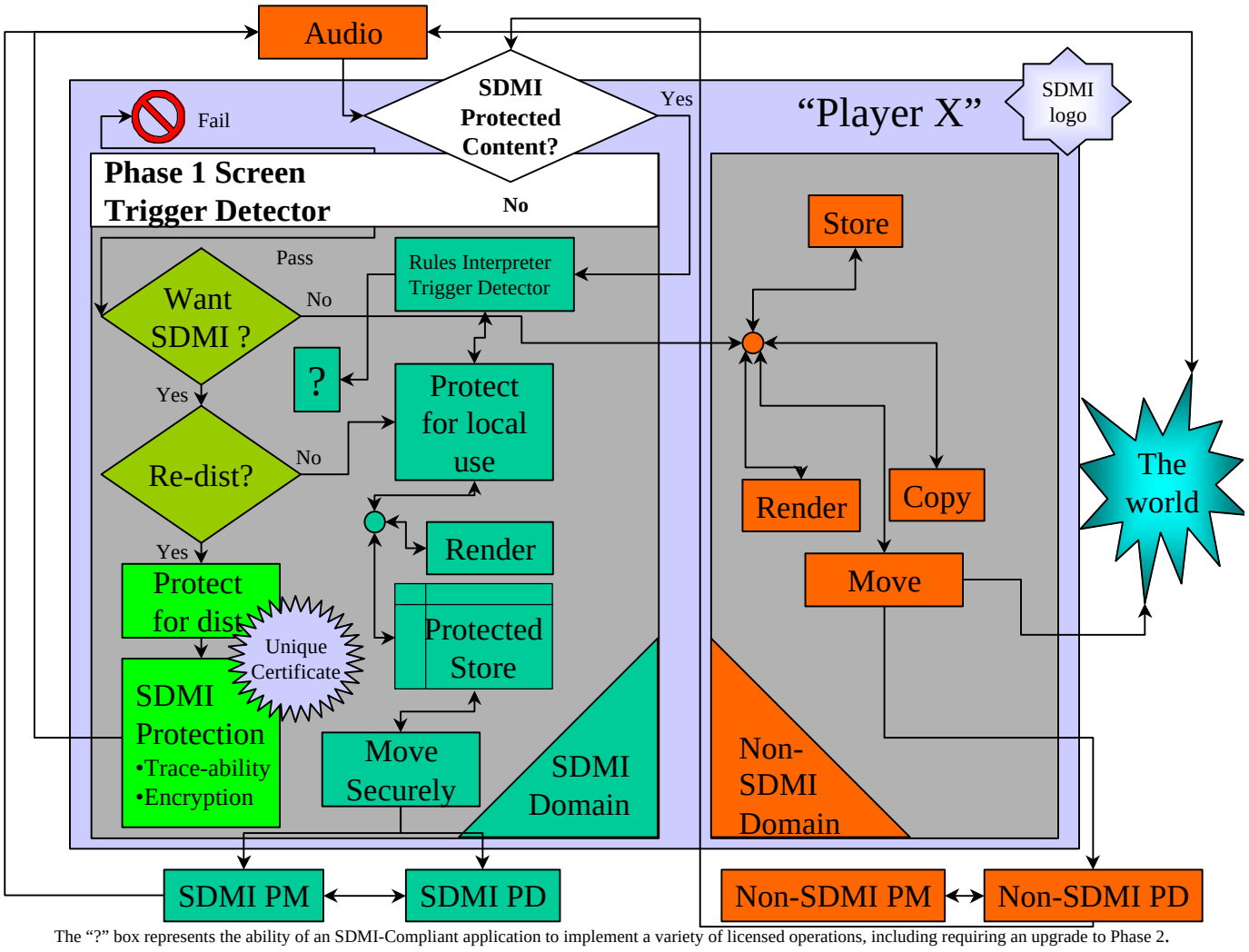


Figure 3: Content Flow and Usage Rule Diagram

5 SDMI Implementation Requirements

5.1 Portable Devices (PD[6])

5.1.1 General Requirements

5.1.1.1 A PD shall not include an LCM.

5.1.1.2 Any Content stored on the PD shall be SDMI Protected Content.

5.1.1.3 PDs shall not violate Content Usage Rules.

5.1.1.4 For Portable Media (PM) input, the PD shall verify that the Content is SDMI Protected Content.

5.1.1.5 If the LCM needs to receive information from the PD about the PD's capabilities, the PD shall support means for the LCM to receive such information.

5.1.2 Input to PD

5.1.2.1 SDMI Protected Content

5.1.2.1.1 A PD shall accept SDMI Protected Content only from an LCM or PM.

5.1.2.2 Embedded Microphone

5.1.2.2.1 A PD may accept analog input from a microphone embedded in the PD, provided that the Content is immediately converted to SDMI Protected Content for Local Use.

5.1.2.2.2 In order to export embedded microphone Content from the SDMI Domain, such Content shall be required to pass the screen. The default rule for such Content is that it may be exported from the SDMI Domain.

5.1.2.2.3 This input will be restricted to mono voice-grade and band-limited (-3 dB at 100 Hz and –60 dB at 8 kHz).

5.1.2.3 Unprotected digital and analog Input

All Content received from unprotected digital and analog inputs shall be screened within the PD.

[6] Note: Unless otherwise indicated, all references to the term "PD" shall mean "Version 1.0 PD".

5.1.3 Output from PD

5.1.3.1 Analog Audio Output

Analog output is permitted as follows:

5.1.3.1.1 Playback

Any playback at a rate higher than 1.5 times normal speed shall be noticeably degraded unless the pitch is corrected to the pitch at the normal speed.

5.1.3.1.2 Seek

If the audio rendered during a seek operation is reproduced at a rate greater than normal speed, then the quality of the audio shall be noticeably degraded.

5.1.3.2 Unprotected Digital Output

Unprotected digital output of Content shall not be allowed from Version 1.0 PDs.

5.1.4 Identification Requirements for PD and PM

5.1.4.1 If Content is bound to a PD and/or a PM, the PD and/or the PM shall have an ID that shall be:

- Readable by the LCM and the PD;
- Statistically or truly unique across all devices or components for a given manufacturer;
- A minimum length of
  - 128 bits, if randomly assigned or
  - 32 bits, if uniquely assigned by an appropriate assignment authority or licensor designated by SDMI;

and

Security shall not be dependent on the secrecy of this ID.

5.2 LCM

5.2.1 General Requirements

5.2.1.1 The LCM shall not violate Content Usage Rules.

5.2.1.2 The LCM shall deliver Content to the PD or PM in an Authenticated and Protected manner in accordance with the Robustness Requirements applicable to Version 1.0 PD's.

5.2.1.3 The LCM shall Authenticate the PD. If an LCM hosts multiple PDs, it shall Authenticate them individually.

5.2.1.4 Where the LCM is not contained in the application, the LCM shall Authenticate SDMI-Compliant applications.

5.2.1.5 If an LCM performs any screening function it shall do so in accordance with Section 6.

5.2.2 LCM Security Criteria

5.2.2.1 Inputs and Outputs

The LCM shall not transfer or permit transfer of Content to or from a non-SDMI-Compliant application or PD/PM except for transfer of SDMI Validated Content or where allowed by Usage Rules.

5.2.2.2 LCM Authentication

The LCM shall Authenticate itself to both SDMI-Compliant applications and to SDMI-Compliant PDs prior to executing any function that requires a SAC.

5.2.2.3 Non-SDMI Devices and Applications

LCMs shall not facilitate interoperability between SDMI-Compliant applications and non-SDMI-Compliant applications except for transfer of SDMI Validated Content or where allowed by Usage Rules.

5.2.2.4 Unknown Content

LCMs shall only operate on Unknown Content for the purpose of screening.

5.2.2.5 Content Transfer to PD or PM

LCMs that transfer SDMI Protected Content to a PD or PM shall be permitted to do so only as specified in Sections 5.1 and 5.4 of this specification.

5.2.3 Secure Authenticated Channel (SAC) Requirements

5.2.3.1 Communication of SDMI Protected Content between SDMI-Compliant applications, LCMs and PDs shall be Authenticated and Protected. This includes communication through a PM.

5.2.3.2 Access to Content transferred via the SAC shall be Protected at all times and shall be in accordance with the Robustness Requirements.

5.2.3.3 Content Usage Rules shall be linked persistently to the Content, implicitly or explicitly.

5.2.3.4 Local compromise of any component shall not result in global compromise of the SDMI Domain subject to the provisions of the Robustness Requirements.

5.2.4 PD Import Control and Associated Interfaces

The PD import control includes a collection of proprietary modules that implement the PD/PM interface. It shall adhere to the requirements set forth in subsections 5.2.4.1.1 through 5.2.4.1.8.

5.2.4.1 LCM-Application Interface

The LCM-application interface enables an SDMI-Compliant application to determine the capabilities of the PD/PM. Use of this interface to determine such capabilities does not require the establishment of a SAC, but the actual use of such capabilities does. The interface:

5.2.4.1.1 Shall support enumeration of the codec(s) supported by PD(s).

5.2.4.1.2 Shall support enumeration of content protection mechanisms supported by PDs (e.g., cryptographic algorithms).

5.2.4.1.3 Shall expose the characteristics of the storage media (e.g., contains media ID, removable, writeable, etc.). Specifically, it shall expose the characteristics of the storage media required pursuant to Section 5.4 of this specification relating to PM.

5.2.4.1.4 Shall support enumeration of transcoding and transcryption capabilities if present.

5.2.4.1.5 Shall expose the memory and storage capacity of PD(s).

5.2.4.1.6 Shall expose the input and output capabilities of PD(s).

5.2.4.1.7 Shall support enumeration of the usage rules that the PD(s) are able to support.

5.2.4.1.8 May support all of these capabilities through a single data structure such as the Query Data Set Example set forth in Appendix B.

5.2.4.2 File and Content Management Interface

The LCM may perform transcoding, transcrypting, and mapping of Usage Rules of the source Content to the corresponding functionalities of the PD.

5.2.4.2.1 File Management Interface

The interface for transferring Content from an application to the PD shall be done via the LCM using a SAC in a manner that does not violate the Usage Rules.

An interface that supports copying, moving and deleting SDMI Protected Content files on a PD/PM shall do so in a manner that does not violate the Usage Rules associated with the Content.

5.2.4.2.2 Content Management Interface

This interface supports transcoding, transcrypting, file formatting and/or rules mapping. Its implementation shall not violate the Usage Rules associated with the Content.

If an application determines via the LCM that it cannot directly support a given PD/PM, the application may use the LCM to perform transcoding, transcrypting, file formatting and/or rules mapping of the Content for transfer to the PD/PM.

5.3 SDMI Compliant Applications

5.3.1 SDMI-Compliant applications shall not violate the Content Usage Rules.

5.3.2 SDMI Default Usage Rules

When Content that does not include Usage Rules is converted to SDMI Protected Content for Local Use, the following default rules shall apply:

The Local SDMI Environment shall contain no more than four usable copies. Three of these copies may be transferred to PDs/PMs.

5.3.3 SDMI-Compliant applications shall Authenticate other applications or LCMs receiving SDMI Protected Content.

5.3.4 Unless allowed by the Content Usage Rules, an application shall not transfer any Content outside the SDMI Domain, other than SDMI Validated Content or Content that originates from a PD embedded microphone that has passed the screen (see Section 5.1.2.2).

5.3.5 Any Content transfer within the SDMI Domain shall be done in a Protected manner. SDMI-Compliant applications shall not act on or transfer Content to other SDMI-Compliant applications or LCMs unless the Content:

- is SDMI Validated Content, or
- has been determined to be SDMI Protected Content for Local Use, or
- has been determined to be SDMI Protected Content for Distribution.

5.3.6 If SDMI-Compliant applications contain a screen they shall be subject to all of the rules in Section 6.2 relating to screening.

5.3.7 Playback for Listening

An SDMI-Compliant application may render Content for local use at normal speed for the user's immediate consumption.

5.4 Portable Media (PM)

5.4.1 PM Types and Binding Requirements

5.4.1.1 SDMI Protected Content shall be Protected in such a way that duplication of such Content shall be restricted according to the related Usage Rules and in accordance with the Robustness Requirements.

5.4.1.2 If the PM has an ID, the SDMI Protected Content shall either be bound to the PM and/or to other allowable IDs in accordance with Section 5.1.4 on IDs.

5.4.1.3 If the PM has no ID, the SDMI Protected Content shall be bound to another ID in the Local SDMI Environment.

5.5 Security

5.5.1 SDMI components shall comply with the Robustness Requirements.

5.5.2 Content originating from EMD sources shall remain Protected to the degree prescribed by the EMD Usage Rules and in accordance with the Robustness Requirements.

5.6 Content provided via EMD

Content delivered via EMD to SDMI-Compliant components shall be traceable back to its unique distributor (e.g., by a digital signature, watermark or other means to be specified by SDMI).

5.7 Move and Check-In/Check-Out

5.7.1 Move

A Move shall be permitted only with respect to SDMI Protected Content for Distribution.

5.7.2 Check-Out to PD/PM and Check-In from PD/PM

- Check-out is permitted provided the number of remaining permitted copies is greater than 0.
- The number of simultaneously usable copies in existence at any given time shall not exceed the number permitted by the Usage Rules.
- Check-In/Check-Out shall be permitted only with respect to SDMI Protected Content for Local Use.

5.7.3 Migrate

Content that originates from the analog input or the unprotected digital input (screened by the PD, see Section 5.1.2.3) may be imported from the PD/PM into the LCM in accordance with the screening rules set forth in Section 6.

6 Screening

The screening technology is specified in two Phases to expedite the time to market of SDMI Compliant components, while allowing such components to be voluntarily upgraded in the future to require the use of the copy protection technologies that will be incorporated in the Phase 2 screen. The Phase 1 screen is only capable of detecting the "*upgrade to Phase 2 trigger*" and is fully specified in Section 6.1. The Phase 2 screen is a more comprehensive solution and will be specified in later specifications. When used in conjunction with Content that has been packaged with the Phase 2 mark, it is expected that the Phase 2 screen will at a minimum determine if such Content has been previously compressed. This capability enables the Content provider to mark such Content as "*do not admit to the SDMI Domain if this Content has been previously compressed.*"

6.1 Phase 1

Content arriving at a Phase 1 Screen shall go through the following steps:

1. If the Content is SDMI Protected Content, then search for trigger.

   - If the trigger *is* present, the Content shall be rejected and an upgrade message to Phase 2 shall be generated. (Only after a successful upgrade of the screen, will Content with a trigger be admitted into the SDMI Domain, as described in Section 6.2.)

   - If the trigger *is not* present, the Content is admitted into the SDMI Domain.

2. If the Content is *not* SDMI Protected Content,

   - If the trigger *is* present, the Content shall be rejected and an upgrade message to Phase 2 shall be generated. (Only after a successful upgrade of the screen, will Content with a trigger, having passed the Phase 2 screen, be admitted into the SDMI Domain, as described in Section 6.2.)

   - If the trigger *is not* present, the Content is admitted into the SDMI Domain.

3. It is expected that screening technology will also be capable of detecting embedded Usage Rules information in Content. If such technology exists (and is specified by SDMI pursuant to the Call for Proposals contained in Appendix A) and such information is present, the embedded Usage Rules shall be obeyed.

6.2 Phase 2 (Informative Text, See Appendix A)

In order to prevent unauthorized reproduction/use, it is *expected* that under Phase 2 the screen will, at a minimum, provide the following functions:

1. If the Phase 2 mark *is* present, and the Content has been previously compressed:

- And it was not supposed to be compressed, reject the Content
- Otherwise admit the Content into the SDMI Domain.

2. If the Phase 2 mark *is not* present, admit the Content into the SDMI Domain.

7 SDMI Compliance

7.1 Trademark

Companies that wish to use SDMI trademarks to indicate compliance with this specification will be required to sign a license agreement relating to the use of the mark. The terms of such license agreement shall be approved by the SDMI Foundation and the SDMI Plenary and will include provisions relating to, among other things, the compliance of such companies' implementations with the specification, including the Robustness Requirements attached hereto as Appendix C, and rules for the enforcement of the license agreement.

7.2 Authentication

Authentication arrangements shall be consistent with the requirements set forth in this specification. For purposes of this PD specification, and until such time as such a specification for Authentication is complete, the details of authentication (and any arrangement for revocation of authentication) shall be the subject of individual arrangements between suppliers of SDMI Protected Content (such as via EMD) and manufacturers of SDMI-Compliant products and services.

8 Appendix A — Transition and Screening

This Appendix A contains the "Call for Proposals for Technology Solutions to Screen Digital Audio Content for LCM Acceptance" that was issued by SDMI on 5th May 1999.

PDWG London May 05, 1999	SDMI SECURE DIGITAL MUSIC INITIATIVE	APPROVED PDWG99050504-TransitionCfP

Call for Proposals for Technology Solutions to Screen Digital Audio Content for LCM Acceptance

8.1 Overview of the Call

This document is a call for proposals ("CfP") for technology for the part of the LCM that determines acceptability of digital audio content entering the Licensed SDMI Compliant Module ("LCM") for conversion (within the LCM) into SDMI compliant formatted content for local use. Local use refers to Content, the use of which is bound, e.g., to the LCM or a connected portable device ("PD"). This CfP describes a technology that screens for local use (see Figure 1), but the technology could be used or might have to be compatible with technology that screens for network distribution. (See Appendix A.)

8.1.1 Antitrust Statement on the Secure Digital Music Initiative

Two points of antitrust law govern the SDMI process:

First, many of the companies participating in this process are competitors of other participants. SDMI is not intended to be, and cannot take the form of, an agreement that limits competition.

Second, the antitrust laws permit, indeed under appropriate circumstances encourage, the creation of neutral standards that benefit the affected industry and consumers.

SDMI is such a standard. Record companies have identified the lack of an open and interoperable standard for security as the single greatest impediment to the growth of legitimate markets for electronic distribution of copyrighted music. Likewise, technology companies developing computer software, hardware and consumer electronics devices that will handle new forms of digital music have realised that an important part of these devices is the presence (or absence) of adequate security for electronic music. The SDMI standard will reflect both the legitimate needs of the

record labels for security of digital music and the technical constraints and realistic needs of technology companies. By supporting a wide variety of agreements between rights owners and consumers, such a Specification will enable multiple new and flexible business models to emerge in the marketplace.

Technology companies can reasonably conclude that a SDMI compliant product will meet the security needs of record companies and that consumers purchasing such devices will have broad, legitimate access to music. Moreover, the SDMI process has the promise of facilitating broad interoperability between compliant software and electronic devices. Both results create value for consumers.

The end result of the process, however, will be a standard, not an agreement. Each label will make its own decision as to the degree of security it finds acceptable in light of marketplace conditions and each technology company will decide whether and the extent to which it incorporates the SDMI standard in its designs.

8.2 [Reserved]

8.3 Scope

Figure 1 shows an overview of one possible configuration of the portion of the LCM that manages and processes audio. The scope of this CfP is limited to the functionality identified by the decision diamond labeled “Screen.”

A.1.1. Phase 1 Screen

Phase 1 Screens determine the presence of unremovable data indicating that:

- The content cannot be accepted by the LCM without upgrading to an LCM with a Phase 2 Screen.
- Content is marked “no more copies,” (e.g., DVD-Audio).

8.3.1 Phase 2 Screen

Phase 2 Screens determine the presence of unremovable data indicating that:

- The content is marked “do not copy if this content is or has been compressed,” and the content, in fact, is or has been compressed; and,
- The content is marked “no more copies,” (e.g., DVD-Audio).

Technologies that are able to identify unauthorized reproduction by methods other than detecting unauthorized compression, e.g., via distribution of PCM files, are also invited.

8.3.2 The Phase 2 technology may replace the Phase 1 technology. However, backward compatibility with the Phase 1 "no more copy" identifier technology solution will be necessary.

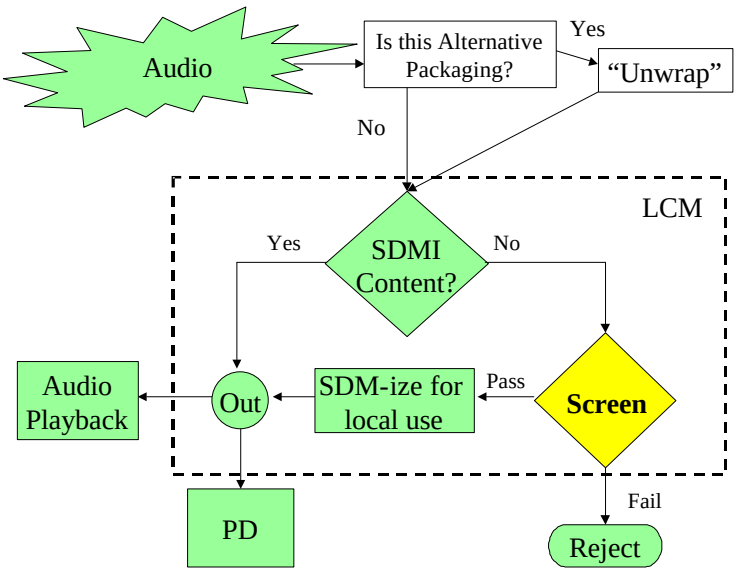


Figure 1

8.3.3 It is expected that watermark technologies will be used in connection with physical disks such as DVD-Audio and Super Audio CD. Interoperability of the Proposer's technology with other security technologies will therefore highly desirable.

8.4 Required Additional Information

Responses to the CfP are required to provide the following information:

8.4.1 Contact information including: company name, name of contact person or persons, title(s) telephone number, facsimile, mailing address, and email address.

8.4.2 Availability of the proposed technology solution:

8.4.2.1 Phase 1 Screen proposed technology shall be available for implementation in connection with the PDWG specification to be completed on June 30, 1999. Proposers shall include detailed information confirming the availability for implementation of the technology solution in that time frame.

8.4.2.2 With respect to the Phase 2 Screen proposed technology, the speed with which it will be available for implementation will be a critical evaluation factor.

8.4.2.3 Information about the availability of samples, commercialization and exportability of the technology solution shall be provided.

8.4.2.4 Information about the gate count, processing power and memory requirements shall be provided.

8.4.3 Material terms and conditions (including pricing structure) on which the technology solution will be licensed shall be described in detail. In addition, Proposers are encouraged, but not legally obligated, to provide information concerning intellectual property rights of third parties that may be applicable to the technology solution proposed.

8.4.4 Both the method for applying the unremovable data in the content, and the method for detecting its presence within the Screen shall be described.

8.4.5 The preferred and possible alternative implementations of the technology solution shall be described.

8.4.6 Methods by which the security of the technology (for both encoding and decoding) will be maintained shall be described. The process by which licensing and access to the technology are managed shall be described. In addition, Proposers shall submit information describing and analysing how to minimize the risks from the Screen being a "single point of failure."

8.4.7 Plans for technical support and any associated costs shall be described.

8.4.8 Technical information shall be provided, to the extent available, with respect to the evaluation criteria set forth in Section 6 below.

8.5 Information for Proposers

8.5.1 Key technical factors likely to be considered include that the method of indication and/or detection be:

8.5.1.1 inaudible;

8.5.1.2 robust (i.e., that it will survive compression, transcoding and other transforms);

8.5.1.3 tamper resistant;

8.5.1.4 reliable, e.g., no false positives;

8.5.1.5 readable without decompressing the file;

8.5.1.6 renewable;

8.5.1.7 easy to implement;

8.5.1.8 commercially practicable;

8.5.1.9 efficient to implement (i.e., computational requirements);

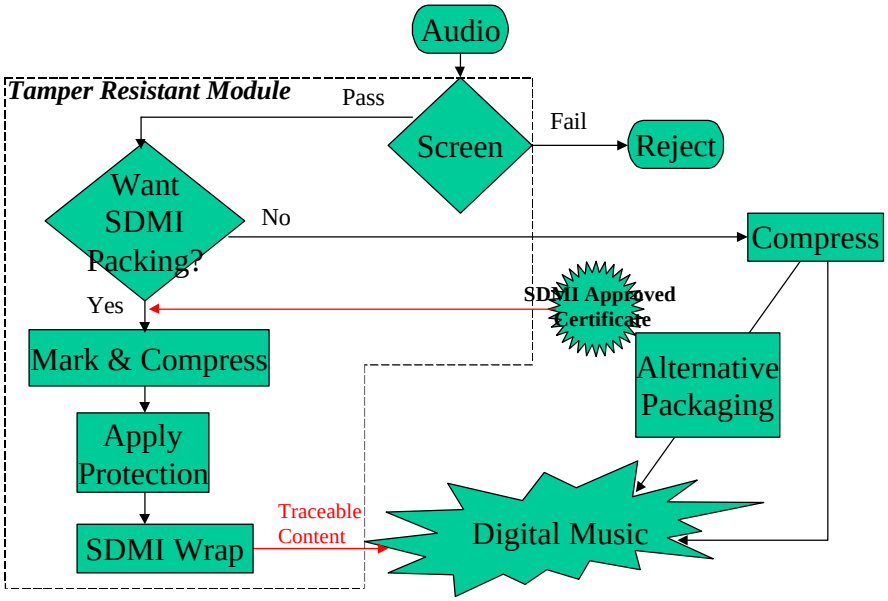
8.5.1.10 should not significantly affect the ability to compress the content; and

8.5.1.11 the analysis of *threat scenarios* in the implementation and maintenance of the Screen technology.

8.6 Implementation Proposals

Responses to this call for proposals are due no later than 2359 hrs PDT on May 23, 1999. All proposals will be posted on the restricted members portion of the SDMI website for review. Should subsequent rounds relating to this CfP be required, they shall be open only to Proposers who submit by the May 23 deadline. In addition, Proposers should be aware that they may be asked to provide additional information concerning intellectual property rights pursuant to a provision to be addressed at the next SDMI Plenary.

The responses to this CfP are to be sent to sdmi@globalintegrity.com. Acceptable formats are zipped archives of Word6, Word7, PDF or HTML documents.



9 Appendix B — SDMI Query Data Set Example

If the LCM supplies an interface for applications the following example suggests a structure for a query data set to allow applications to discover the LCM and its capabilities

```
<DD>
      <Identification>
         <Name>   </Name>
         <Manufacturer Name> </Manufacturer Name>
         <SDMI Manufacturer ID> </SDMI Manufacturer ID>
         <Version> </Version>
         <Date> </Date>
      </Identification>

      <Device>
         <Identification>
            <ID> </ID>
            <Type> </Type>
         </Identification>

         <Codec>
            <Name> </Name>
            <Version> </Version>
         </Codec>
      </Device>

      <Security>
         <Certification>
            <Cert> </Cert>
            <Type> </Type>
            <Issuing Authority> </Issuing Authority>
         </Certification>
      </Security>
</DD>
```

10 Appendix C — Robustness Requirements

10.1 General

10.1.1 Scope

These Robustness Requirements apply to implementations ("Implementations") of the SDMI Portable Device Specification, Part 1, Version 1.0 (the "Specification") and are incorporated in the Specification. Capitalized terms not defined herein shall have the meanings set forth in the Specification.

10.1.1.1 Objective

Implementations shall protect SDMI Protected Content against unauthorized access, copying and distribution. Implementations shall maintain SDMI Protected Content in a protected state or a protected environment at all times except while such Content is being rendered in decompressed form.

10.1.2 Construction

Implementations shall comply with the Specification and be designed and manufactured so as to effectively frustrate attempts to modify such products so as to defeat the functions of the Specification, as more specifically described below.

10.1.3 Defeating Functions and Features

Implementations shall not include switches, jumpers or traces that may be cut, or control functions means (such as end user remote control functions or keyboard, command or keystroke bypass) by which content protection technologies or other mandatory provisions of the Specification may be defeated or by which compressed, decrypted SDMI Protected Content may be exposed to unauthorized copying, usage or distribution.

10.1.4 Maintain Security

Implementations shall be designed and manufactured so as to effectively frustrate attempts to: (i) discover or reveal non-public keys or cryptographic algorithms or other secrets/confidential information used to protect Content in Implementations, (ii) defeat the functions related to Authentication, encryption, decryption, SDMI screening, watermark screening, watermark insertion, the Secure Authenticated Channel and storage of SDMI Protected Content, as defined and required in the Specification, including the control functions or Usage Rules, to the extent such functions and rules are implemented in the foregoing, and (iii) change embedded identities (collectively, clauses (i), (ii) and (iii) of this Section 10.1.4 are referred to herein as the "Security Functions and Features"). Furthermore, in SDMI-Compliant products, where SDMI Protected Content is delivered from one part of the SDMI-Compliant product to another--whether among

integrated circuits, software modules, or a combination thereof--the portions of such product that perform the_Security Functions and Features shall be designed and otherwise integrated and associated with each other such that SDMI Protected Content in a usable form flowing between them shall be Protected from being intercepted and copied or distributed.

10.2 Methods Of Making Functions Robust

Implementations shall use at least the following techniques to be designed to effectively frustrate efforts to circumvent or defeat the functions and protections described in the Specification and these Robustness Requirements:

10.2.1 Accessibility of Content

Decrypted SDMI Protected Content shall not be available on outputs other than those specified in the Specification or these Robustness Requirements and, within Implementations, such Content shall not be present on any user accessible buses in useable form in such a manner that permits users to circumvent or defeat the Security Functions and Features. For these purposes, a "user accessible bus" shall mean a data bus which is designed for end user upgrades or access, such as PCMCIA, device bay, IEEE 1394 or Cardbus, but not PCI buses, memory buses, CPU buses, and similar portions of a device's internal architecture. The foregoing shall also apply to interfaces between or among SDMI-Compliant products, such that SDMI Protected Content is transmitted in a Protected manner.

10.2.2 Playback

Unprotected digital playback (e.g., via USB speakers) shall be limited to linear PCM at 48 kHz 16 bit or below, and any playback at a rate higher than 1.5 times normal speed shall be noticeably degraded unless the pitch is corrected to the pitch at the normal speed.

10.2.3 Robustness Requirements Applicable to Software Implementations

Any portion of an Implementation that implements one or more of the security functions set forth in the Specification in software that could allow compromise of SDMI Protected Content shall include all of the characteristics set forth in Sections 10.1 and 10.2.1 of these Robustness Requirements. In addition, such Implementations shall:

10.2.3.1 Use one or more reasonable methods, which may include, but shall not be 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 of software, using techniques of obfuscation to disguise and hamper attempts to discover the approaches used.

10.2.3.2 Be designed so as to perform self-checking of the integrity of its component parts and be designed to result in a failure of the Implementation to provide the authorized Authentication and/or decryption function in the event of unauthorized modification. For these purposes, a

"modification" includes any change in, or disturbance or invasion of features or characteristics, or interruption of processing. This provision requires at a minimum the use of "signed code" or other means of tagging or operating throughout the code which are equivalent or more robust. For purposes hereof, "component parts" are those that interact with SDMI Protected Content.

10.2.4 Robustness Requirements Applicable to Hardware Implementations

Any portion of an SDMI-Compliant product that implements a part of the Specification in hardware shall include all of the characteristics set forth in Sections 10.1 and 10.2.1 of these Robustness Requirements. The fact that a software Implementation operates on a hardware computing platform shall not, in and of itself, cause such hardware computer platform to be subject to the requirements set forth in Sections 10.2.4 and 10.2.5. If, however, the software Implementation relies on hardware or any hardware component to satisfy these Robustness Requirements, then such hardware or hardware component shall be governed by the robustness rules set forth herein for hardware implementations. In addition, such Implementation shall:

10.2.4.1 Use any reasonable means including, but not limited to: embedding encryption keys and algorithms in silicon circuitry or firmware which cannot be read, or the techniques described above for software.

10.2.4.2 Be designed such that attempts to remove or replace hardware elements in a way that would compromise the content protection features of the Specification would pose a serious risk of damaging such product so that it would no longer be able to receive or playback SDMI Protected Content. By way of example, a component which is soldered rather than socketed may be appropriate for these means.

10.2.4.3 Be designed such that the failure of a Security Function or Feature would cause the product to no longer be able to receive or playback SDMI Protected Content.

10.2.5 Robustness Requirements Applicable to Hybrid Implementations

The interfaces between hardware and software Implementations of an SDMI-Compliant product or between or among SDMI-Compliant products shall be designed so that they provide the level of protection that would be provided by a purely hardware or purely software Implementation as described above.

10.3 Required Levels Of Robustness

The Security Functions and Features and the characteristics set forth in Section 10.1.4 shall be implemented so that it is reasonably certain that they:

10.3.1 Cannot be defeated or circumvented using Widely Available Tools (as defined below) or Specialized Tools (as defined below) **and**

10.3.2 Can only with difficulty be defeated or circumvented using Professional Tools (as defined below).

Widely Available Tools shall mean general purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips, and soldering irons.

Specialized Tools shall mean specialized electronic tools that are widely available at a reasonable price, such as memory readers and writers, debuggers, decompilers, or similar software development products other than devices or technologies that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies that are required by the Specification, i.e., "Circumvention Devices".

Professional Tools shall mean professional tools or equipment, such as logic analyzers, chip disassembly systems, or in circuit emulators, but not including either professional tools or equipment that are made available on the basis of a non-disclosure agreement or Circumvention Devices.

10.4 New Circumstances

If an Implementation when designed and shipped complies with the requirements set forth above, but at any time thereafter circumstances arise which –had they been existing at the time of design—would have caused such Implementation to fail to comply with the Specification ("New Circumstances"), then upon having reasonable notice of such New Circumstances, the developer of such Implementation (the "SDMI Participant") shall promptly redesign affected product(s) or make available upgrades to its affected product(s), and, as soon as reasonably practicable, consistent with ordinary product cycles and taking into account the level of threat to Content under the New Circumstances, shall incorporate such redesign or replacement into its affected product(s), cease manufacturing such affected product(s) and cease selling such affected product(s).

10.5 Examination/Inspection

Under reasonable terms, including execution of mutually acceptable non-disclosure/non-use agreements, and upon reasonable notice to the SDMI Participant and the SDMI Foundation by one of the RIAA, the IFPI or the RIAJ (each referred to herein as a "Recording Company Association"), such Recording Company Association may at its own expense have an independent expert (acceptable to the SDMI Participant whose product(s) are to be inspected) inspect the details necessary to an understanding of such product(s)' implementation of the Specification and these Robustness Requirements and such details sufficient to determine whether such product(s) is/are SDMI-Compliant. Such SDMI Participant's approval of such proposed expert shall not be unreasonably withheld. Details which may be inspected include the executable object code, functional design diagrams, examples of the product, or block diagrams, but shall not include the source code, the Verilog Hardware Description Language (VHDL) or similar highly confidential information as reasonably designated by the SDMI Participant. Any report made by the independent expert shall be

made available to both the Recording Company Association and the SDMI Participant. The SDMI Participant shall not be precluded or estopped from challenging the opinion of such expert in any forum. Nothing in this paragraph shall limit the role or testimony of such expert, if any, in a judicial proceeding under such protective orders as a court may impose. This provision may not be invoked more than once per implementation, model or version, provided that such right of inspection shall include the right to re-inspect such implementation, model or version if it has been revised in an effort to cure any alleged failure of compliance. Any investigation conducted hereunder shall be based on reasonable grounds and commenced in a good faith attempt to determine whether an Implementation is SDMI-Compliant.

11 Appendix D — List of Figures

Figure 1: Reference Model Functional Layers 10
Figure 2: Version 1.0 Functional Reference Model 11
Figure 3: Content Flow and Usage Rule Diagram 13