

EXHIBIT 1

COMPLIANCE RULES FOR MICROSOFT IMPLEMENTATION OF WMFSDK WMDRM PLATFORMS

These Compliance Rules set forth the procedures and mechanisms through which the Microsoft Implementation of WMDRM running on the Windows Media Format SDK enforces the WMDRM controls applicable to the Copying, Streaming, playback or rendering of WMDRM Content on personal computers and to the issuance of WMDRM Licenses with Output controls from personal computers to devices, including when such devices are connected to Licensed Products implementing WMDRM-ND and WMDRM-PD. At this time, Microsoft does not license implementation of WMDRM on the WMF SDK to third parties.

1. DEFINITIONS

The following terms have the meanings set forth below. Other initially capitalized terms not defined in these Compliance Rules have the meanings ascribed to them in the Microsoft Implementation or in the Compliance Rules for Windows Media SDK WMDRM Applications.

- 1.1 “Anti-Rollback Clock” means a real time clock that is verified to have continued to advance each time WMDRM is executed.
- 1.2 “Certificate” means a unique WMDRM object used to assess trust.
- 1.3 “Certificate Chain” means a collection of Certificates that can trace the assessed trust back to the Microsoft Root Certificate.
- 1.4 “Certificate Revocation List” or “CRL” means a list of Certificates that have been revoked.
- 1.5 “Clock Rollback Event” means the detection by WMDRM that the current date and time precedes the date and time last recorded by WMDRM.
- 1.6 “Company” means an entity licensed under a License Agreement to develop Licensed Products.
- 1.7 “Consistent with the Microsoft Implementation” means a Licensed Product (i) provides equivalent functionality to the Microsoft Implementation, (ii) equals or exceeds the security of the Microsoft Implementation, and (iii) maintains compatibility and interoperability with the Microsoft Implementation.
- 1.8 “Content Key” means a symmetric key used to decrypt WMDRM Content.

- 1.9 “Content” means audio and/or video which are transmitted or distributed, either by broadcast, cablecast or other means of distribution to the general public or on demand.
- 1.10 “Copy” means to transport encrypted WMDRM Content over a USB connection, to the extent permitted by applicable WMDRM Policy, to a Licensed Product implementing WMDRM-PD for Passing to Outputs at any time and/or for as many times as permitted by applicable WMDRM Policy.
- 1.11 “Copy Protection Level” means a number included in WMDRM Policy that corresponds to the content protection that must be applied when issuing WMDRM Licenses and Copying WMDRM Content. The Copy Protection Level may be determined and assigned by the content owner or may be assigned by the WMDRM Implementation for specific categories of WMDRM Content.
- 1.12 “Cryptographically Random” means unpredictable, in that no polynomial-time algorithm, given any sequence of bits, can guess the succeeding K bits with probability greater than $\frac{1}{2}^K + 1/P(K)$ for any (positive) polynomial P and sufficiently large K.
- 1.13 “Device Key” means unique Cryptographically Random key or keys generated by Company for each of its Licensed Products or by its Licensed Products for the purpose of decrypting Content Keys.
- 1.14 “Direct License Acquisition” or “DLA” means the process of acquiring a WMDRM license directly from a WMDRM Server.
- 1.15 “ILA Receiver” means Licensed Products that may connect to ILA Transmitters and acquire WMDRM Licenses.
- 1.16 “ILA Transmitter” means Licensed Products that may connect to ILA Receivers and issue WMDRM Licenses.
- 1.17 “Indirect License Acquisition” or “ILA” means the process of acquiring a WMDRM license via an ILA Transmitter using the MTP or RAPI protocol over USB.
- 1.18 “License Acquisition” means acquiring a WMDRM License from an ILA Transmitter or WMDRM Server.
- 1.19 “License Agreement” means an agreement under which Microsoft licenses entities to develop and distribute products that include the Windows Media Format SDK redistributable components.

- 1.20 “License Evaluation” means, but is not limited to, the process of parsing the WMDRM License, verifying the signature and evaluating the syntax for the purpose of determining the WMDRM Policy and the Content Key.
- 1.21 “Licensed Product” means a hardware device or software application (or other software component, which may be a separately identifiable subset of a software application or operating system), that (i) implements WMDRM functionality subject to a license from Microsoft and/or (ii) is capable of playing back WMDRM Content. Licensed Products interact with and make use of the WMDRM functionality in the Microsoft Implementation, pursuant to applicable Compliance Rules, to control the Copying, Streaming, playback and rendering, and Output of WMDRM Content by the Licensed Products.
- 1.22 “Media Transfer Protocol” or “MTP” means Microsoft’s Media Transfer Protocol for device control, metadata exchange and media transfer, which is only supported over USB 1.0 or later.
- 1.23 “Metering” is a feature of WMDRM designed to securely collect and report content usage information.
- 1.24 “Microsoft Implementation” means the Microsoft implementation of WMDRM.
- 1.25 “Microsoft Root Certificate” means a Certificate controlled by Microsoft that is inherently trusted by the Microsoft Implementation and is the root source of trust for Licensed Products.
- 1.26 “Output” means Analog Audio Outputs, Analog Computer Monitor Outputs, Analog Television Outputs, Digital Audio Outputs, Digital Video Outputs, Internal Video Outputs and USB Audio Outputs. Output does not include Copying WMDRM Content over a USB connection to a Licensed Product implementing WMDRM-PD or Streaming WMDRM Content to a WMDRM-ND Receiver.
- 1.27 “Pass” means to direct decrypted WMDRM Content to flow to Outputs, optionally (though not necessarily) through intermediate components such as a codec or device driver.
- 1.28 “PD-WMDRM” means Portable Device WMDRM. For avoidance of doubt, this is not the same as WMDRM-PD.
- 1.29 “Persistent Storage” means storage that can retain data for an indefinite period of time after power is withdrawn.

- 1.30 “Privacy Key” means an asymmetric public key provided by Microsoft for the purpose of encrypting sensitive communication sent over a public network.
- 1.31 “Secure Clock Service” means an Internet service authorized by Microsoft for the purpose of providing the current UTC date and time through a secure protocol.
- 1.32 “Secure Clock” means a hardware real time clock that has been secured from unauthorized access.
- 1.33 “Security Level” means a number in the WMDRM Policy associated with specific WMDRM Content that specifies the minimum security level necessary for a Licensed Product to be able to acquire a WMDRM License for the WMDRM Content.
- 1.34 “Stream” means to transport encrypted WMDRM Content over a network, to the extent permitted by applicable WMDRM Policy, to a WMDRM-ND Receiver for Passing to an Output immediately or shortly after receipt of the WMDRM Content in the WMDRM-ND Receiver.
- 1.35 “UTC” means Universal Time Coordinated.
- 1.36 “WMDRM” means Windows Media Digital Rights Management technology.
- 1.37 “WMDRM Content” means audio or audiovisual content that has been encrypted and recorded using WMDRM.
- 1.38 “WMDRM Data Stores” means the secure databases required for mandatory and optional WMDRM features. This includes, but is not limited to, License store, Secure store, Metering store and License Synchronization store as defined in the Microsoft Implementation.
- 1.39 “WMDRM License” means a data structure that contains, but is not limited to, WMDRM Policy and an encrypted Content Key associated with specific WMDRM Content.
- 1.40 “WMDRM Policy” means the description of the actions permitted and/or required with WMDRM Content and restrictions on those actions as described in the WMDRM License associated with the WMDRM Content.
- 1.41 “WMDRM Server” means a Licensed Product capable of issuing WMDRM Licenses over a network connection.

- 1.42 “WMDRM Technology” means the methods for local decryption and renewability developed by Microsoft for use with Windows Media Digital Rights Management.
- 1.43 “WMDRM-ND Receiver” means a Licensed Product that may connect to WMDRM-ND Transmitters and acquire WMDRM Content.
- 1.44 “WMDRM-ND Transmitter” means a Licensed Product that may connect to WMDRM-ND Receivers and issue WMDRM Licenses and WMDRM Content.
- 1.45 “WMDRM-PD MTP Extensions Technical Documentation” means the Technical Documentation, included in the Microsoft Implementation of WMDRM-PD, that describes how to call WMDRM-PD from MTP.
- 1.46 “WMDRM-PD” means WMDRM for Portable Devices.

2. REQUIREMENTS FOR WMDRM PLATFORMS

2.1 **Functionality.** The Microsoft Implementation of WMDRM will comply with all of the specific Compliance Rules set forth in this document.

2.2 **Random Number Generator.** The Microsoft Implementation will implement and make use of a random number generator that is Cryptographically Random. For the avoidance of doubt, linear congruential random number generators are not acceptable.

2.3 **Serial Number.** The Microsoft Implementation will implement a serial number with a minimum length of 128 bits that is uniquely generated based on characteristics of the platform on which it is running.

2.4 **Data Stores.** The Microsoft Implementation will support WMDRM Data Stores. If Optional Features are implemented, the corresponding Data Stores will be supported.

2.5 **Direct License Acquisition.** The Microsoft Implementation will support Direct License Acquisition functionality.

2.6 **License Evaluation.** The Microsoft Implementation will implement License Evaluation.

2.7 Cryptographic Keys

2.7.1 **Device Key.** A Cryptographically Random Device Key will be generated by Microsoft or for the Microsoft Implementation. The Device Key will be unique to each product on which the Microsoft Implementation is installed.

2.7.2 **Privacy Public Key.** The Microsoft Implementation will securely store the Privacy Public Key for use on Licensed Products. All DLA transmissions will be encrypted with the Privacy Public Key.

2.8 **Real time clock.** Microsoft Implementations that support use of WMDRM Licenses including expiration, as described in Section 4.1, will implement a Real Time Clock. The Microsoft Implementation may implement an Anti-Rollback Clock as described below.

2.8.1 **Anti-Rollback Clock.** Anti-Rollback Clock, if supported, will be implemented as follows:

2.8.1.1 **Clock Reset.** When power is lost, the clock will be automatically reset to a date and time preceding the last valid date and time recorded by WMDRM.

2.8.1.2 **Clock Rollback.** When the Microsoft Implementation detects a Clock Rollback Event, it will iterate through all WMDRM Licenses stored in the WMDRM License Store and take the appropriate actions as specified in Sections 3.3.5 and 3.3.6.

3. REQUIREMENTS FOR COMPLYING WITH WMDRM POLICY

3.1 **Security Level.** The Microsoft Implementation will decrypt WMDRM Content using only WMDRM Licenses that have a Security Level less than or equal to the Security Level for the Microsoft Implementation.

3.2 **Unspecified policy.** WMDRM Policy may specify additional rights, restrictions or parameters that are not covered in these Compliance Rules. Nevertheless the Microsoft Implementation will only take action based on rights and enforce restrictions covered in this document. To the extent that WMDRM Policy (or a particular WMDRM License) describes additional rights, restrictions or parameters that are not described in these Compliance Rules, the Microsoft Implementation will ignore such additional rights, restrictions or parameters.

3.3 **Expiration.** Microsoft Implementations that support a Clock will implement expiration support as follows:

3.3.1 **Begin Date.** If specified in the WMDRM License, the Microsoft Implementation will not allow the associated WMDRM Content to be decrypted before the specified date and time.

3.3.2 **End Date.** If specified in the WMDRM License, the Microsoft Implementation will not allow the associated WMDRM Content to be decrypted after the specified date and time.

3.3.3 ExpirationAfterFirstUse. If specified in the WMDRM License, upon first use of the associated WMDRM Content the specified number of hours will be added to the current date and time and the sum stored in the Secure Store. This sum will then be evaluated as specified in Section 3.3.2.

3.3.4 ExpirationOnStore. If specified in the WMDRM License, upon storing the WMDRM License the specified number of hours will be added to the current date and time and the sum stored in the Secure Store. This sum will then be evaluated as specified in Section 3.3.2.

3.3.5 DisableOnClockRollback. If the Microsoft Implementation Anti-Rollback Clock detects a Clock Rollback Event, WMDRM will make inaccessible any WMDRM License that specifies DisableOnClockRollback. When WMDRM detects that the current date and time exceeds the last known valid date and time, it will re-enable access to any WMDRM License that specifies DisableOnClockRollback.

3.3.6 DeleteOnClockRollback. If the Microsoft Implementation implements Anti-Rollback Clock as described in Section 2.8.1 and detects and processes a Clock Rollback Event, WMDRM will delete any WMDRM License that specifies DeleteOnClockRollback.

3.4 Metering. Metering, if supported, will be implemented as follows:

3.4.1 Implementation. Each time a WMDRM License that includes a Metering ID is used to decrypt and Pass WMDRM Content, the Microsoft Implementation will update the WMDRM Metering Store.

3.4.2 Metering Update. When accessing WMDRM Content with an associated WMDRM License that requires Metering, the Metering Store will be updated the first time the associated WMDRM Content is decrypted and Passed.

3.4.3 Insufficient Storage. If a Licensed Product does not have Persistent Storage available to persist updates to Metering, the Microsoft Implementation will not decrypt and Pass WMDRM Content using any WMDRM License specifying a Metering ID.

3.5 Play Count. Play count, if present in the WMDRM License, specifies the number of times that a WMDRM License may be used to decrypt and Pass WMDRM Content. The Microsoft Implementation will implement Play count as follows:

3.5.1 Implementation. If Play count is specified in the WMDRM License, the Microsoft Implementation will limit the number of Plays to the specified maximum number. A play count is decremented when WMDRM Content is first decrypted and Passed.

3.5.2 **Insufficient Storage.** If a Licensed Product does not have available Persistent Storage to record Play count, the Microsoft Implementation will not decrypt WMDRM Content using any WMDRM License that specifies a Play Count.

4. RULES FOR COPYING TO LICENSED PRODUCTS

4.1 **Policy Verification.** The Microsoft Implementation may permit WMDRM Licenses to be rebound to a portable device only if the appropriate rights are specified.

4.1.1 **Transfer to Non SDMI Device.** If the right AllowTransferToNonSDMI is specified, fixed WMDRM Licenses may be copied to a portable device supporting WMDRM-PD or PD-WMDRM.

4.1.2 **Transfer to SDMI Device.** If the right AllowTransferToSDMI is specified, fixed WMDRM Licenses may be copied to a portable device supporting WMDRM-PD or PD-WMDRM.

4.1.3 **Copy with CPL 0 to 300.** If the right AllowCopy with a Copy Protection Level less than or equal to 300 is specified, fixed WMDRM Licenses may be copied to a portable device supporting PD-WMDRM.

4.1.4 **Copy with CPL 0 to 400.** If the right AllowCopy with a Copy Protection Level less than or equal to 400 is specified, fixed WMDRM Licenses may be copied to a portable device supporting WMDRM-PD.

4.2 **Copy to WMDRM-PD portable device.** Microsoft Implementations that enable rebinding of WMDRM Licenses to a portable device running WMDRM-PD will comply with all requirements specified in this Section 4.2.

4.2.1 **Device Certificate.** The Microsoft Implementation will retrieve the Device Certificate from the portable device running WMDRM-PD. If the Microsoft Implementation is unable to retrieve a Device Certificate, the Microsoft Implementation will not copy a WMDRM License to the portable device. If verification of any signatures on the Device Certificate fails, the Microsoft Implementation will not copy a WMDRM License to the portable device.

4.2.2 **Revocation Check.** The Microsoft Implementation will compare the Device Certificate retrieved from the portable device against a CRL. If the Device Certificate is found to have been revoked, the Microsoft Implementation will not copy a WMDRM License to the portable device.

4.2.3 **Serial Number.** The Microsoft Implementation will permit WMDRM Licenses to be copied to the portable device only if the value of the serial

number in the Device Certificate is greater than or equal to the serial number specified in the WMDRM License.

4.2.4 Feature verification. The Microsoft Implementation will permit WMDRM Licenses to be copied to the portable device only if the Device Certificate specifies that the portable device supports the functionality required by the WMDRM License. For example, in order for a WMDRM License including expiration to be issued to a portable device, the portable device's Device Certificate must specify that the portable device supports a Secure Clock or Anti-Rollback Clock.

4.2.5 Derived License. The Microsoft Implementation may use a WMDRM License to derive a new WMDRM License containing only the rights and restrictions present in the original WMDRM License. The derived WMDRM License will include a Content Key encrypted using the public key retrieved from the Device Certificate retrieved from the portable device.

4.2.6 Secure Clock. If a portable device supports a Secure Clock, the Microsoft Implementation will not transfer derived WMDRM Licenses to the portable device if the Secure Clock is unset. The Microsoft Implementation will facilitate setting the Secure Clock on the device via the Secure Clock Service.

4.2.7 License Synchronization. The Microsoft Implementation will support retrieving a list of licenses that need to be updated from the portable device. If the corresponding WMDRM Licenses are available as described in Section 4.1, the Microsoft Implementation will derive WMDRM Licenses for the portable device consistent with Section 4.2.5.

4.3 Copy to PD-WMDRM portable device. Microsoft Implementations that enable rebinding WMDRM Licenses to a portable device running PD-WMDRM will comply with all requirements specified in this Section 4.2.

4.3.1 Serial Number. The Microsoft Implementation will query a PD-WMDRM capable portable device for the portable device's serial number.

4.3.2 Derived License. The Microsoft Implementation will use the serial number and PD-WMDRM global key to encrypt the Content Key and bind it to the device. The Microsoft Implementation will create a PD-WMDRM compatible license that includes rights to play on the device. The Derived License will be transferred to the portable device.

4.4 Transfer of Clear Content. If the right AllowTransferToNonSDMI, AllowTransferToSDMI or AllowCopy is set in the WMDRM License, the portable device does not support WMDRM-PD or PD-WMDRM, and the Security Level specified in the WMDRM License is less than or equal to 150, the Microsoft Implementation may decrypt WMDRM Content and transfer decrypted WMDRM Content to the portable device.

5. RULES FOR STREAMING TO LICENSED PRODUCTS

5.1 Proximity Detection Policy

5.1.1 **Round Trip Time (RTT) Verification.** The Microsoft Implementation will securely verify that the RTT between the WMDRM-ND Transmitter and the WMDRM-ND Receiver is no more than seven (7) milliseconds.

5.1.2 **Time to Live (TTL).** The Microsoft Implementation will set the TTL to three (3) on Round Trip Time measurement packets.

5.2 **Concurrent Streaming WMDRM-ND Receivers.** The Microsoft Implementation will enforce that only ten (10) WMDRM-ND Receivers are able concurrently to receive Streamed WMDRM Content at a single moment in time.

5.3 **Certificate Revocation List.** The Microsoft Implementation will enforce WMDRM-ND Receiver revocation based on the contents of the Certificate Revocation List. If any part of the WMDRM-ND Receiver Certificate Chain appears in the Certificate Revocation List then the Microsoft Implementation will not Stream WMDRM Content to the WMDRM-ND Receiver.

5.4 **Security Level.** The Microsoft Implementation will verify that the Security Level of the WMDRM-ND Receiver is no less than the Security Level of the requested WMDRM Content. If the verification of the Security Level fails, the Microsoft Implementation will not Stream the WMDRM Content.

5.5 **WMDRM-ND Receiver Certificates.** The Microsoft Implementation will verify that the WMDRM-ND Receiver Certificates have been properly signed. The Microsoft Implementation will also verify that the Certificate Chain can be traced back to Microsoft Root Certificate. If the verification of the WMDRM-ND Receiver Certificates fails, the Microsoft Implementation will not Stream the WMDRM Content.

5.6 **Preserve Content Rights.** The Microsoft Implementation may use a WMDRM License to derive a new WMDRM License containing only the rights and restrictions present in the original WMDRM License.

COMPLIANCE RULES FOR MICROSOFT IMPLEMENTATION OF WMFSDK WMDRM PLATFORMS

These Compliance Rules set forth the procedures and mechanisms through which the Microsoft Implementation of WMDRM running on the Windows Media Format SDK enforces the WMDRM controls applicable to the ~~copying, streaming~~Copying, Streaming, playback or rendering of WMDRM Content on personal computers and to the issuance of WMDRM Licenses with ~~output~~Output controls from personal computers to devices, including when such devices are connected to Licensed Products implementing WMDRM-ND and WMDRM-PD. At this time, Microsoft does not license implementation of WMDRM on the WMF SDK to third parties.

1. DEFINITIONS

The following terms have the meanings set forth below. Other initially capitalized terms not defined in these Compliance Rules have the meanings ascribed to them in the Microsoft Implementation: [or in the Compliance Rules for Windows Media SDK WMDRM Applications.](#)

- 1.1 “Anti-Rollback Clock” means a real time clock that is verified to have continued to advance each time WMDRM is executed.
- 1.2 “Certificate” means a unique WMDRM object used to assess trust.
- 1.3 “Certificate Chain” means a collection of Certificates that can trace the assessed trust back to the Microsoft Root Certificate.
- 1.4 “Certificate Revocation List” or “CRL” means a list of Certificates that have been revoked.
- 1.5 “Clock Rollback Event” means the detection by WMDRM that the current date and time precedes the date and time last recorded by WMDRM.
- 1.6 “Company” means an entity licensed under a License Agreement to develop Licensed Products.
- 1.7 “Consistent with the Microsoft Implementation” means a Licensed Product (i) provides equivalent functionality to the Microsoft Implementation, (ii) equals or exceeds the security of the Microsoft Implementation, and (iii) maintains compatibility and interoperability with the Microsoft Implementation.
- 1.8 “Content Key” means a symmetric key used to decrypt WMDRM Content.

- 1.9 “Content” means audio and/or video which are transmitted or distributed, either by broadcast, cablecast or other means of distribution to the general public or on demand.
- 1.10** **“Copy” means to transport encrypted WMDRM Content over a USB connection, to the extent permitted by applicable WMDRM Policy, to a Licensed Product implementing WMDRM-PD for Passing to Outputs at any time and/or for as many times as permitted by applicable WMDRM Policy.**
- 1.11** ~~1.10~~ “Copy Protection Level” means a number included in WMDRM Policy that corresponds to the content protection that must be applied when issuing WMDRM Licenses and ~~copying~~**Copying** WMDRM Content. The Copy Protection Level may be determined and assigned by the content owner or may be assigned by the WMDRM Implementation for specific categories of WMDRM Content.
- 1.12** ~~1.11~~ “Cryptographically Random” means unpredictable, in that, ~~at any point regardless of how many preceding~~ **no polynomial-time algorithm, given any sequence of** bits ~~are available, can guess~~ the ~~probability of predicting the next~~ succeeding K bits **is with probability** greater than $\frac{1}{2}^K + \frac{1}{P(K)}$ **for any (positive) polynomial P and sufficiently large K.**
- 1.13** ~~1.12~~ “Device Key” means unique Cryptographically Random key or keys generated by Company for each of its Licensed Products or by its Licensed Products for the purpose of decrypting Content Keys.
- 1.14** ~~1.13~~ “Direct License Acquisition” or “DLA” means the process of acquiring a WMDRM license directly from a WMDRM Server.
- 1.15** ~~1.14~~ “ILA Receiver” means Licensed Products that may connect to ILA Transmitters and acquire WMDRM Licenses.
- 1.16** ~~1.15~~ “ILA Transmitter” means Licensed Products that may connect to ILA ~~Receiver~~**Receivers** and ~~acquire~~**issue** WMDRM Licenses.
- 1.17** ~~1.16~~ “Indirect License Acquisition” or “ILA” means the process of acquiring a WMDRM license via an ILA Transmitter using the MTP or RAPI protocol over USB.
- 1.18** ~~1.17~~ “License Acquisition” means acquiring a WMDRM License from an ILA Transmitter or WMDRM Server.

- 1.19 ~~1.18~~ “License Agreement” means ~~the an~~ agreement under which Microsoft licenses entities to develop and distribute products that include the Windows Media Format SDK redistributable components.
- 1.20 ~~1.19~~ “License Evaluation” means, but is not limited to, the process of parsing the WMDRM License, verifying the signature and evaluating the syntax for the purpose of determining the WMDRM Policy and the Content Key.
- 1.21 ~~1.20~~ “Licensed Product” means a hardware device or software application (or other software component, which may be a separately identifiable subset of a software application or operating system), that (i) implements WMDRM functionality subject to a license from Microsoft and/or (ii) is capable of playing back WMDRM Content. Licensed Products interact with and make use of the WMDRM functionality in the Microsoft Implementation, pursuant to applicable Compliance Rules, to control the ~~copying, streaming~~ Copying, Streaming, playback and rendering, and ~~output~~ Output of WMDRM Content by the Licensed Products.
- 1.22 ~~1.21~~ “Media Transfer Protocol” or “MTP” means Microsoft’s Media Transfer Protocol for device control, metadata exchange and media transfer, which is only supported over USB 1.0 or later.
- 1.23 ~~1.22~~ “Metering” is a feature of WMDRM designed to securely collect and report content usage information.
- 1.24 ~~1.23~~ “Microsoft Implementation” means the Microsoft implementation of WMDRM.
- 1.25 ~~1.24~~ “Microsoft Root Certificate” means a Certificate controlled by Microsoft that is inherently trusted by the Microsoft Implementation and is the root source of trust for Licensed Products.
- 1.26 “Output” means Analog Audio Outputs, Analog Computer Monitor Outputs, Analog Television Outputs, Digital Audio Outputs, Digital Video Outputs, Internal Video Outputs and USB Audio Outputs. Output does not include Copying WMDRM Content over a USB connection to a Licensed Product implementing WMDRM-PD or Streaming WMDRM Content to a WMDRM-ND Receiver.
- 1.27 “Pass” means to direct decrypted WMDRM Content to flow to Outputs, optionally (though not necessarily) through intermediate components such as a codec or device driver.
- 1.28 ~~1.25~~ “PD-WMDRM” means Portable Device WMDRM. For avoidance of doubt, this is not the same as WMDRM-PD.

- [1.29](#) ~~1.26~~ “Persistent Storage” means storage that can retain data for an indefinite period of time after power is withdrawn.
- [1.30](#) ~~1.27~~ “Privacy Key” means an asymmetric public key provided by Microsoft for the purpose of encrypting sensitive communication sent over a public network.
- [1.31](#) ~~1.28~~ “Secure Clock Service” means an Internet service authorized by Microsoft for the purpose of providing the current UTC date and time through a secure protocol.
- [1.32](#) ~~1.29~~ “Secure Clock” means a hardware real time clock that has been secured from unauthorized access.
- [1.33](#) ~~1.30~~ “Security Level” means a number in the WMDRM Policy associated with specific WMDRM Content that specifies the minimum security level necessary for a Licensed Product to be able to acquire a WMDRM License for the WMDRM Content.
- [1.34](#) “Stream” means to transport encrypted WMDRM Content over a network, to the extent permitted by applicable WMDRM Policy, to a WMDRM-ND Receiver for Passing to an Output immediately or shortly after receipt of the WMDRM Content in the WMDRM-ND Receiver.
- [1.35](#) ~~1.31~~ “UTC” means Universal Time Coordinated.
- [1.36](#) ~~1.32~~ “WMDRM” means Windows Media Digital Rights Management technology.
- [1.37](#) ~~1.33~~ “WMDRM Content” means audio or audiovisual content that has been encrypted and recorded using WMDRM.
- [1.38](#) ~~1.34~~ “WMDRM Data Stores” means the secure databases required for mandatory and optional WMDRM features. This includes, but is not limited to, License store, Secure store, Metering store and License Synchronization store as defined in the Microsoft Implementation.
- [1.39](#) ~~1.35~~ “WMDRM License” means a data structure that contains, but is not limited to, WMDRM Policy and an encrypted Content Key associated with specific WMDRM Content.
- [1.40](#) ~~1.36~~ “WMDRM Policy” means the description of the actions permitted and/or required with WMDRM Content and restrictions on those actions as described in the WMDRM License associated with the WMDRM Content.

- [1.41](#) ~~1.37~~ “WMDRM Server” means a Licensed Product capable of issuing WMDRM Licenses over a network connection.
- [1.42](#) ~~1.38~~ “WMDRM Technology” means the methods for local decryption and renewability developed by Microsoft for use with Windows Media Digital Rights Management.
- [1.43](#) ~~1.39~~ “WMDRM-ND Receiver” means a Licensed Product that may connect to WMDRM-ND Transmitters and acquire WMDRM Content.
- [1.44](#) ~~1.40~~ “WMDRM-ND Transmitter” means a Licensed Product that may connect to WMDRM-ND Receivers and issue WMDRM Licenses and WMDRM Content.
- [1.45](#) ~~1.41~~ “WMDRM-PD MTP Extensions Technical Documentation” means the Technical Documentation, included in the Microsoft Implementation of WMDRM-PD, that describes how to call WMDRM-PD from MTP.
- [1.46](#) ~~1.42~~ “WMDRM-PD” means WMDRM for Portable Devices.

2. REQUIREMENTS FOR WMDRM PLATFORMS

2.1 **Functionality.** The Microsoft Implementation of WMDRM will comply with all of the specific Compliance Rules set forth in this document.

2.2 **Random Number Generator.** The Microsoft Implementation will implement and make use of a random number generator that is Cryptographically Random. For the avoidance of doubt, linear congruential random number generators are not acceptable.

2.3 **Serial Number.** The Microsoft Implementation will implement a serial number with a minimum length of 128 bits that is uniquely generated based on characteristics of the platform on which it is running.

2.4 **Data Stores.** The Microsoft Implementation will support WMDRM Data Stores. If Optional Features are implemented, the corresponding Data Stores will be supported.

2.5 **Direct License Acquisition.** The Microsoft Implementation will support Direct License Acquisition functionality.

2.6 **License Evaluation.** The Microsoft Implementation will implement License Evaluation.

2.7 **Cryptographic Keys**

2.7.1 **Device Key.** A Cryptographically Random Device Key will be generated by Microsoft or for the Microsoft Implementation. The Device Key will be unique to each product on which the Microsoft Implementation is installed.

2.7.2 **Privacy Public Key.** The Microsoft Implementation will securely store the Privacy Public Key for use on Licensed Products. All DLA transmissions will be encrypted with the Privacy Public Key.

2.8 **Real time clock.** Microsoft Implementations that support use of WMDRM Licenses including expiration, as described in Section 4.1, will implement a Real Time Clock. The Microsoft Implementation may implement an Anti-Rollback Clock as described below.

2.8.1 **Anti-Rollback Clock.** Anti-Rollback Clock, if supported, will be implemented as follows:

2.8.1.1 **Clock Reset.** When power is lost, the clock will be automatically reset to a date and time preceding the last valid date and time recorded by WMDRM.

2.8.1.2 **Clock Rollback.** When the Microsoft Implementation detects a Clock Rollback Event, it will iterate through all WMDRM Licenses stored in the WMDRM License Store and take the appropriate actions as specified in Sections 3.3.5 and 3.3.6.

3. REQUIREMENTS FOR COMPLYING WITH WMDRM POLICY

3.1 **Security Level.** The Microsoft Implementation will decrypt WMDRM Content using only WMDRM Licenses that have a Security Level less than or equal to the Security Level for the Microsoft Implementation.

3.2 **Unspecified policy.** WMDRM Policy may specify additional rights, restrictions or parameters that are not covered in these Compliance Rules. Nevertheless the Microsoft Implementation will only take action based on rights and enforce restrictions covered in this document. To the extent that WMDRM Policy (or a particular WMDRM License) describes additional rights, restrictions or parameters that are not described in these Compliance Rules, the Microsoft Implementation will ignore such additional rights, restrictions or parameters.

3.3 **Expiration.** Microsoft Implementations that support a Clock will implement expiration support as follows:

3.3.1 **Begin Date.** If specified in the WMDRM License, the Microsoft Implementation will not allow the associated WMDRM Content to be **passed**[decrypted](#) before the specified date and time.

3.3.2 **End Date.** If specified in the WMDRM License, the Microsoft Implementation will not allow the associated WMDRM Content to be ~~passed~~decrypted after the specified date and time.

3.3.3 **ExpirationAfterFirstUse.** If specified in the WMDRM License, upon first use of the associated WMDRM Content the specified number of hours will be added to the current date and time and the sum stored in the Secure Store. This sum will then be evaluated as specified in Section 3.3.2.

3.3.4 **ExpirationOnStore.** If specified in the WMDRM License, upon storing the WMDRM License the specified number of hours will be added to the current date and time and the sum stored in the Secure Store. This sum will then be evaluated as specified in Section 3.3.2.

3.3.5 **DisableOnClockRollback.** If the Microsoft Implementation Anti-Rollback Clock detects a Clock Rollback Event, WMDRM will make inaccessible any WMDRM License that specifies DisableOnClockRollback. When WMDRM detects that the current date and time exceeds the last known valid date and time, it will re-enable access to any WMDRM License that specifies DisableOnClockRollback.

3.3.6 **DeleteOnClockRollback.** If the Microsoft Implementation implements Anti-Rollback Clock as described in Section 2.8.1 and detects and processes a Clock Rollback Event, WMDRM will delete any WMDRM License that specifies DeleteOnClockRollback.

3.4 **Metering.** Metering, if supported, will be implemented as follows:

3.4.1 **Implementation.** Each time a WMDRM License that includes a Metering ID is used to decrypt and ~~pass~~Pass WMDRM Content, the Microsoft Implementation will update the WMDRM Metering Store.

3.4.2 **Metering Update.** When accessing WMDRM Content with an associated WMDRM License that requires Metering, the Metering Store will be updated the first time the associated WMDRM Content is decrypted and ~~passed-~~Passed.

3.4.3 **Insufficient Storage.** If a Licensed Product does not have Persistent Storage available to persist updates to Metering, the Microsoft Implementation will not decrypt and ~~pass~~Pass WMDRM Content using any WMDRM License specifying a Metering ID.

3.5 **Play Count.** Play count, if present in the WMDRM License, specifies the number of times that a WMDRM License may be used to decrypt and ~~pass~~Pass WMDRM Content. The Microsoft Implementation will implement Play count as follows:

3.5.1 **Implementation.** If Play count is specified in the WMDRM License, the Microsoft Implementation will limit the number of Plays to the specified maximum number. A play count is decremented when WMDRM Content is first decrypted and ~~passed~~.Passed.

3.5.2 **Insufficient Storage.** If a Licensed Product does not have available Persistent Storage to record Play count, the Microsoft Implementation will not decrypt WMDRM Content using any WMDRM License that specifies a Play Count.

4. RULES FOR COPYING TO LICENSED PRODUCTS

4.1 **Policy Verification.** The Microsoft Implementation may permit WMDRM Licenses to be rebound to a portable device only if the appropriate rights are specified.

4.1.1 **Transfer to Non SDMI Device.** If the right AllowTransferToNonSDMI is specified, fixed WMDRM Licenses may be copied to a portable device supporting WMDRM-PD or PD-WMDRM.

4.1.2 **Transfer to SDMI Device.** If the right AllowTransferToSDMI is specified, fixed WMDRM Licenses may be copied to a portable device supporting WMDRM-PD or PD-WMDRM.

4.1.3 **Copy with CPL 0 to 300.** If the right AllowCopy with a Copy Protection Level less than or equal to 300 is specified, fixed WMDRM Licenses may be copied to a portable device supporting PD-WMDRM.

4.1.4 **Copy with CPL 0 to 400.** If the right AllowCopy with a Copy Protection Level less than or equal to 400 is specified, fixed WMDRM Licenses may be copied to a portable device supporting WMDRM-PD.

4.2 **Copy to WMDRM-PD portable device.** Microsoft Implementations that enable rebinding of WMDRM Licenses to a portable device running WMDRM-PD will comply with all requirements specified in this Section 4.2.

4.2.1 **Device Certificate.** The Microsoft Implementation will retrieve the Device Certificate from the portable device running WMDRM-PD. If the Microsoft Implementation is unable to retrieve a Device Certificate, the Microsoft Implementation will not copy a WMDRM License to the portable device. If verification of any signatures on the Device Certificate fails, the Microsoft Implementation will not copy a WMDRM License to the portable device.

4.2.2 **Revocation Check.** The Microsoft Implementation will compare the Device Certificate retrieved from the portable device against a CRL. If the Device

Certificate is found to have been revoked, the Microsoft Implementation will not copy a WMDRM License to the portable device.

4.2.3 Serial Number. The Microsoft Implementation will permit WMDRM Licenses to be copied to the portable device only if the value of the serial number in the Device Certificate is greater than or equal to the serial number specified in the WMDRM License.

4.2.4 Feature verification. The Microsoft Implementation will permit WMDRM Licenses to be copied to the portable device only if the Device Certificate specifies that the portable device supports the functionality required by the WMDRM License. For example, in order for a WMDRM License including expiration to be issued to a portable device, the portable device's Device Certificate must specify that the portable device supports a Secure Clock or Anti-Rollback Clock.

4.2.5 Derived License. The Microsoft Implementation may use a WMDRM License to derive a new WMDRM License containing only the rights and restrictions present in the original WMDRM License. The derived WMDRM License will include a Content Key encrypted using the public key retrieved from the Device Certificate retrieved from the portable device.

4.2.6 Secure Clock. If a portable device supports a Secure Clock, the Microsoft Implementation will not transfer derived WMDRM Licenses to the portable device if the Secure Clock is unset. The Microsoft Implementation will facilitate setting the Secure Clock on the device via the Secure Clock Service.

4.2.7 License Synchronization. The Microsoft Implementation will support retrieving a list of licenses that need to be updated from the portable device. If the corresponding WMDRM Licenses are available as described in Section 4.1, the Microsoft Implementation will derive WMDRM Licenses for the portable device consistent with Section 4.2.5.

4.3 Copy to PD-WMDRM portable device. Microsoft Implementations that enable rebinding WMDRM Licenses to a portable device running PD-WMDRM will comply with all requirements specified in this Section 4.2.

4.3.1 Serial Number. The Microsoft Implementation will query a PD-WMDRM capable portable device for the portable device's serial number.

4.3.2 Derived License. The Microsoft Implementation will use the serial number and PD-WMDRM global key to encrypt the Content Key and bind it to the device. The Microsoft Implementation will create a PD-WMDRM compatible license that includes rights to play on the device. The Derived License will be transferred to the portable device.

4.4 **Transfer of Clear Content.** If the right AllowTransferToNonSDMI, AllowTransferToSDMI or AllowCopy is set in the WMDRM License, the portable device does not support WMDRM-PD or PD-WMDRM, and the Security Level specified in the WMDRM License is less than or equal to 150, the Microsoft Implementation may decrypt WMDRM Content and transfer decrypted WMDRM Content to the portable device.

5. RULES FOR STREAMING TO LICENSED PRODUCTS

5.1 Proximity Detection Policy

5.1.1 **Round Trip Time (RTT) Verification.** The Microsoft Implementation will securely verify that the RTT between the WMDRM-ND Transmitter and the WMDRM-ND Receiver is no more than seven (7) milliseconds.

5.1.2 **Time to Live (TTL).** The Microsoft Implementation will set the TTL to three (3) on Round Trip Time measurement packets.

5.2 **Concurrent Streaming WMDRM-ND Receivers.** The Microsoft Implementation will enforce that only ten (10) ~~concurrent streaming~~ WMDRM-ND Receivers are able concurrently to receive Streamed WMDRM Content at a single moment in time.

5.3 **Certificate Revocation List.** The Microsoft Implementation will enforce WMDRM-ND Receiver revocation based on the contents of the Certificate Revocation List. If any part of the WMDRM-ND Receiver Certificate Chain appears in the Certificate Revocation List then the Microsoft Implementation will not ~~pass content~~ Stream WMDRM Content to the WMDRM-ND Receiver.

5.4 **Security Level.** The Microsoft Implementation will verify that the Security Level of the WMDRM-ND Receiver is no less than the Security Level of the requested WMDRM Content. If the verification of the Security Level fails, the Microsoft Implementation will not ~~pass~~ Stream the WMDRM Content.

5.5 **WMDRM-ND Receiver Certificates.** The Microsoft Implementation will verify that the WMDRM-ND Receiver Certificates have been properly signed. The Microsoft Implementation will also verify that the ~~Root Trust Authority~~ Certificate Chain can be traced back to Microsoft Root Certificate. If the verification of the WMDRM-ND Receiver Certificates fails, the Microsoft Implementation will not ~~pass~~ Stream the WMDRM Content.

5.6 **Preserve Content Rights.** The Microsoft Implementation may use a WMDRM License to derive a new WMDRM License containing only the rights and restrictions present in the original WMDRM License.

EXHIBIT 2

COMPLIANCE RULES FOR FOR WMF SDK WMDRM APPLICATIONS

1. DEFINITIONS

The following terms have the meanings set forth below. Other initially capitalized terms not defined in these Compliance Rules have the meanings ascribed to them in the License Agreement and the Microsoft Implementation.

- 1.1 “AES” means Advanced Encryption Standard.
- 1.2 “Analog Audio Output” means a connector for an analog sound reproduction device such as a speaker or headphones. For avoidance of doubt, this includes both external jacks to connect speakers and/or headphones and built-in speakers and/or headphones.
- 1.3 “Analog Computer Monitor Output” means a connector for an analog monitor that is typically found and associated with a Computer Product and that carries uncompressed analog video signals. The term expressly includes those outputs known as VGA, SVGA, XGA, DVI Analog, and various non-standardized analog monitor connections that have been implemented by manufacturers, and expressly does not include such typical consumer electronics connectors as NTSC, PAL, SECAM, SCART, YPrPb, S-Video and Consumer RGB, whether or not such connectors are found on any Computer Product.
- 1.4 “Analog Protection System (APS) trigger bits (APSTB)” means the Analog Protection System bits as specified (a) for NTSC video signals, in IEC 61880 (for inclusion of such value on Line 20) or EIA-608-B (for inclusion of such value on Line 21) or (b) for YUV (525/60 systems) signals, in IEC 61880 (for inclusion of such value on Line 20) or EIA-608-B (for inclusion of such value on Line 21).
- 1.5 “Analog Television Output” means such typical consumer electronics analog connectors as NTSC, PAL, SECAM, SCART, YPrPb, S-Video and Consumer RGB.
- 1.6 “Automatic Gain Control (AGC)” means the so-named copy control system as specified (a) for NTSC, PAL, SECAM or YUV analog video signals, in the document entitled “Specification of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999,” and (b) for a 480p progressive scan analog video signal, in the document entitled “Specification of the Macrovision AGC Copy Protection Waveforms for DVD Applications with 525p (480p) Progressive Scan Outputs, Revision 1.03 (December 22, 1999).”

- 1.7 “Certificate” means a unique WMDRM object used to assess trust .
- 1.8 “Certified Output Protection Protocol” or “COPP” enables robust signaling and content delivery mechanism between applications and video device drivers.
- 1.9 “CGMS-A” means the Copy Generation Management System (Analog) as specified (a) for NTSC analog video signals, in IEC 61880 (for inclusion on Line 20) or in EIA-608-B (for inclusion on Line 21), (b) for PAL, SECAM or YUV analog video signals, in IEC 61880 (for inclusion on Line 20) or in EIA-608-B (for inclusion on Line 21) or in EIA-805 (for inclusion on Line 41) for YUV (525/60 systems) signals or in ETS 300924 for PAL, SECAM and YUV (625/50 systems) signals, or (c) for 480p progressive scan analog video signals, in, or adapted without material change from, EIAJ CPR1204-1 (defining the signal waveform carrying the CGMS-A) and IEC 61880 (defining the bit assignment for CGMS-A).
- 1.10 “Colorstripe” means the so-named copy control system as specified for NTSC analog video signals in the document entitled “Specification of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999.”
- 1.11 “Company” means an entity licensed under a License Agreement to develop Licensed Products.
- 1.12 “Computer Product” means a device that is designed or permits the end user to install software applications thereon, including, but not limited to, personal computers, handheld “Personal Digital Assistants,” and the like.
- 1.13 “Consistent with the Microsoft Implementation” means the Licensed Product (i) provides equivalent functionality to the Microsoft Implementation, (ii) equals or exceeds the security of the Microsoft Implementation, and (iii) maintains compatibility and interoperability with the Microsoft Implementation.
- 1.14 “Content” means audio and/or video that are transmitted or distributed, either by broadcast, cablecast or other means of distribution to the general public or on demand.
- 1.15 “Content Key” means a symmetric key used to encrypt and decrypt WMDRM Content.
- 1.16 “Copy” means to transport encrypted WMDRM Content over a USB connection, to the extent permitted by applicable WMDRM Policy, to a device implementing WMDRM-PD for Passing to Outputs at any time and/or for as many times as permitted by applicable WMDRM Policy.

- 1.17 “Cryptographically Random” means unpredictable, in that no polynomial-time algorithm, given any sequence of bits, can guess the succeeding K bits with probability greater than $\frac{1}{2}^K + 1/P(K)$ for any (positive) polynomial P and sufficiently large K.
- 1.18 “DES” means Data Encryption Standard.
- 1.19 “Digital Audio Content” means sound recordings, as defined in 17 U.S.C. § 101, recorded in a digital format.
- 1.20 “Digital Audio Output” means digital audio signals conforming to IEC-958, IEC-60958, or IEC-61937.
- 1.21 “Digital Video Content” means audiovisual works, as defined in 17 U.S.C. § 101, recorded in a digital format.
- 1.22 “Digital Video Output” includes Digital Visual Interface (DVI) and High-Definition Multimedia Interface (HDMI). DVI is a digital interface standard created by the Digital Display Working Group (DDWG). HDMI includes DVI and support for digital audio. For the purposes of this definition, Digital Video Output refers to the DVI capability of HDMI. This definition applies only to the digital interface on DVI and/or HDMI and does not include DVI Analog.
- 1.23 “HDCP” means High-Bandwidth Digital Content Protection (“HDCP”) protected Output. The HDCP specification and license agreement are available from Digital Content Protection, LLC at <http://www.digital-cp.com/>.
- 1.24 “Internal Video Output” includes any display that is permanently connected to the Licensed Product, including but not limited to, a liquid crystal display (“LCD”).
- 1.25 “License Agreement” means the agreement under which Microsoft licenses entities to develop and distribute products that use the WMDRM components contained in the Windows Media Format SDK redistributable components.
- 1.26 “Licensed Product” means a hardware device or software application (or other software component, which may be a separately identifiable subset of a software application or operating system) that (i) implements Windows Media Format SDK subject to a license from Microsoft and (ii) is capable of playing back WMDRM Content.
- 1.27 “Metering” is a feature of WMDRM designed to securely collect and report content usage information.

- 1.28 “Microsoft Implementation” means the implementation of WMDRM functionality provided as source code, binaries, technical documentation, tools and/or sample files as provided to the Company under the License Agreement.
- 1.29 “Output” means Analog Audio Outputs, Analog Computer Monitor Outputs, Analog Television Outputs, Digital Audio Outputs, Digital Video Outputs, Internal Video Outputs and USB Audio Outputs. Output does not include Copying WMDRM Content over a USB connection to a device implementing WMDRM-PD or Streaming WMDRM Content to a WMDRM-ND Receiver.
- 1.30 “Output Protection Level” means a number included in WMDRM Policy that corresponds to the content protection that must be applied when Passing WMDRM Content. The Output Protection Level may be determined and assigned by the content owner or may be assigned by the WMDRM Implementation for specific categories of WMDRM Content.
- 1.31 “Pass” means to direct decrypted WMDRM Content to flow to Outputs, optionally through intermediate components such as a codec or device driver.
- 1.32 “Privacy Key” means an asymmetric public key provided by Microsoft for the purpose of encrypting sensitive communication sent over a public network.
- 1.33 “Redbook CD” means "Compact Disc Digital Audio Standard" standard, as described in CEI IEC 908.
- 1.34 “Secure Audio Path” or “SAP” means a Microsoft technology for protecting audio from the point at which it is decrypted in the WMF SDK to the point at which it is Passed to the audio device driver.
- 1.35 “Stream” means to transport encrypted WMDRM Content over a network, to the extent permitted by applicable WMDRM Policy, to a WMDRM-ND Receiver for Passing to an Output immediately or shortly after the receipt of the WMDRM Content in the WMDRM-ND Receiver.
- 1.36 “USB Audio Output” means a speaker, headphones or other sound reproduction device attached that complies with the Universal Serial Bus (USB) Audio Specification available from the USB Forum.
- 1.37 “WMDRM” means Windows Media Digital Rights Management technology.

- 1.38 “WMDRM Certificate” means a certificate provided by Microsoft for the purpose of enabling the Licensed Product to access WMDRM functionality.
- 1.39 “WMDRM Content” means audio or audiovisual content that has been encrypted and recorded using WMDRM.
- 1.40 “WMDRM Data Stores” means the secure databases required for mandatory and optional WMDRM features. This includes, but is not limited to, License Store, Secure Store, Metering Store and License Synchronization Store as described in the Microsoft Implementation.
- 1.41 “WMDRM License” means a data structure that contains, but is not limited to, WMDRM Policy and an encrypted Content Key associated with specific WMDRM Content.
- 1.42 “WMDRM Policy” means the description of the actions permitted and/or required for or with WMDRM Content and restrictions on those actions as described in the WMDRM License associated with the WMDRM Content.
- 1.43 “WMDRM Technology” means the methods for local decryption and renewability developed by Microsoft for use with Windows Media Digital Rights Management.
- 1.44 “WMDRM-ND Receiver” means a product licensed under the License Agreement for WMDRM-ND Applications that complies with the applicable Compliance Rules and may connect to WMDRM-ND Transmitters and acquire WMDRM Licenses and WMDRM Content from such WMDRM-ND Transmitters.
- 1.45 “WMDRM-ND Technical Documentation” means all of the technical documentation entitled "Implementing the Windows Media Digital Rights Management for Network Devices Protocol," as such technical documentation may be amended from time to time by Microsoft.
- 1.46 “WMDRM-ND Transmitter” means a product or application licensed or implemented by Microsoft that complies with the applicable Compliance Rules and may connect to WMDRM-ND Receivers and issue WMDRM Licenses and WMDRM Content.
- 1.47 “WMDRM-ND” means WMDRM for Network Devices.
- 1.48 “WMDRM-PD” means of WMDRM for Portable Devices.
- 1.49 “WMF SDK Technical Documentation” means documentation provided with the WMF SDK.

1.50 “WMF SDK” means Windows Media Format Software Development Kit.

2. SCOPE. These Compliance Rules apply to Licensed Products that make use of the WMDRM functionality included in the WMF SDK. These Compliance Rules set forth the requirements pursuant to which licensed software applications running on the WMF SDK may transfer, play back or render, and Output WMDRM Content.

3. REQUIREMENTS FOR COMPLYING WITH WMDRM POLICY

3.1 **Unspecified policy.** WMDRM Policy may specify additional rights, restrictions or parameters that are not covered in these Compliance Rules. Nevertheless Licensed Products must only take action based on rights and must enforce only restrictions covered in this document. To the extent that WMDRM Policy (or a particular WMDRM License) describes additional rights, restrictions or parameters that are not described in these Compliance Rules, Licensed Products must ignore such additional rights, restrictions or parameters.

3.2 DRM Certificates

3.2.1 **Unique Certificate.** Company shall request from Microsoft and use a unique WMDRM Certificate for each major version of Licensed Products released by Company. If more than three months have elapsed from the Company’s last release of a Licensed Product, Company shall obtain from Microsoft a new WMDRM Certificate prior to Company’s releasing a new version of a Licensed Product and shall incorporate such new WMDRM Certificate in the next release of any Licensed Product.

3.2.2 **Certificate Implementation.** Company shall statically link the WMDRM Certificate into Licensed Products. Company shall use the WMDRM Certificate solely to enable Licensed Products to interoperate with the WMF SDK.

3.2.3 **Revocation.** If a Licensed Product receives the NS_E_DRM_APPCERT_REVOKED or NS_E_DRM_LICENSE_APP_NOTALLOWED error from WMDRM, Licensed Product must either (A) invoke an internal upgrade mechanism to restore the security of the Licensed Product, or (B) direct the user to a Company web site page that explains the security compromise and how to restore the security of the Licensed Product and allows the user to reinstate complete functionality of the Licensed Product.

3.3 **Individualization.** “Individualization” is the process of downloading and installing from a Microsoft service unique WMDRM component(s) for the purpose of improving security of WMDRM. Licensed Products supporting Direct License Acquisition functionality must initiate Individualization (A) during setup, (B) by end-user invocation, or (C) when Licensed Product receives one of the following error codes: WMT_NEEDS_INDIVIDUALIZATION or

NS_E_DRM_NEEDS_INDIVIDUALIZATION. When initiating a Security Upgrade, Microsoft recommends that each Licensed Product adhere to the user interface conventions for WMDRM Security Upgrades posted on <http://go.microsoft.com/fwlink/?LinkId=9265> in the section labeled "Privacy and the Windows Media Format SDK". Licensed Products must first receive an end user's explicit informed consent before performing a Security Upgrade.

3.4 Encryption. "Personal WMDRM" is the process of encrypting content into WMDRM Content and creating a WMDRM License bound to the local machine. If a Licensed Product encrypts WMDRM Content using the Personal WMDRM feature of WMDRM, Licensed Product must specify only rights for which pre-defined constants beginning with WMT_RIGHT exist in the WMF SDK. For avoidance of doubt, specifying WMT_RIGHT_PLAYBACK is allowed and specifying 0xFFFF is disallowed.

3.5 COPP Support. Licensed Products that Pass the video portion of WMDRM Content to Outputs under the Play policy specified in Section 4 must implement support for COPP. Licensed Products must engage COPP to confirm that the required Output protection is enabled as required in section 4.2.

3.5.1 Application Programming Interfaces (APIs). Licensed Products meeting the conditions of section 3.5 must use the APIs exposed by the DirectShow Video Mixing Renderer (VMR) 7 or 9 to establish the secure channel to the COPP-complaint graphics driver, and to send or receive COPP command or status information. These APIs are described in Section 7 of the Certified Output Protection Protocol (HDCP, CGMS-A and Analog Copy Protection Support) Technical Documentation. The VMR provides a new interface, IAMCertifiedOutputProtection, and associated data structures for this purpose. Methods on the interface are:

3.5.1.1 KeyExchange() – initiate the cryptographic key exchange with the driver, retrieving its generated random number and digital certificate

3.5.1.2 SessionSequenceStart() – provide driver random number, session data integrity key, and command and status sequence starting random numbers to driver for completion of key exchange

3.5.1.3 ProtectionCommand() – issue formatted command to driver for setting desired Output protection states

3.5.1.4 ProtectionStatus() – retrieve formatted data block containing requested status information from driver

3.5.2 Revocation List. Licensed Products must not Pass WMDRM Content if the COPP driver's certificate appears on the COPP driver CRL, which can be retrieved by calling IWMDRMReader::GetDRMProperty() with a value of g_wszWMDRMNet_Revocation.

3.5.3 **Exception.** Licensed Products that implement support for only Collaborative Play policy as defined in Section 5 are not required to implement COPP or support Output Protection Levels.

4. PLAYBACK AND OUTPUT CONTROL RULES FOR LICENSED PRODUCTS

Licensed Products must comply with the following:

4.1 **Playback Control.** Licensed Products must comply with the following rules for playback control:

4.1.1 **Playback.** Licensed Products may Pass decrypted, decompressed WMDRM Content through the Outputs described in Section 4.2 and 4.3 only if the right to Play is specified in a WMDRM License associated with the WMDRM Content. Licensed Products may verify this by specifying `g_wszWMDRM_ActionAllowed_Playback` when calling `IWMDRMReader::SetDRMProperty()` or specifying `WMT_RIGHT_PLAYBACK` when calling `WMCreateReader()`.

4.2 **Restricted Outputs.** Licensed Products must detect and accurately respond to the Output Protection Levels for WMDRM Content. Licensed Products that Playback content must call `IWMDRMReader2::SetEvaluateOutputLevelLicenses(TRUE)` to specify that the application handles Output Protection Levels and `IWMDRMReader2::GetPlayOutputLevels()` to determine what, if any, Output Protection Levels are associated with the WMDRM License.

4.2.1 **Output Control for Digital Compressed Audio Content.** If a Licensed Product Passes compressed Digital Audio Content, the Licensed Product must follow restrictions as specified in the WMDRM License by querying for Output Protection Levels as described above and responding based on the value of `DRM_MINIMUM_OUTPUT_PROTECTION_LEVELS.wCompressedDigitalAudio`

4.2.1.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may Pass without restriction compressed Digital Audio Content of such decrypted WMDRM Content to Audio Outputs.

4.2.1.2 **Level 101 to 200.** If the Output Protection Level specified in the WMDRM License is greater than 100 and less than or equal to 200, Licensed Products may Pass compressed Digital Audio Content of decrypted WMDRM Content only using Secure Audio Path. Licensed Product must engage SAP by calling `IWMDRMReader::SetDRMProperty()` with the parameters `g_wszWMSAPLevel` and 200. Digital compressed audio portion of such decrypted WMDRM Content may be Passed to Digital Audio Outputs.

4.2.1.3 **Level 201 to 300.** If the Output Protection level specified in the WMDRM Licenses is greater than 200 and less than or equal to 300, Licensed Products may Pass compressed Digital Audio Content of decrypted WMDRM Content only using Secure Audio Path. Licensed Product must engage SAP by calling `IWMDRMReader::SetDRMProperty()` with the parameters `g_wszWMSAPLevel` and 300. Digital compressed audio portion of such decrypted WMDRM Content must not be Passed to Digital Audio Outputs.

4.2.1.4 **Level 301 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not Pass compressed Digital Audio Content of decrypted WMDRM Content.

4.2.2 **Output Control for Digital Uncompressed Audio Content.** If a Licensed Product Passes digital uncompressed audio, the Licensed Product must follow restrictions as specified in the WMDRM License by querying for Output Protection Levels as described above and responding based on the value of `DRM_MINIMUM_OUTPUT_PROTECTION_LEVELS.wUncompressedDigitalAudio`

4.2.2.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may Pass without restriction uncompressed Digital Audio Content of such decrypted WMDRM Content to Audio Outputs.

4.2.2.2 **Level 101 to 200.** If the Output Protection Level specified in the WMDRM Licenses is greater than 100 and less than or equal to 200, Licensed Products may Pass uncompressed Digital Audio Content of decrypted WMDRM Content only using Secure Audio Path. Licensed Product must engage SAP by calling `IWMDRMReader::SetDRMProperty()` with the parameters `g_wszWMSAPLevel` and 200. Digital uncompressed audio portion of such decrypted WMDRM Content may be Passed to Digital Audio Outputs.

4.2.2.3 **Level 201 to 300.** If the Output Protection Level specified in the WMDRM License is greater than 200 and less than or equal to 300, Licensed Products may Pass uncompressed Digital Audio Content of decrypted WMDRM Content only using Secure Audio Path. Licensed Product must engage SAP by calling `IWMDRMReader::SetDRMProperty()` with the parameters `g_wszWMSAPLevel` and 300. Digital uncompressed audio portion of such decrypted WMDRM Content must not be Passed to Digital Audio Outputs.

4.2.2.4 **Level 301 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not Pass uncompressed Digital Audio Content of decrypted WMDRM Content.

4.2.3 **Output Control for Digital Compressed Video Content.** Licensed Products must not Pass decrypted Digital Compressed Video Content to any Output, except that a Licensed Product may Pass Content marked with the ATSC

Standard A/65B Redistribution Control descriptor (rc_descriptor()) to any Output protected by a digital content protection technology approved by the Federal Communications Commission (or otherwise approved in accordance with applicable Federal Communications Commission rules) for use with such Content.

4.2.4 Output Control for Digital Uncompressed Video Content. If a Licensed Product Passes uncompressed Digital Video Content, Licensed Products must follow restrictions as specified in the WMDRM License by querying for Output Protection Levels as described above and responding based on the value of DRM_MINIMUM_OUTPUT_PROTECTION_LEVELS.wUncompressedDigitalVideo.

4.2.4.1 Level 0 to 100. If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may Pass, without restriction, the uncompressed Digital Video Content of decrypted WMDRM Content on Video Outputs.

4.2.4.2 Level 101 to 300. If the Output Protection Level specified in the WMDRM Licenses is greater than 100 and less than or equal to 300 and Licensed Products is Passing Digital Video Content to Digital Video Outputs, Licensed Products must engage HDCP using COPP to protect the uncompressed Digital Video Content of decrypted WMDRM Content. Licensed Products must verify using COPP that the HDCP Source Function is engaged and able to deliver protected content, which means HDCP encryption is operational on such Output.

4.2.4.3 Level 301 or greater. If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not Pass uncompressed Digital Video Content of decrypted WMDRM Content on Digital Video Outputs.

4.2.5 Output Control for Analog Video Content. If a Licensed Product Passes the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs, the Licensed Product must follow restrictions as specified in the WMDRM License by querying for Output Protection Levels and responding based on the value of DRM_MINIMUM_OUTPUT_PROTECTION_LEVELS.wAnalogVideo. Additional restrictions may be required as specified in Section 4.2.6.

4.2.5.1 Level 0 to 100. If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may Pass without restriction the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs.

4.2.5.2 Level 101 to 200. If the Output Protection Level specified in the WMDRM Licenses is greater than 100 but less than or equal to 200 and Licensed Products is Passing the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs, Licensed Products must engage CGMS-A using COPP with the CGMS field in the copy set to '11' ("no more copies").

4.2.5.3 Level 201 or greater. If the Output Protection Level specified in the WMDRM License exceeds 200, Licensed Products must not Pass the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs.

4.2.6 Output Control for Extended Analog Video Content. If a Licensed Product Passes the video portion of decrypted WMDRM Content to Analog Television Outputs, the Licensed Product must follow restrictions as specified in the WMDRM License by querying for Output Protection Levels and taking appropriate action as described below. Additional restrictions may be required as specified in Section 4.2.5

4.2.6.1 Automatic Gain Control and ColorStripe. If a Licensed Product is Passing the video portion of decrypted WMDRM Content to Analog Television Outputs and any DRM_VIDEO_OUTPUT_PROTECTION.guidID has a value of “C3FD11C6-F8B7-4d20-B008-1DB17D61F2DA”, the Licensed Product must engage Automatic Gain Control and ColorStripe via COPP and specify for the value of DRM_VIDEO_OUTPUT_PROTECTION.bConfigData for the APSTB field. Additional technologies and restrictions may be required as specified in Section 4.2.5. For avoidance of doubt, the value of bConfigData for AGC and ColorStripe is as follows:

APSTB values	Description	NTSC	PAL
00	AGC and ColorStripe	Off	Off
01	AGC Only	APS1	APS1
10	AGC and 2 line ColorStripe	APS2	APS1
11	AGC and 4 line ColorStripe	APS3	APS1

4.3 Unrestricted Outputs. Licensed Products may Pass without restriction WMDRM Content to the following Outputs provided the requirements in Section 4.2 are met.

4.3.1 Analog Audio Outputs. Licensed Products may Pass without restriction the Analog Audio Content of decrypted WMDRM Content to Analog Audio Outputs.

4.3.2 USB Audio Outputs. Licensed Products may Pass without restriction the uncompressed Digital Audio Content of decrypted WMDRM Content to USB Audio Outputs.

4.3.3 Analog Computer Monitor Outputs. Licensed Products may Pass without restriction the uncompressed Analog Video Content of decrypted WMDRM Content to Analog Computer Monitor Outputs.

4.3.4 Internal Video Outputs. Licensed Products may Pass without restriction the uncompressed Digital Video Content of decrypted WMDRM Content to Internal Video Outputs.

5. COLLABORATIVE PLAY RULES FOR LICENSED PRODUCTS

5.1.1 Requesting Rights. Licensed Products that will Pass decrypted the audio and/or video portion of WMDRM Content using the Collaborative Play model must request the `g_wszWMDRM_ActionAllowed_CollaborativePlay` right via calls to `IWMDRMReader::SetDRMProperty()`. If the return code is anything other than `S_OK`, Licensed Products must not Pass the WMDRM Content.

5.1.2 Re-encode. Licensed Products that Pass compressed Digital Audio Content of decrypted WMDRM Content or compressed Digital Video Content of decrypted WMDRM Content using the Collaborative Play model must degrade the quality of Digital Audio Content and/or Digital Video Content before WMDRM Content is transmitted.

5.1.2.1 Audio Encoding. Licensed Products must re-compress the Audio portion of WMDRM Content with the Windows Media Audio codec, specifying a maximum bit rate of 64Kbps, 44.1 KHz and 16-bit Stereo.

5.1.2.2 Video Encoding. Licensed Products must re-compress the Video portion of WMDRM Content with the Windows Media Video codec, with the maximum bit rate in Kbps not exceeding the product of the horizontal resolution, vertical resolution and the value four (4), but in no case to exceed 512Kbps. For example, the maximum bit rate for a resolution of 320x240 will be 300Kbps. The maximum frame rate must not exceed 30fps.

5.1.3 Re-encryption. Licensed Products must encrypt the re-encoded audio and/or video portion of WMDRM Content using DES encryption with a minimum key length of 56-bit or AES with a minimum key length of 128-bit. The Licensed Product must use a random number generator that is Cryptographically Random to generate strong symmetric keys for content encryption.

5.1.4 Key Management. Licensed Products must distribute Content Keys to other Licensed Products in a secure manner. Licensed Products must distribute content keys only to other Licensed Products that are known to be secure and to comply with these Compliance Rules. Licensed Products must not tamper with the License Acquisition URL and content metadata.

5.1.5 Concurrent Playback. Licensed Products may Pass collaborative audio and/or video WMDRM Content only to Outputs while connected to other Licensed Products and only while the Licensed Product that was the source of the WMDRM Content is also concurrently Passing the Content to Outputs. Licensed Products must limit to a maximum of ten (10) the number of Licensed Products that can concurrently Pass the audio and/or video portion of decrypted WMDRM Content to Outputs.

5.1.6 Protocol. Licensed Products must use a protocol that is proven to be robust against common attacks including “man in the middle” and replay attacks. Licensed Products must declare themselves to the group when joining a peer group. Licensed Products must not share WMDRM Content with other Licensed Products until the Licensed Products to receive the Content have declared themselves to the peer group and the Licensed Product that will be Passing the Content has verified that the maximum number of members in the group does not exceed ten (10).

5.1.7 Purchase Option. Licensed Products must provide the end user with a purchase option when the audio and/or video portion of WMDRM Content is being Passed to Outputs. This mechanism must be prominent and available for the user to select at any time. When a user invokes this mechanism, Licensed Products may direct the user to a default service supported by the Licensed Product. If the content is unavailable through the default service, the Licensed Product must direct the user to a web site using the License Acquisition URL. The License Acquisition URL may be retrieved for the WMDRM Content being Passed using the API `IWM DRMReader::GetDRMProperty()` with a parameter of `g_wszWMDRM_DRMHeader_LicenseAcqURL`.

6. REDBOOK CD BURNING RULES FOR LICENSED PRODUCTS

6.1 Redbook CD Burning

6.1.1 Licensed Products may Pass the decompressed audio portion of decrypted WMDRM Content to a CD-R or CD-RW drive for the purpose of creating a Redbook Audio CD only if the WMDRM License permits such CD burning and only in the manner described in this Section 6.1.

6.1.2 Licensed Products may temporarily cache the decompressed audio portion of decrypted WMDRM Content prior to beginning to master a Redbook CD, provided that the decrypted content is stored as part of a single file and the temporary cached copy is hidden and deleted from Persistent Storage once the operation is complete. The single file must prevent playback by widely available media playback software.

6.2 Requesting Burn permission. Licensed Products must first call `IWMReaderPlaylistBurn::InitPlaylistBurn` to initialize the Playlist Burning interface and

must Pass a complete list of files to be burned including the fully qualified path and filename to the files.

6.3 Verify Permission. Licensed Products must next call `IWMReaderPlaylistBurn::GetInitResults` to determine whether the Licensed Product may proceed with burning the specified playlist. If the return code of `GetInitResults` includes any value other than `S_OK`, Licensed Products must not burn the playlist.

6.4 Finalizing burn. Licensed Products must call `IWMReaderPlaylistBurn::EndPlaylistBurn` after the entire playlist has been burned successfully. If an unrecoverable error occurs before the last track in the Playlist has been Burned, Licensed Products are not required to call `IWMReaderPlaylistBurn::EndPlaylistBurn`.

7. RULES FOR COPYING TO LICENSED PRODUCTS

7.1 Copy to Device. Licensed Products may not Copy or transfer WMDRM Content to a portable device except by using the WM Device Manager functionality in the WMF SDK.

8. RULES FOR STREAMING TO LICENSED PRODUCTS

8.1 WMDRM-ND Protocol Messages.

8.1.1 Implementation. Licensed Products must implement all WMDRM-ND Protocol Messages Consistent with the Microsoft Implementation.

8.1.2 Data. Licensed Products must not modify or augment the data within the WMDRM-ND Protocol Messages as described in the Microsoft Implementation.

8.2 Limiting Concurrent WMDRM-ND Receivers

8.2.1 Opening WMDRM-ND Receivers. A Licensed Product must call `IWMRegisteredDevice::Open` prior to Streaming WMDRM Content to a WMDRM-ND Receiver.

8.2.2 Closing WMDRM-ND Receivers. A Licensed Product must call `IWMRegisteredDevice::Close` after the Licensed Product has completed Streaming the WMDRM Content to the open WMDRM-ND Receiver. A Licensed Product must call `IWMRegisteredDevice::Close` except in the case of a fatal application error.

COMPLIANCE RULES FOR FOR WMF SDK WMDRM APPLICATIONS

1. DEFINITIONS

The following terms have the meanings set forth below. Other initially capitalized terms not defined in these Compliance Rules have the meanings ascribed to them in the License Agreement and the Microsoft Implementation.

- 1.1 “AES” means Advanced Encryption Standard.
- 1.2 “Analog Audio ~~Outputs~~Output” means a connector for an analog sound reproduction device such as a speaker or headphones. For avoidance of doubt, this includes both external jacks to connect speakers and/or headphones and built-in speakers and/or headphones.
- 1.3 “Analog Computer Monitor Output” means a connector for an analog monitor that is typically found and associated with a Computer Product and that carries uncompressed analog video signals. The term expressly includes those outputs known as VGA, SVGA, XGA, DVI Analog, and various non-standardized analog monitor connections that have been implemented by manufacturers, and expressly does not include such typical consumer electronics connectors as NTSC, PAL, SECAM, SCART, YPrPb, S-Video and Consumer RGB, whether or not such connectors are found on any Computer Product.
- 1.4 “Analog Protection System (APS) trigger bits (APSTB)” means the Analog Protection System bits as specified (a) for NTSC video signals, in IEC 61880 (for inclusion of such value on Line 20) or EIA-608-B (for inclusion of such value on Line 21) or (b) for YUV (525/60 systems) signals, in IEC 61880 (for inclusion of such value on Line 20) or EIA-608-B (for inclusion of such value on Line 21).
- 1.5 “Analog Television Output” means such typical consumer electronics analog connectors as NTSC, PAL, SECAM, SCART, YPrPb, S-Video and Consumer RGB.
- ~~1.6 “Approved Outputs” means Analog Audio Outputs, Analog Computer Monitor Outputs, Analog Television Outputs, Digital Audio Outputs, Digital Video Outputs, Internal Video Outputs and USB Audio Outputs.~~
- 1.6 ~~1.7~~ “Automatic Gain Control (AGC)” means the so-named copy control system as specified (a) for NTSC, PAL, SECAM or YUV analog video signals, in the document entitled “Specification of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999,” and (b) for a 480p progressive scan analog video signal, in the

document entitled “Specification of the Macrovision AGC Copy Protection Waveforms for DVD Applications with 525p (480p) Progressive Scan Outputs, Revision 1.03 (December 22, 1999).”

- 1.7 ~~1.8~~ “Certificate” means a unique WMDRM object used to assess trust .
- 1.8 ~~1.9~~ “Certified Output Protection Protocol” or “COPP” enables robust signaling and content delivery mechanism between applications and video device drivers.
- 1.9 ~~1.10~~ “CGMS-A” means the Copy Generation Management System (Analog) as specified (a) for NTSC analog video signals, in IEC 61880 (for inclusion on Line 20) or in EIA-608-B (for inclusion on Line 21), (b) for PAL, SECAM or YUV analog video signals, in IEC 61880 (for inclusion on Line 20) or in EIA-608-B (for inclusion on Line 21) or in EIA-805 (for inclusion on Line 41) for YUV (525/60 systems) signals or in ETS 300924 for PAL, SECAM and YUV (625/50 systems) signals, or (c) for 480p progressive scan analog video signals, in, or adapted without material change from, EIAJ CPR1204-1 (defining the signal waveform carrying the CGMS-A) and IEC 61880 (defining the bit assignment for CGMS-A).
- 1.10 ~~1.11~~ “Colorstripe” means the so-named copy control system as specified for NTSC analog video signals in the document entitled “Specification of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999.”
- 1.11 ~~1.12~~ “Company” means an entity licensed under a License Agreement to develop Licensed Products.
- 1.12 ~~1.13~~ “Computer Product” means a device that is designed or permits the end user to install software applications thereon, including, but not limited to, personal computers, handheld “Personal Digital Assistants,” and the like.
- 1.13 ~~1.14~~ “Consistent with the Microsoft Implementation” means the Licensed Product (i) provides equivalent functionality to the Microsoft Implementation, (ii) equals or exceeds the security of the Microsoft Implementation, and (iii) maintains compatibility and interoperability with the Microsoft Implementation.
- ~~1.15~~ “~~Content Key~~” means a symmetric key used to ~~decrypt~~ **WMDRM Content**.

- 1.14 ~~1.16~~ “Content” means audio and/or video that are transmitted or distributed, either by broadcast, cablecast or other means of distribution to the general public or on demand.
- 1.15 “Content Key” means a symmetric key used to encrypt and decrypt WMDRM Content.
- 1.16 “Copy” means to transport encrypted WMDRM Content over a USB connection, to the extent permitted by applicable WMDRM Policy, to a device implementing WMDRM-PD for Passing to Outputs at any time and/or for as many times as permitted by applicable WMDRM Policy.
- 1.17 “Cryptographically Random” means unpredictable, in that no polynomial-time algorithm, given any sequence of bits, can guess the succeeding K bits with probability greater than $\frac{1}{2}^K + 1/P(K)$ for any (positive) polynomial P and sufficiently large K.
- 1.18 ~~1.17~~ “DES” means Data Encryption Standard.
- ~~1.18~~ ~~“Device Private Key” means a unique, Cryptographically Random asymmetric private key generated by or for Licensed Products for the purpose of decrypting Content Keys.~~
- 1.19 “Digital Audio Content” means sound recordings, as defined in 17 U.S.C. § 101, recorded in a digital format.
- 1.20 “Digital Audio Output” means digital audio signals conforming to IEC-958, IEC-60958, or IEC-61937.
- 1.21 “Digital Video Content” means audiovisual works, as defined in 17 U.S.C. § 101, recorded in a digital format.
- 1.22 “Digital Video Output” includes Digital Visual Interface (DVI) and High-Definition Multimedia Interface (HDMI). DVI is a digital interface standard created by the Digital Display Working Group (DDWG). HDMI includes DVI and support for digital audio. For the purposes of this definition, Digital Video Output refers to the DVI capability of HDMI. This definition applies only to the digital interface on DVI and/or HDMI and does not include DVI Analog.
- 1.23 “HDCP” means High-Bandwidth Digital Content Protection (“HDCP”) protected ~~output~~Output. The HDCP specification and license agreement are available from Digital Content Protection, LLC at <http://www.digital-cp.com/>.

- 1.24 “Internal Video Output” includes any display that is permanently connected to the Licensed Product, including but not limited to, a liquid crystal display (“LCD”).
- 1.25 “License Agreement” means the agreement under which Microsoft licenses entities to develop and distribute products that ~~include and~~ use the WMDRM components contained in the Windows Media Format SDK redistributable components.
- 1.26 “Licensed Product” means a hardware device or software application (or other software component, which may be a separately identifiable subset of a software application or operating system) that (i) implements Windows Media Format SDK subject to a license from Microsoft and (ii) is capable of playing back WMDRM Content.
- 1.27 “Metering” is a feature of WMDRM designed to securely collect and report content usage information.
- 1.28 “Microsoft Implementation” means the implementation of WMDRM functionality provided as source code, binaries, technical documentation, tools and/or sample files as provided to the Company under the License Agreement.
- 1.29 “Output” means Analog Audio Outputs, Analog Computer Monitor Outputs, Analog Television Outputs, Digital Audio Outputs, Digital Video Outputs, Internal Video Outputs and USB Audio Outputs. Output does not include Copying WMDRM Content over a USB connection to a device implementing WMDRM-PD or Streaming WMDRM Content to a WMDRM-ND Receiver.
- 1.30 ~~1.29~~ “Output Protection Level” means a number included in WMDRM Policy that corresponds to the content protection that must be applied when ~~passing~~Passing WMDRM Content. The Output Protection Level may be determined and assigned by the content owner or may be assigned by the WMDRM Implementation for specific categories of WMDRM Content.
- 1.31 “Pass” means to direct decrypted WMDRM Content to flow to Outputs, optionally through intermediate components such as a codec or device driver.
- 1.32 ~~1.30~~ “Privacy Key” means an asymmetric public key provided by Microsoft for the purpose of encrypting sensitive communication sent over a public network.

- 1.33** ~~1.31~~—“Redbook CD” means "Compact Disc Digital Audio Standard" standard, as described in CEI IEC 908.
- 1.34** ~~1.32~~—“Secure Audio Path” or “SAP” means a Microsoft technology for protecting audio from the point at which it is decrypted in the WMF SDK to the point at which it is ~~passed~~Passed to the audio device driver.
- 1.35** “Stream” means to transport encrypted WMDRM Content over a network, to the extent permitted by applicable WMDRM Policy, to a WMDRM-ND Receiver for Passing to an Output immediately or shortly after the receipt of the WMDRM Content in the WMDRM-ND Receiver.
- 1.36** ~~1.33~~—“USB Audio Output” means a speaker, headphones or other sound reproduction device attached that complies with the Universal Serial Bus (USB) Audio Specification available from the USB Forum.
- 1.37** ~~1.34~~—“WMDRM” means Windows Media Digital Rights Management technology.
- 1.38** ~~1.35~~—“WMDRM Certificate” means a certificate provided by Microsoft for the purpose of enabling the Licensed Product to access WMDRM functionality.
- 1.39** ~~1.36~~—“WMDRM Content” means audio or audiovisual content that has been encrypted and recorded using WMDRM.
- 1.40** ~~1.37~~—“WMDRM Data Stores” means the secure databases required for mandatory and optional WMDRM features. This includes, but is not limited to, License Store, Secure Store, Metering Store and License Synchronization Store as described in the Microsoft Implementation.
- 1.41** ~~1.38~~—“WMDRM License” means a data structure that contains, but is not limited to, WMDRM Policy and an encrypted Content Key associated with specific WMDRM Content.
- 1.42** ~~1.39~~—“WMDRM Policy” means the description of the actions permitted and/or required for or with WMDRM Content and restrictions on those actions as described in the WMDRM License associated with the WMDRM Content.
- 1.43** ~~1.40~~—“WMDRM Technology” means the methods for local decryption and renewability developed by Microsoft for use with Windows Media Digital Rights Management.
- 1.44** ~~1.41~~—“WMDRM-ND Receiver” means a product licensed under the License Agreement for WMDRM-ND Applications that complies with the

applicable Compliance Rules and may connect to WMDRM-ND Transmitters and acquire WMDRM Licenses and WMDRM Content from such WMDRM-ND Transmitters.

1.45 ~~1.42~~ “WMDRM-ND Technical Documentation” means all of the technical documentation entitled "Implementing the Windows Media Digital Rights Management for Network Devices Protocol," as such technical documentation may be amended from time to time by Microsoft.

1.46 ~~1.43~~ “WMDRM-ND Transmitter” means a product or application licensed or implemented by Microsoft that complies with the applicable Compliance Rules and may connect to WMDRM-ND Receivers and issue WMDRM Licenses and WMDRM Content.

1.47 ~~1.44~~ “WMDRM-ND” means WMDRM for Network Devices.

1.48 ~~1.45~~ “WMDRM-PD” means of WMDRM for Portable Devices.

1.49 ~~1.46~~ “WMF SDK Technical Documentation” means documentation provided with the WMF SDK.

1.50 ~~1.47~~ “WMF SDK” means Windows Media Format Software Development Kit.

2. SCOPE. These Compliance Rules apply to Licensed Products that make use of the WMDRM functionality included in the WMF SDK. These Compliance Rules set forth the requirements pursuant to which licensed software applications running on the WMF SDK may transfer, play back or render, and ~~output~~Output WMDRM Content.

3. REQUIREMENTS FOR COMPLYING WITH WMDRM POLICY

3.1 **Unspecified policy.** WMDRM Policy may specify additional rights, restrictions or parameters that are not covered in these Compliance Rules. Nevertheless Licensed Products must only take action based on rights and must enforce only restrictions covered in this document. To the extent that WMDRM Policy (or a particular WMDRM License) describes additional rights, restrictions or parameters that are not described in these Compliance Rules, Licensed Products must ignore such additional rights, restrictions or parameters.

3.2 DRM Certificates

3.2.1 **Unique Certificate.** Company shall request from Microsoft and use a unique WMDRM Certificate for each major version of Licensed Products released by Company. If more than three months have elapsed from the Company’s last release of a Licensed Product, Company shall obtain from Microsoft a new WMDRM Certificate

prior to Company's releasing a new version of a Licensed Product and shall incorporate such new WMDRM Certificate in the next release of any Licensed Product.

3.2.2 Certificate Implementation. Company shall statically link the WMDRM Certificate into Licensed Products. Company shall use the WMDRM Certificate solely to enable Licensed Products to interoperate with the WMF SDK.

3.2.3 Revocation. If a Licensed Product receives the NS_E_DRM_APPCERT_REVOKED or NS_E_DRM_LICENSE_APP_NOTALLOWED error from WMDRM, Licensed Product must either (A) invoke an internal upgrade mechanism to restore the security of the Licensed Product, or (B) direct the user to a Company web site page that explains the security compromise and how to restore the security of the Licensed Product and allows the user to reinstate complete functionality of the Licensed Product.

3.3 Individualization. "Individualization" is the process of downloading and installing from a Microsoft service unique WMDRM component(s) for the purpose of improving security of WMDRM. Licensed Products supporting Direct License Acquisition functionality must initiate Individualization (A) during setup, (B) by end-user invocation, or (C) when Licensed Product receives one of the following error codes: WMT_NEEDS_INDIVIDUALIZATION or NS_E_DRM_NEEDS_INDIVIDUALIZATION. When initiating a Security Upgrade, Microsoft recommends that each Licensed Product adhere to the user interface conventions for WMDRM Security Upgrades posted on <http://go.microsoft.com/fwlink/?LinkId=9265> in the section labeled "Privacy and the Windows Media Format SDK". Licensed Products must first receive an end user's explicit informed consent before performing a Security Upgrade.

3.4 Encryption. "Personal WMDRM" is the process of encrypting content into WMDRM Content and creating a WMDRM License bound to the local machine. If a Licensed Product encrypts WMDRM Content using the Personal WMDRM feature of WMDRM, Licensed Product must specify only rights for which pre-defined constants beginning with WMT_RIGHT exist in the WMF SDK. For avoidance of doubt, specifying WMT_RIGHT_PLAYBACK is allowed and specifying 0xFFFF is disallowed.

3.5 COPP Support. Licensed Products that ~~pass~~Pass the video portion of WMDRM Content to ~~Approved~~ Outputs under the Play policy specified in Section 4 must implement support for COPP. Licensed Products must engage COPP to confirm that the required ~~output~~Output protection is enabled as required in section 4.2.

3.5.1 Application Programming Interfaces (APIs). Licensed Products meeting the conditions of section 3.5 must use the APIs exposed by the DirectShow Video Mixing Renderer (VMR) 7 or 9 to establish the secure channel to the COPP-complaint graphics driver, and to send or receive COPP command or status information. These APIs are described in Section 7 of the Certified Output Protection Protocol

(HDCP, CGMS-A and Analog Copy Protection Support) Technical Documentation. The VMR provides a new interface, IAMCertifiedOutputProtection, and associated data structures for this purpose. Methods on the interface are:

3.5.1.1 KeyExchange() – initiate the cryptographic key exchange with the driver, retrieving its generated random number and digital certificate

3.5.1.2 SessionSequenceStart() – provide driver random number, session data integrity key, and command and status sequence starting random numbers to driver for completion of key exchange

3.5.1.3 ProtectionCommand() – issue formatted command to driver for setting desired ~~output~~Output protection states

3.5.1.4 ProtectionStatus() – retrieve formatted data block containing requested status information from driver

3.5.2 **Revocation List.** Licensed Products must ~~compare~~not Pass WMDRM Content if the COPP driver's certificate ~~against~~appears on the COPP ~~Driver—revocation—list~~driver CRL, which can be retrieved by calling IWMDRMReader::GetDRMProperty() with a value of g_wszWMDRMNet_Revocation.

3.5.3 **Exception.** Licensed Products that implement support for only Collaborative Play policy as defined in Section 5 are not required to implement COPP or support Output Protection Levels.

4. PLAYBACK AND OUTPUT CONTROL RULES FOR LICENSED PRODUCTS

Licensed Products must comply with the following:

4.1 **Playback Control.** Licensed Products must comply with the following rules for playback control:

4.1.1 **Playback.** Licensed Products may ~~pass~~Pass decrypted, decompressed WMDRM Content through the ~~outputs~~Outputs described in Section 4.2 and 4.3 only if the right to Play is specified in a WMDRM License associated with the WMDRM Content. Licensed Products may verify this by specifying g_wszWMDRM_ActionAllowed_Playback when calling IWMDRMReader::SetDRMProperty() or specifying WMT_RIGHT_PLAYBACK when calling WMCreateReader().

4.2 **Restricted Outputs.** Licensed Products must detect and accurately respond to the Output Protection Levels for WMDRM Content. Licensed Products that Playback content must call IWMDRMReader2::SetEvaluateOutputLevelLicenses(TRUE) to specify that the application handles Output Protection Levels and

IWMDRMReader2::GetPlayOutputLevels() to determine what, if any, Output Protection Levels are associated with the WMDRM License.

4.2.1 Output Control for Digital Compressed Audio Content. If a Licensed Product **passes**Passes compressed Digital Audio Content, the Licensed Product must follow restrictions as specified in the WMDRM License by querying for Output Protection Levels as described above and responding based on the value of DRM_MINIMUM_OUTPUT_PROTECTION_LEVELS.wCompressedDigitalAudio

4.2.1.1 Level 0 to 100. If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may **pass**Pass without restriction compressed Digital Audio Content of such decrypted WMDRM Content to Audio Outputs.

4.2.1.2 Level 101 to 200. If the Output Protection Level specified in the WMDRM License is greater than 100 and less than or equal to 200, Licensed Products may **pass**Pass compressed Digital Audio Content of decrypted WMDRM Content only using Secure Audio Path. Licensed Product must engage SAP by calling IWMDRMReader::SetDRMProperty() with the parameters g_wszWMSAPLevel and 200. Digital compressed audio portion of such decrypted WMDRM Content may be **passed**Passed to Digital Audio Outputs.

4.2.1.3 Level 201 to 300. If the Output Protection level specified in the WMDRM Licenses is greater than 200 and less than or equal to 300, Licensed Products may **pass**Pass compressed Digital Audio Content of decrypted WMDRM Content only using Secure Audio Path. Licensed Product must engage SAP by calling IWMDRMReader::SetDRMProperty() with the parameters g_wszWMSAPLevel and 300. Digital compressed audio portion of such decrypted WMDRM Content must not be **passed**Passed to Digital Audio Outputs.

4.2.1.4 Level 301 or greater. If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not **pass**Pass compressed Digital Audio Content of decrypted WMDRM Content.

4.2.2 Output Control for Digital Uncompressed Audio Content. If a Licensed Product **passes**Passes digital uncompressed audio, the Licensed Product must follow restrictions as specified in the WMDRM License by querying for Output Protection Levels as described above and responding based on the value of DRM_MINIMUM_OUTPUT_PROTECTION_LEVELS.wUncompressedDigitalAudio

4.2.2.1 Level 0 to 100. If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may **pass**Pass without restriction uncompressed Digital Audio Content of such decrypted WMDRM Content to Audio Outputs.

4.2.2.2 **Level 101 to 200.** If the Output Protection Level specified in the WMDRM Licenses is greater than 100 and less than or equal to 200, Licensed Products may ~~pass~~Pass uncompressed Digital Audio Content of decrypted WMDRM Content only using Secure Audio Path. Licensed Product must engage SAP by calling `IWMDRMReader::SetDRMProperty()` with the parameters `g_wszWMSAPLevel` and 200. Digital uncompressed audio portion of such decrypted WMDRM Content may be ~~passed~~Passed to Digital Audio Outputs.

4.2.2.3 **Level 201 to 300.** If the Output Protection Level specified in the WMDRM License is greater than 200 and less than or equal to 300, Licensed Products may ~~pass~~Pass uncompressed Digital Audio Content of decrypted WMDRM Content only using Secure Audio Path. Licensed Product must engage SAP by calling `IWMDRMReader::SetDRMProperty()` with the parameters `g_wszWMSAPLevel` and 300. Digital uncompressed audio portion of such decrypted WMDRM Content must not be ~~passed~~Passed to Digital Audio Outputs.

4.2.2.4 **Level 301 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not ~~pass~~Pass uncompressed Digital Audio Content of decrypted WMDRM Content.

4.2.3 **Output Control for Digital Compressed Video Content.** Licensed Products must not ~~pass~~Pass ~~decrypted~~ Digital Compressed Video Content to any ~~output~~Output, except that a Licensed Product may Pass Content marked with the ATSC Standard A/65B Redistribution Control descriptor (rc descriptor()) to any Output protected by a digital content protection technology approved by the Federal Communications Commission (or otherwise approved in accordance with applicable Federal Communications Commission rules) for use with such Content.

4.2.4 **Output Control for Digital Uncompressed Video Content.** If a Licensed Product ~~passes~~Passes uncompressed Digital Video Content, Licensed Products must follow restrictions as specified in the WMDRM License by querying for Output Protection Levels as described above and responding based on the value of `DRM_MINIMUM_OUTPUT_PROTECTION_LEVELS.wUncompressedDigitalVideo`.

4.2.4.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may ~~pass~~Pass, without restriction, the uncompressed Digital Video Content of decrypted WMDRM Content on Video Outputs.

4.2.4.2 **Level 101 to 300.** If the Output Protection Level specified in the WMDRM Licenses is greater than 100 and less than or equal to 300 and Licensed Products is ~~passing~~Passing Digital Video Content to Digital Video Outputs, Licensed Products must engage HDCP using COPP to protect the uncompressed Digital Video Content of decrypted WMDRM Content. Licensed Products must verify using COPP that the HDCP Source Function is engaged and able to deliver protected content, which means HDCP encryption is operational on such ~~output~~Output.

4.2.4.3 **Level 301 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not **passPass** uncompressed Digital Video Content of decrypted WMDRM Content on Digital Video Outputs.

4.2.5 **Output Control for Analog Video Content.** If a Licensed Product **passesPasses** the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs, the Licensed Product must follow restrictions as specified in the WMDRM License by querying for Output Protection Levels and responding based on the value of DRM_MINIMUM_OUTPUT_PROTECTION_LEVELS.wAnalogVideo. Additional restrictions may be required as specified in Section 4.2.6.

4.2.5.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may **passPass** without restriction the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs.

4.2.5.2 **Level 101 to 200.** If the Output Protection Level specified in the WMDRM Licenses is greater than 100 but less than or equal to 200 and Licensed Products is **passingPassing** the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs, Licensed Products must engage CGMS-A using COPP with the CGMS field in the copy set to ‘11’ (“no more copies”).

4.2.5.3 **Level 201 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 200, Licensed Products must not **passPass** the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs.

4.2.6 **Output Control for Extended Analog Video Content.** If a Licensed Product **passesPasses** the video portion of decrypted WMDRM Content to Analog Television Outputs, the Licensed Product must follow restrictions as specified in the WMDRM License by querying for Output Protection Levels and taking appropriate action as described below. Additional restrictions may be required as specified in Section 4.2.5

4.2.6.1 **Automatic Gain Control and ColorStripe.** If a Licensed Product is **passingPassing** the video portion of decrypted WMDRM Content to Analog Television Outputs and any DRM_VIDEO_OUTPUT_PROTECTION.guidID has a value of “C3FD11C6-F8B7-4d20-B008-1DB17D61F2DA”, the Licensed Product must engage Automatic Gain Control and ColorStripe via COPP and specify for the value of DRM_VIDEO_OUTPUT_PROTECTION.bConfigData for the APSTB field. Additional technologies and restrictions may be required as specified in Section 4.2.5. For avoidance of doubt, the value of bConfigData for AGC and ColorStripe is as follows:

APSTB values	Description	NTSC	PAL

00	AGC and ColorStripe is-disabled	Disabled <u>Off</u>	Disable <u>dOff</u>
01	AGC Only	APS1	APS1
10	AGC and 2 line ColorStripe	APS2	APS1
11	AGC and 4 line ColorStripe	APS3	APS1

4.3 **Unrestricted Outputs.** Licensed Products may ~~pass~~Pass without restriction WMDRM Content to the following ~~outputs~~Outputs provided the requirements in Section 4.2 are met.

4.3.1 **Analog Audio Outputs.** Licensed Products may ~~pass~~Pass without restriction the Analog Audio Content of decrypted WMDRM Content to Analog Audio Outputs.

4.3.2 **USB Audio Outputs.** Licensed Products may ~~pass~~Pass without restriction the uncompressed Digital Audio Content of decrypted WMDRM Content to USB Audio Outputs.

4.3.3 **Analog Computer Monitor Outputs.** Licensed Products may ~~pass~~Pass without restriction the uncompressed Analog Video Content of decrypted WMDRM Content to Analog Computer Monitor Outputs.

4.3.4 **Internal Video Outputs.** Licensed Products may ~~pass~~Pass without restriction the uncompressed Digital Video Content of decrypted WMDRM Content to Internal Video Outputs.

5. COLLABORATIVE PLAY RULES FOR LICENSED PRODUCTS

5.1.1 **Requesting Rights.** Licensed Products that will ~~pass~~Pass decrypted the audio and/or video portion of WMDRM Content using the Collaborative Play model must request the g_wszWMDRM_ActionAllowed_CollaborativePlay right via calls to IWMDRMReader::SetDRMProperty(). If the return code is anything other than S_OK, Licensed Products must not ~~pass~~Pass the WMDRM Content.

5.1.2 **Re-encode.** Licensed Products that ~~pass~~Pass ~~compressed Digital Audio Content of~~ decrypted ~~the audio and/or video portion of~~WMDRM Content or compressed Digital Video Content of decrypted WMDRM Content using the Collaborative Play model must degrade the quality of ~~audio~~Digital Audio Content and/or ~~video~~Digital Video Content before WMDRM Content is transmitted.

5.1.2.1 **Audio Encoding.** Licensed Products must re-compress the Audio portion of WMDRM Content with the Windows Media Audio codec, specifying a maximum bit rate of 64Kbps, 44.1 KHz and 16-bit Stereo.

5.1.2.2 **Video Encoding.** Licensed Products must re-compress the Video portion of WMDRM Content with the Windows Media Video codec, with the maximum bit rate in Kbps not exceeding the product of the horizontal resolution, vertical resolution and the value four (4), but in no case to exceed 512Kbps. For example, the maximum bit rate for a resolution of 320x240 will be 300Kbps. The maximum frame rate must not exceed 30fps.

5.1.3 **Re-encryption.** Licensed Products must encrypt the re-encoded audio and/or video portion of WMDRM Content using DES encryption with a minimum key length of 56-bit or AES with a minimum key length of 128-bit. The Licensed Product must use a random number generator that is Cryptographically Random to generate strong symmetric keys for content encryption.

5.1.4 **Key Management.** Licensed Products must distribute Content Keys to other Licensed Products in a secure manner. Licensed Products must distribute content keys only to other Licensed Products that are known to be secure and to comply with these Compliance Rules. Licensed Products must not tamper with the License Acquisition URL and content metadata.

5.1.5 **Concurrent Playback.** Licensed Products may ~~pass~~Pass collaborative audio and/or video WMDRM Content only to ~~Approved~~ Outputs while connected to other Licensed Products and only while the Licensed Product that was the source of the WMDRM Content is also concurrently ~~passing~~Passing the Content to ~~Approved~~ Outputs. Licensed Products must limit to a maximum of ten (10) the number of Licensed Products that can concurrently ~~pass~~Pass the audio and/or video portion of decrypted WMDRM Content to ~~Approved~~ Outputs.

5.1.6 **Protocol.** Licensed Products must use a protocol that is proven to be robust against common attacks including “man in the middle” and replay attacks. Licensed Products must declare themselves to the group when joining a peer group. Licensed Products must not share WMDRM Content with other Licensed Products until the Licensed Products to receive the Content have declared themselves to the peer group and the Licensed Product that will be ~~passing~~Passing the Content has verified that the maximum number of members in the group does not exceed ten (10).

5.1.7 **Purchase Option.** Licensed Products must provide the end user with a purchase option when the audio and/or video portion of WMDRM Content is being ~~passed~~Passed to ~~Approved~~ Outputs. This mechanism must be prominent and available for the user to select at any time. When a user invokes this mechanism, Licensed Products may direct the user to a default service supported by the Licensed Product. If the content is unavailable through the default service, the Licensed Product must direct the user to a web site using the License Acquisition URL. The License

Acquisition URL may be retrieved for the WMDRM Content being **passed**Passed using the API `IWMReader::GetDRMProperty()` with a parameter of `g_wszWMDRM_DRMHeader_LicenseAcqURL`.

6. REDBOOK CD BURNING RULES FOR LICENSED PRODUCTS

6.1 Redbook CD Burning

6.1.1 Licensed Products may **pass**Pass the decompressed audio portion of decrypted WMDRM Content to a CD-R or CD-RW drive for the purpose of creating a Redbook Audio CD only if the WMDRM License permits such CD burning and only in the manner described in this Section 6.1.

6.1.2 Licensed Products may temporarily cache the decompressed audio portion of decrypted WMDRM Content prior to beginning to master a Redbook CD, provided that the decrypted content is stored as part of a single file and the temporary cached copy is hidden and deleted from Persistent Storage once the operation is complete. The single file must prevent playback by widely available media playback software.

6.2 **Requesting Burn permission.** Licensed Products must first call `IWMReaderPlaylistBurn::InitPlaylistBurn` to initialize the Playlist Burning interface and must **pass**Pass a complete list of files to be burned including the fully qualified path and filename to the files.

6.3 **Verify Permission.** Licensed Products must next call `IWMReaderPlaylistBurn::GetInitResults` to determine whether the Licensed Product may proceed with burning the specified playlist. If the return code of `GetInitResults` includes any value other than `S_OK`, Licensed Products must not burn the playlist.

6.4 **Finalizing burn.** Licensed Products must call `IWMReaderPlaylistBurn::EndPlaylistBurn` after the entire playlist has been burned successfully. If an unrecoverable error occurs before the last track in the Playlist has been Burned, Licensed Products are not required to call `IWMReaderPlaylistBurn::EndPlaylistBurn`.

7. RULES FOR COPYING TO LICENSED PRODUCTS

7.1 **Copy to Device.** Licensed Products may not **copy**Copy or transfer WMDRM Content to a portable device except by using the WM Device Manager functionality in the WMF SDK.

8. RULES FOR STREAMING TO LICENSED PRODUCTS

8.1 WMDRM-ND Protocol Messages.

8.1.1 **Implementation.** Licensed Products must implement all WMDRM-ND Protocol Messages Consistent with the Microsoft Implementation.

8.1.2 **Data.** Licensed Products must not modify or augment the data within the WMDRM-ND Protocol Messages as described in the Microsoft Implementation.

8.2 Limiting Concurrent WMDRM-ND Receivers

8.2.1 **Opening WMDRM-ND Receivers.** A Licensed Product must call `IWMRegisteredDevice::Open` prior to ~~passing~~Streaming WMDRM Content to a WMDRM-ND Receiver.

8.2.2 **Closing WMDRM-ND Receivers.** A Licensed Product must call `IWMRegisteredDevice::Close` after the Licensed Product has completed passingStreaming the WMDRM Content to the open WMDRM-ND Receiver. ~~If an unrecoverable error occurs before the WMDRM Content is passed, Licensed Products are not required to~~A Licensed Product must call `IWMRegisteredDevice::Close` except in the case of a fatal application error.

EXHIBIT 3

COMPLIANCE RULES FOR WMDRM FOR NETWORK DEVICES PLATFORMS

1. DEFINITIONS

The following terms have the meanings set forth below. Other initially capitalized terms not defined in these Compliance Rules have the meanings ascribed to them in the License Agreement, the Compliance Rules for WMDRM for Network Devices Applications, or the Microsoft Implementation.

- 1.1 “Certificate” means a unique WMDRM object used to assess trust.
- 1.2 “Certificate Chain” means a collection of Certificates that can trace the assessed trust back to the Microsoft Root Certificate.
- 1.3 “Company” means an entity licensed under a License Agreement to develop Licensed Products.
- 1.4 “Consistent with the Microsoft Implementation” means the Licensed Product (i) provides equivalent functionality to the Microsoft Implementation, (ii) equals or exceeds the security of the Microsoft Implementation, and (iii) maintains compatibility and interoperability with the Microsoft Implementation.
- 1.5 “Content” means audio and/or video that are transmitted or distributed, either by broadcast, cablecast, or other means of distribution to the general public or on demand.
- 1.6 “Cryptographically Random” means unpredictable, in that no polynomial-time algorithm, given any sequence of bits, can guess the succeeding K bits with probability greater than $\frac{1}{2}^K + 1/P(K)$ for any (positive) polynomial P and sufficiently large K.
- 1.7 “Device Certificate” means a Certificate issued by or on behalf of Company, assigned to a Licensed Product, and used, for example, to evaluate whether the Licensed Product is trusted and eligible to receive WMDRM Content.
- 1.8 “License Agreement” means the agreement under which Microsoft licenses entities to develop and distribute WMDRM-ND Receivers that include implementations of WMDRM-ND.
- 1.9 “Licensed Product” means a hardware device or software application (or other software component, which may be a separately identifiable subset of a software application or operating system), that (i) implements

WMDRM-ND subject to a license from Microsoft and (ii) is capable of playing back WMDRM Content.

- 1.10 “Microsoft Implementation” means the implementation of WMDRM-ND functionality provided as source code, binaries, technical documentation, tools and/or sample files as provided to the Company under the License Agreement.
- 1.11 “Microsoft Root Certificate” means a Certificate controlled by Microsoft that is inherently trusted by the WMDRM-ND Transmitter and is the root source of trust for Licensed Products.
- 1.12 “Output” means Analog Audio Outputs, Analog Computer Monitor Outputs, Analog Television Outputs, Digital Audio Outputs, Digital Video Outputs, Internal Video Outputs and USB Audio Outputs. Output does not include Streaming WMDRM Content to a WMDRM-ND Receiver.
- 1.13 “Pass” means to direct decrypted WMDRM Content to flow to Outputs, optionally (though not necessarily) through intermediate components such as a codec or device driver.
- 1.14 “Persistent Storage” means storage that can retain data for an indefinite period of time after power is withdrawn.
- 1.15 “Serial Number” means an identifier with a minimum length of 128 bits that must be unique to each Licensed Product manufactured by or on behalf of Company.
- 1.16 “Stream” means to transport encrypted WMDRM Content over a network, to the extent permitted by applicable WMDRM Policy, to a WMDRM-ND Receiver for Passing to an Output immediately or shortly after receipt of the WMDRM Content in the WMDRM-ND Receiver.
- 1.17 “WMDRM” means Windows Media Digital Rights Management technology.
- 1.18 “WMDRM Content” means audio or audiovisual content that has been encrypted and recorded using WMDRM.
- 1.19 “WMDRM License” means a data structure that contains, but is not limited to, WMDRM Policy and an encrypted Content Key associated with specific WMDRM Content.
- 1.20 “WMDRM Policy” means the description of the actions permitted and/or required for or with WMDRM Content and restrictions on those actions as described in the WMDRM License associated with the WMDRM Content.

- 1.21 “WMDRM-ND” means WMDRM for Network Devices.
- 1.22 “WMDRM-ND Protocol Messages” means the message exchanges between the WMDRM-ND Receiver and WMDRM-ND Transmitter defined in the Microsoft Implementation.
- 1.23 “WMDRM-ND Receiver” means a Licensed Product that complies with the applicable Compliance Rules and may connect to WMDRM-ND Transmitters and acquire WMDRM Licenses and WMDRM Content from such WMDRM-ND Transmitters.
- 1.24 “WMDRM-ND Transmitter” means a product or application implemented or licensed by Microsoft that complies with the applicable Compliance Rules and may connect to WMDRM-ND Receivers and issue WMDRM Licenses and WMDRM Content.

2. SCOPE. These Compliance Rules apply to Licensed Products implementing WMDRM-ND Receiver functionality. These Compliance Rules set forth the requirements pursuant to which Licensed Products must enforce the WMDRM controls applicable to the playback and Output of WMDRM Content on WMDRM-ND Receivers.

3. REQUIREMENTS FOR WMDRM-ND PLATFORMS

3.1 **Functionality.** When a Licensed Product implements any WMDRM-ND functionality, it must do so in a manner Consistent with the Microsoft Implementation. This requirement is in addition to all of the specific compliance rules set forth in this document. In the event of a conflict between how the Microsoft Implementation implements a given WMDRM-ND functionality and how a specific compliance rule in this document describes how such implementation must be accomplished, the compliance rule is controlling.

3.2 **Persistent Storage.** Licensed Products must provide Persistent Storage for the Device Certificate and the Certificate Chain.

3.3 **Random Number Generator.** Licensed Products must implement and make use of a random number generator that is Cryptographically Random. For the avoidance of doubt, linear congruential random number generators are not acceptable.

3.4 WMDRM-ND Protocol Messages

3.4.1 **Implementation.** Licensed Products must implement all WMDRM-ND Protocol Messages Consistent with the Microsoft Implementation.

3.4.2 Registration Messages

3.4.2.1 **Serial Number Verification.** Licensed Products must abort the current procedure if the Serial Number in the Registration Response is different from that of the Licensed Product's Serial Number. The verification of the Serial Number must be Consistent with the Microsoft Implementation.

3.4.2.2 **Signature Verification.** Licensed Products must abort the current procedure if the verification of the Signature returned in the Registration Response Message fails. The verification of the Signature must be Consistent with the Microsoft Implementation.

3.4.3 **Policy Messages.**

3.4.3.1 **Rights Identifier Generation.** Licensed Products must generate a Cryptographically Random Rights Identifier for use in the Policy Request Message.

3.4.3.2 **Rights Identifier Verification.** Licensed Products must abort the current procedure if the Rights Identifier in the Policy Response Message is different from that of the Rights Identifier submitted by the Licensed Product in the Policy Request Message.

3.4.3.3 **Serial Number Verification.** Licensed Products must abort the current procedure if the Serial Number in the WMDRM License is different from that of the Licensed Product's Serial Number.

3.4.3.4 **Signature Verification.** Licensed Products must abort the current procedure if the verification of the returned WMDRM License Signature fails. The verification of the WMDRM License Signature must be Consistent with the Microsoft Implementation.

3.4.3.5 **Unspecified policy.** WMDRM Policy may specify additional rights, restrictions or parameters that are not covered in these Compliance Rules. Nevertheless Licensed Products must only take action based on rights and enforce restrictions covered in this document and Consistent with the Microsoft Implementation.

3.4.4 **Data Transfer**

3.4.4.1 **Content Request.** Licensed Products must not request transfer of the WMDRM Content if the Licensed Product has determined that it cannot properly enforce the restrictions specified in the WMDRM License associated with the WMDRM Content.

COMPLIANCE RULES FOR WMDRM FOR NETWORK DEVICES PLATFORMS

1. DEFINITIONS

The following terms have the meanings set forth below. Other initially capitalized terms not defined in these Compliance Rules have the meanings ascribed to them in the License Agreement, [the Compliance Rules for WMDRM for Network Devices Applications](#), or the Microsoft Implementation.

- 1.1 “Certificate” means a unique WMDRM object used to assess trust.
- 1.2 “Certificate Chain” means a collection of Certificates that can trace the assessed trust back to the Microsoft Root Certificate.
- 1.3 “Company” means an entity licensed under a License Agreement to develop Licensed Products.
- 1.4 “Consistent with the Microsoft Implementation” means the Licensed Product (i) provides equivalent functionality to the Microsoft Implementation, (ii) equals or exceeds the security of the Microsoft Implementation, and (iii) maintains compatibility and interoperability with the Microsoft Implementation.
- 1.5 “Content” means audio and/or video that are transmitted or distributed, either by broadcast, cablecast, or other means of distribution to the general public or on demand.
- 1.6 “Cryptographically Random” means unpredictable, in that, ~~at no polynomial-time algorithm, given~~ any ~~point regardless of how many preceding sequence of~~ bits ~~are available~~, ~~can guess~~ the ~~probability of predicting the next~~ succeeding K bits ~~is~~ with probability greater than $\frac{1}{2^K} + \frac{1}{P(K)}$ for any (positive) polynomial P and sufficiently large K.
- 1.7 “Device Certificate” means a Certificate issued by or on behalf of Company, assigned to a Licensed Product, and used, for example, to evaluate whether the Licensed Product is trusted and eligible to receive WMDRM Content.
- 1.8 “License Agreement” means the agreement under which Microsoft licenses entities to develop and distribute ~~products~~ WMDRM-ND Receivers that include implementations of WMDRM-ND.
- 1.9 “Licensed Product” means a hardware device or software application (or other software component, which may be a separately identifiable subset

of a software application or operating system), that (i) implements WMDRM-ND subject to a license from Microsoft and (ii) is capable of playing back WMDRM Content.

- 1.10 “Microsoft Implementation” means the implementation of WMDRM-ND functionality provided as source code, binaries, technical documentation, tools and/or sample files as provided to the Company under the License Agreement.
- 1.11 “Microsoft Root Certificate” means a Certificate controlled by Microsoft that is inherently trusted by the WMDRM-ND Transmitter and is the root source of trust for Licensed Products.
- 1.12 ~~1.12~~ “Output” means Analog Audio Outputs, Analog Computer Monitor Outputs, Analog Television Outputs, Digital Audio Outputs, Digital Video Outputs, Internal Video Outputs and USB Audio Outputs. Output does not include Streaming WMDRM Content to a WMDRM-ND Receiver.
- 1.13 ~~1.13~~ “Pass” means to direct decrypted WMDRM Content to flow to Outputs, optionally (though not necessarily) through intermediate components such as a codec or device driver.
- 1.14 ~~1.12~~ “Persistent Storage” means storage that can retain data for an indefinite period of time after power is withdrawn.
- 1.15 ~~1.13~~ “Serial Number” means an identifier with a minimum length of 128 bits that must be unique to each Licensed Product manufactured by or on behalf of Company.
- 1.16 ~~1.16~~ “Stream” means to transport encrypted WMDRM Content over a network, to the extent permitted by applicable WMDRM Policy, to a WMDRM-ND Receiver for Passing to an Output immediately or shortly after receipt of the WMDRM Content in the WMDRM-ND Receiver.
- 1.17 ~~1.14~~ “WMDRM” means Windows Media Digital Rights Management technology.
- 1.18 ~~1.15~~ “WMDRM Content” means audio or audiovisual content that has been encrypted and recorded using WMDRM.
- 1.19 ~~1.16~~ “WMDRM License” means a data structure that contains, but is not limited to, WMDRM Policy and an encrypted Content Key associated with specific WMDRM Content.

- 1.20** ~~1.17~~ “WMDRM Policy” means the description of the actions permitted and/or required for or with WMDRM Content and restrictions on those actions as described in the WMDRM License associated with the WMDRM Content.
- 1.21** ~~1.18~~ “WMDRM-ND” means WMDRM for Network Devices.
- 1.22** ~~1.19~~ “WMDRM-ND Protocol Messages” means the message exchanges between the WMDRM-ND Receiver and WMDRM-ND Transmitter defined in the Microsoft Implementation.
- 1.23** ~~1.20~~ “WMDRM-ND Receiver” means a Licensed Product that complies with the applicable Compliance Rules and may connect to WMDRM-ND Transmitters and acquire WMDRM Licenses and WMDRM Content from such WMDRM-ND Transmitters.
- 1.24** ~~1.21~~ “WMDRM-ND Transmitter” means a product or application implemented or licensed by Microsoft that complies with the applicable Compliance Rules and may connect to WMDRM-ND Receivers and issue WMDRM Licenses and WMDRM Content.

2. SCOPE. These Compliance Rules apply to Licensed Products implementing WMDRM-ND Receiver functionality. These Compliance Rules set forth the requirements pursuant to which Licensed Products must enforce the WMDRM controls applicable to the playback and ~~output~~Output of WMDRM Content on WMDRM-ND Receivers.

3. REQUIREMENTS FOR WMDRM-ND PLATFORMS

3.1 Functionality. When a Licensed Product implements any WMDRM-ND functionality, it must do so in a manner Consistent with the Microsoft Implementation. This requirement is in addition to all of the specific compliance rules set forth in this document. In the event of a conflict between how the Microsoft Implementation implements a given WMDRM-ND functionality and how a specific compliance rule in this document describes how such implementation must be accomplished, the compliance rule is controlling.

3.2 Persistent Storage. Licensed Products must provide Persistent Storage for the Device Certificate and the Certificate Chain.

3.3 Random Number Generator. Licensed Products must implement and make use of a random number generator that is Cryptographically Random. For the avoidance of doubt, linear congruential random number generators are not acceptable.

3.4 WMDRM-ND Protocol Messages

3.4.1 **Implementation.** Licensed Products must implement all WMDRM-ND Protocol Messages Consistent with the Microsoft Implementation.

3.4.2 **Registration Messages**

3.4.2.1 **Serial Number Verification.** Licensed Products must abort the current procedure if the Serial Number in the Registration Response is different from that of the Licensed Product's Serial Number. The verification of the Serial Number must be Consistent with the Microsoft Implementation.

3.4.2.2 **Signature Verification.** Licensed Products must abort the current procedure if the verification of the Signature returned in the Registration Response Message fails. The verification of the Signature must be Consistent with the Microsoft Implementation.

3.4.3 **Policy Messages.**

3.4.3.1 **Rights Identifier Generation.** Licensed Products must generate a Cryptographically Random Rights Identifier for use in the Policy Request Message.

3.4.3.2 **Rights Identifier Verification.** Licensed Products must abort the current procedure if the Rights Identifier in the Policy Response Message is different from that of the Rights Identifier submitted by the Licensed Product in the Policy Request Message.

3.4.3.3 **Serial Number Verification.** Licensed Products must abort the current procedure if the Serial Number in the WMDRM License is different from that of the Licensed Product's Serial Number.

3.4.3.4 **Signature Verification.** Licensed Products must abort the current procedure if the verification of the returned WMDRM License Signature fails. The verification of the WMDRM License Signature must be Consistent with the Microsoft Implementation.

3.4.3.5 **Unspecified policy.** WMDRM Policy may specify additional rights, restrictions or parameters that are not covered in these Compliance Rules. Nevertheless Licensed Products must only take action based on rights and enforce restrictions covered in this document and Consistent with the Microsoft Implementation.

3.4.4 **Data Transfer**

3.4.4.1 **Content Request.** Licensed Products must not request transfer of the WMDRM Content if the Licensed Product has determined that it cannot properly enforce the restrictions specified in the WMDRM License associated with the WMDRM Content.

EXHIBIT 4

COMPLIANCE RULES FOR WMDRM FOR NETWORK DEVICES APPLICATIONS

1. DEFINITIONS

The following terms have the meanings set forth below. Other initially capitalized terms not defined in these Compliance Rules have the meanings ascribed to them in the License Agreement or the Microsoft Implementation.

- 1.1 “Analog Audio Outputs” means a connector for an analog sound amplification reproduction device such as a speaker or headphones. For avoidance of doubt, this includes both external jacks to connect speakers and/or headphones and built-in speakers and/or headphones.
- 1.2 “Analog Computer Monitor Output” means a connector for an analog monitor typically found and associated with a Computer Product and that carries uncompressed analog video signals. The term expressly includes those outputs known as VGA, SVGA, XGA, DVI Analog, and various non-standardized analog monitor connections which have been implemented by manufacturers, and expressly does not include such typical consumer electronics connectors as NTSC, PAL, SECAM, SCART, YPrPb, S-Video and Consumer RGB, whether or not such connectors are found on any Computer Product.
- 1.3 “Analog Protection System (APS) trigger bits (APSTB)” means the bits as specified (a) for NTSC video signals, in IEC 61880 (for inclusion of such value on Line 20) or EIA-608-B (for inclusion of such value on Line 21) or (b) for YUV (525/60 systems) signals, in IEC 61880 (for inclusion of such value on Line 20) or EIA-608-B (for inclusion of such value on Line 21).
- 1.4 “Analog Television Output” means such typical consumer electronics analog connectors as NTSC, PAL, SECAM, SCART, YPrPb, S-Video and Consumer RGB.
- 1.5 “Analog Video Content” means audiovisual works, as defined in 17 U.S.C. § 101, recorded in an analog format.
- 1.6 “Audio Outputs” means Analog Audio Outputs, Digital Audio Outputs and USB Audio Outputs.
- 1.7 “Automatic Gain Control (AGC)” means the so-named copy control system as specified (a) for NTSC, PAL, SECAM or YUV analog video signals, in the document entitled “Specification of the Macrovision Copy

Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999,” and (b) for a 480p progressive scan analog video signal, in the document entitled “Specification of the Macrovision AGC Copy Protection Waveforms for DVD Applications with 525p (480p) Progressive Scan Outputs, Revision 1.03 (December 22, 1999).”

- 1.8 “CGMS-A” means the Copy Generation Management System (Analog) as specified (a) for NTSC analog video signals, in IEC 61880 (for inclusion on Line 20) or in EIA-608-B (for inclusion on Line 21), (b) for PAL, SECAM or YUV analog video signals, in IEC 61880 (for inclusion on Line 20) or in EIA-608-B (for inclusion on Line 21) or in EIA-805 (for inclusion on Line 41) for YUV (525/60 systems) signals or in ETS 300924 for PAL, SECAM and YUV (625/50 systems) signals, or (c) for 480p progressive scan analog video signals, in, or adapted without material change from, EIAJ CPR1204-1 (defining the signal waveform carrying the CGMS-A) and IEC 61880 (defining the bit assignment for CGMS-A).
- 1.9 “Certificate” means a unique WMDRM object used to assess trust.
- 1.10 “Colorstripe” means the so-named copy control system as specified for NTSC analog video signals in the document entitled “Specification of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999.”
- 1.11 “Company” means an entity licensed under a License Agreement to develop Licensed Products.
- 1.12 “Company Certificate” means a Certificate issued by Microsoft and unique to Company.
- 1.13 “Computer Product” means a device that is designed or permits the end user to install software applications thereon, including, but not limited to, personal computers, handheld “Personal Digital Assistants,” and the like.
- 1.14 “Consistent with the Microsoft Implementation” means the Licensed Product (i) provides equivalent functionality to the Microsoft Implementation, (ii) equals or exceeds the security of the Microsoft Implementation, and (iii) maintains compatibility and interoperability with the Microsoft Implementation.
- 1.15 “Content” means audio and/or video that are transmitted or distributed, either by broadcast, cablecast, or other means of distribution to the general public or on demand.
- 1.16 “Content Key” means a symmetric key used to decrypt WMDRM Content.

- 1.17 “Contract Manufacturer Certificate” means a Certificate issued by Company and unique to a contract manufacturer for use on Company’s behalf.
- 1.18 “Cryptographically Random” means unpredictable, in that no polynomial-time algorithm, given any sequence of bits, can guess the succeeding K bits with probability greater than $\frac{1}{2}^K + 1/P(K)$ for any (positive) polynomial P and sufficiently large K.
- 1.19 “Device Certificate” means a Certificate issued by or on behalf of Company, assigned to a Licensed Product and used, for example, to evaluate whether the Licensed Product is trusted and eligible to receive WMDRM Content.
- 1.20 “Device Keys” means an associated pair of Cryptographically Random asymmetric keys generated by or on behalf of Company for inclusion in Licensed Products, comprising a “Device Public Key” and a “Device Private Key”.
- 1.21 “Device Private Key” means a unique, Cryptographically Random asymmetric private key generated by or for Licensed Products for the purpose of decrypting Content Keys.
- 1.22 “Device Public Key” means the public portion of the Device Keys.
- 1.23 “Digital Audio Content” means sound recordings, as defined in 17 U.S.C. § 101, recorded in a digital format.
- 1.24 “Digital Audio Output” means digital audio signals conforming to IEC-958, IEC-60958, or IEC-61937.
- 1.25 “Digital Video Content” means audiovisual works, as defined in 17 U.S.C. § 101, recorded in a digital format.
- 1.26 “Digital Video Output” means the digital interface portion only of Digital Visual Interface (DVI), a digital interface standard created by the Digital Display Working Group (DDWG), and the DVI digital interface portion of the High-Definition Multimedia Interface (HDMI).
- 1.27 “Firmware Certificate” means a Certificate issued by or on behalf of Company that is unique to each model number and/or firmware revision of a Licensed Product.
- 1.28 “HDCP” means High-Bandwidth Digital Content Protection (“HDCP”) protected Output. The HDCP specification and license agreement are available from Digital Content Protection, LLC at <http://www.digital-cp.com/>.

- 1.29 “Internal Video Output” means any display that is permanently connected to the Licensed Product, including, but not limited to, a liquid crystal display (“LCD”).
- 1.30 “License Agreement” means the agreement under which Microsoft licenses entities to develop and distribute WMDRM-ND Receivers that include implementations of WMDRM-ND.
- 1.31 “Licensed Product” means a hardware device or software application (or other software component, which may be a separately identifiable subset of a software application or operating system) that (i) implements WMDRM-ND subject to a license from Microsoft and (ii) is capable of playing back WMDRM Content.
- 1.32 “Microsoft Implementation” means the implementation of WMDRM-ND functionality provided as source code, binaries, technical documentation, tools and sample files as provided to the Company under the License Agreement.
- 1.33 “Output” means Analog Audio Outputs, Analog Computer Monitor Outputs, Analog Television Outputs, Digital Audio Outputs, Digital Video Outputs, Internal Video Outputs and USB Audio Outputs. Output does not include Streaming WMDRM Content to a WMDRM-ND Receiver.
- 1.34 “Output Protection Level” means a number included in WMDRM Policy that corresponds to the content protection that must be applied when Passing WMDRM Content. The Output Protection Level may be determined and assigned by the content owner or may be assigned by the WMDRM Implementation for specific categories of WMDRM Content.
- 1.35 “Pass” means to direct decrypted WMDRM Content to flow to Outputs, optionally (though not necessarily) through intermediate components such as a codec or device driver.
- 1.36 “Play” means the first decrypt of WMDRM Content.
- 1.37 “Secure Audio Device Drivers” means audio device drivers that either 1) are not capable of being replaced by an end user or 2) are verified not to have been modified, are trusted not to expose decrypted WMDRM Content, and ensure that only the secure driver is capable of receiving the WMDRM Content through encryption or other means. For avoidance of doubt, a Licensed Product that prevents end users from upgrading the audio device drivers is considered to have Secure Audio Device Drivers.
- 1.38 “Secure Codecs” means audio and/or video codecs that either 1) are not capable of being replaced by an end user or 2) are verified not to have

been modified, are trusted not to expose decrypted WMDRM Content, and prevent intermediate software from accessing WMDRM Content. For avoidance of doubt, a Licensed Product that prevents end users from replacing the codecs is considered to have Secure Codecs.

- 1.39 “Security Level” means a number in the WMDRM Policy associated with specific WMDRM Content that specifies the minimum security level necessary for a Licensed Product to be able to acquire a WMDRM License for the WMDRM Content.
- 1.40 “Stream” means to transport encrypted WMDRM Content over a network, to the extent permitted by applicable WMDRM Policy, to a WMDRM-ND Receiver for Passing to an Output immediately or shortly after receipt of the WMDRM Content in the WMDRM-ND Receiver.
- 1.41 “Temporary Storage” means storage that cannot retain data for an indefinite period of time after power is withdrawn.
- 1.42 “Unrestricted Audio Outputs” means Analog Audio Outputs and USB Audio Outputs.
- 1.43 “USB Audio Output” means a speaker, headphones or other sound reproduction device attached that complies with the Universal Serial Bus (USB) Audio Specification available from the USB Forum.
- 1.44 “WMDRM” means Windows Media Digital Rights Management technology.
- 1.45 “WMDRM Content” means audio or audiovisual content that has been encrypted and recorded using WMDRM.
- 1.46 “WMDRM License” means a data structure that contains, but is not limited to, WMDRM Policy and an encrypted Content Key associated with specific WMDRM Content.
- 1.47 “WMDRM Policy” means the description of the actions permitted and/or required for or with WMDRM Content and restrictions on those actions as described in the WMDRM License associated with the WMDRM Content.
- 1.48 “WMDRM-ND” means WMDRM for Network Devices.
- 1.49 “WMDRM-ND Receiver” means a product licensed under the License Agreement for WMDRM-ND Applications that complies with the applicable Compliance Rules and may connect to WMDRM-ND Transmitters and acquire WMDRM Licenses and WMDRM Content from such WMDRM-ND Transmitters.

- 1.50 “WMDRM-ND Transmitter” means a product or application licensed or implemented by Microsoft that complies with the applicable Compliance Rules and may connect to WMDRM-ND Receivers and issue WMDRM Licenses and WMDRM Content.

2. SCOPE. These Compliance Rules apply to Licensed Products implementing WMDRM-ND functionality and receiving content from WMDRM-ND Transmitters. These Compliance Rules set forth the requirements pursuant to which WMDRM-ND Receivers may play back and Output WMDRM Content.

3. REQUIREMENTS FOR WMDRM-ND APPLICATIONS

3.1 **Content Caching.** Licensed Products may store up to but no more than five (5) minutes of WMDRM Content per content stream in Temporary Storage for the sole purpose of reducing the effects of network congestion and optimizing playback performance. Licensed Products must delete the cached reference of WMDRM Content from Temporary Storage once Licensed Products begin Passing a new piece of WMDRM Content.

3.2 **Serial Number.** Company or a contract manufacturer acting on Company’s behalf must assign a unique Serial Number with a minimum length of 128 bits to each Licensed Product manufactured by or on behalf of Company.

3.3 WMDRM-ND Certificates.

3.3.1 **Company Certificate.** Microsoft shall provide to Company the Company Certificate. Company shall use the Company Certificate to sign Firmware Certificates and/or Contract Manufacturer Certificates.

3.3.2 **Contract Manufacturer Certificates.** Contract Manufacturer Certificates are optional except that if Company uses a contract manufacturer, then Company shall issue a unique Contract Manufacturer Certificate for use by the contract manufacturer on Company’s behalf. Each Contract Manufacturer Certificate must be signed with the Private Key corresponding to the Company Certificate. Contract Manufacturer Certificates must be Consistent with the Microsoft Implementation.

3.3.2.1 **SignCertificate.** Contract Manufacturer Certificates must only contain a KeyUsage right of SignCertificate.

3.3.3 **Firmware Certificates.** Firmware Certificates must be unique for each model number of a Licensed Product. If a Licensed Product undergoes a firmware revision, then each firmware version must have a unique Firmware Certificate. Firmware Certificates must be signed with the Private Key corresponding to the

Company Certificate or the Contract Manufacturer Certificate. Firmware Certificates must be Consistent with the Microsoft Implementation.

3.3.3.1 **SignCertificate.** Firmware Certificates must only contain a KeyUsage right of SignCertificate.

3.3.4 **Device Certificates.** Company or a contract manufacturer acting on Company's behalf shall issue a unique Device Certificate for inclusion in each model or firmware/revision of each Licensed Product manufactured by or on behalf of Company. Device Certificates must be signed with the Private Key corresponding to the Firmware Certificate. Device Certificates must be Consistent with the Microsoft Implementation.

3.3.4.1 **EncryptKey.** Device Certificates must only contain a KeyUsage right of EncryptKey.

3.3.4.2 **Security Level.** Device Certificates must contain the appropriate Security Level as provided to Company by Microsoft.

3.3.5 **WMDRM-ND Certificate Keys.** A Cryptographically Random Public Key and Private Key must be generated by Company or a contract manufacturer acting on Company's behalf for inclusion in all WMDRM-ND Certificates. The Public Key and Private Key must be unique for each Certificate.

4. REQUIREMENTS FOR COMPLYING WITH WMDRM POLICY

The following Compliance Rule is applicable to the WMDRM Policy as specified in the WMDRM License:

4.1 **Unspecified policy.** WMDRM Policy may specify additional rights, restrictions or parameters that are not covered in these Compliance Rules. Nevertheless Licensed Products must only take action based on rights and enforce restrictions covered in this document and in a manner Consistent with the Microsoft Implementation.

5. PLAYBACK AND OUTPUT CONTROL RULES FOR LICENSED PRODUCTS

Licensed Products must comply with the following:

5.1 **Playback Control.** Licensed Products must comply with the following rules for playback control:

5.1.1 **Playback.** Licensed Products may Pass decrypted WMDRM Content through the Outputs described in Sections 5.2 and 5.3 only if the right to Play is included in a WMDRM License associated with such WMDRM Content.

5.2 **Restricted Outputs.** Licensed Products must detect and accurately respond to the Output Protection Levels for WMDRM Content.

5.2.1 **Output Control for Digital Compressed Audio Content.** If a Licensed Product Passes compressed Digital Audio Content, the Licensed Product must follow restrictions as specified in the WMDRM License and this Section 5.2.1. Licensed Products may Pass compressed Digital Audio Content to Secure Codecs provided the decompressed Digital Audio Content is handled consistent with Section 5.2.2.

5.2.1.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may Pass without restriction compressed Digital Audio Content of decrypted WMDRM Content to Audio Outputs.

5.2.1.2 **Level 101 to 200.** If the Output Protection Level specified in the WMDRM License is greater than 100 and less than or equal to 200, Licensed Products may Pass, without restriction, the compressed Digital Audio Content of decrypted WMDRM Content via Secure Audio Device Drivers to Audio Outputs.

5.2.1.3 **Level 201 to 300.** If the Output Protection Level specified in the WMDRM License is greater than 200 and less than or equal to 300, Licensed Products may Pass compressed Digital Audio Content of decrypted WMDRM Content via Secure Audio Device Drivers to Unrestricted Audio Outputs.

5.2.1.4 **Level 301 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not Pass compressed Digital Audio Content of decrypted WMDRM Content.

5.2.2 **Output Control for Digital Uncompressed Audio Content.** If a Licensed Product Passes uncompressed Digital Audio Content, the Licensed Products must follow restrictions as specified in the WMDRM License and this Section 5.2.2.

5.2.2.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may Pass without restriction digital uncompressed Digital Audio Content of decrypted WMDRM Content to Audio Outputs.

5.2.2.2 **Level 101 to 200.** If the Output Protection Level specified in the WMDRM License is greater than 100 and less than or equal to 200, Licensed Products may Pass, without restriction, the uncompressed Digital Audio Content of decrypted WMDRM Content via Secure Audio Device Drivers to Audio Outputs.

5.2.2.3 **Level 201 to 300.** If the Output Protection Level specified in the WMDRM License is greater than 200 and less than or equal to 300,

Licensed Products may Pass uncompressed Digital Audio Content of decrypted WMDRM Content via Secure Audio Device Drivers to Unrestricted Audio Outputs.

5.2.2.4 Level 301 or greater. If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not Pass uncompressed Digital Audio Content of decrypted WMDRM Content.

5.2.3 Output Control for Digital Compressed Video Content. Licensed Products must not Pass decrypted compressed Digital Video Content to any Output, except that a Licensed Product may Pass Content marked with the ATSC Standard A/65B Redistribution Control descriptor (rc_descriptor()) to any Output protected by a digital content protection technology approved by the Federal Communications Commission (or otherwise approved in accordance with applicable Federal Communications Commission rules) for use with such Content.. Licensed Products may Pass compressed Digital Video Content to Secure Codecs provided that the decompressed Digital Video Content is handled consistent with Section 5.2.4.

5.2.4 Output Control for Digital Uncompressed Video Content. If a Licensed Product Passes uncompressed Digital Video Content, the Licensed Product must follow restrictions as specified in the WMDRM License and this Section 5.2.4.

5.2.4.1 Level 0 to 100. If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may Pass, without restriction, the uncompressed Digital Video Content of decrypted WMDRM Content on Video Outputs.

5.2.4.2 Level 101 to 300. If the Output Protection Level specified in the WMDRM License is greater than 100 and less than or equal to 300 and Licensed Product is Passing Digital Video Content to Digital Video Outputs, the Licensed Product must engage HDCP to protect the uncompressed Digital Video Content of decrypted WMDRM Content. Licensed Products must verify that the HDCP Source Function is engaged and able to deliver protected content, which means HDCP encryption is operational on such Output.

5.2.4.3 Level 301 or greater. If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not Pass uncompressed Digital Video Content of decrypted WMDRM Content on Digital Video Outputs.

5.2.5 Output Control for Analog Video Content. If a Licensed Product Passes the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs, the Licensed Product must follow restrictions as specified in the WMDRM License and this Section 5.2.5. Additional restrictions may be required as specified in Section 5.2.6.

5.2.5.1 Level 0 to 100. If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may Pass without restriction the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs.

5.2.5.2 Level 101 to 200. If the Output Protection Level specified in the WMDRM Licenses is greater than 100 but less than or equal to 200 and the Licensed Product is Passing the Analog Video Content of decrypted WMDRM Content to the Analog Television Outputs, the Licensed Product must engage CGMS-A with the CGMS field in the copy set to '11' ("no more copies").

5.2.5.3 Level 201 or greater. If the Output Protection Level specified in the WMDRM License exceeds 200, Licensed Products must not Pass the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs.

5.2.6 Output Control for Extended Analog Video Content. If a Licensed Product Passes the video portion of Decrypted WMDRM Content to Analog Television Outputs, the Licensed Product must follow restrictions as specified in the WMDRM License and this Section 5.2.6. Additional restrictions may be required as specified in Section 5.2.5.

5.2.6.1 Automatic Gain Control and ColorStripe. If Extended Analog Video Protection List in the WMDRM License includes "C3FD11C6-F8B7-4d20-B008-1DB17D61F2DA", Licensed Products must engage Automatic Gain Control and ColorStripe and set the APSTB field as based on the Extended Analog Video Protection Configuration Data included in the WMDRM License. Additional technologies and restrictions may be required as specified in Section 5.2.5. For avoidance of doubt, the permitted APSTB values in the WMDRM License are as follows:

APSTB values	Description	NTSC	PAL
00	AGC and ColorStripe	Off	Off
01	AGC Only	APS1	APS1
10	AGC and 2 line ColorStripe	APS2	APS1
11	AGC and 4 line ColorStripe	APS3	APS1

5.3 Unrestricted Outputs. Unless otherwise specified in Section 5.2, Licensed Products may Pass without restriction WMDRM Content to the following Outputs provided the requirements in Section 5.1.1 are met.

5.3.1 **Analog Audio Outputs.** Licensed Products may Pass without restriction the Analog Audio Content of decrypted WMDRM Content to Analog Audio Outputs.

5.3.2 **USB Audio Outputs.** Licensed Products may Pass without restriction the uncompressed Digital Audio Content of decrypted WMDRM Content to USB Audio Outputs.

5.3.3 **Analog Computer Monitor Outputs.** Licensed Products may Pass without restriction the uncompressed Analog Video Content of decrypted WMDRM Content to Analog Computer Monitor Outputs.

5.3.4 **Internal Video Outputs.** Licensed Products may Pass without restriction the uncompressed Digital Video Content of decrypted WMDRM Content to Internal Video Outputs.

COMPLIANCE RULES FOR WMDRM FOR NETWORK DEVICES APPLICATIONS

1. DEFINITIONS

The following terms have the meanings set forth below. Other initially capitalized terms not defined in these Compliance Rules have the meanings ascribed to them in the License Agreement or the Microsoft Implementation.

- 1.1 “Analog Audio Outputs” means a connector for an analog sound amplification reproduction device such as a speaker or headphones. For avoidance of doubt, this includes both external jacks to connect speakers and/or headphones and built-in speakers and/or headphones.
- 1.2 “Analog Computer Monitor Output” means a connector for an analog monitor typically found and associated with a Computer Product and that carries uncompressed analog video signals. The term expressly includes those outputs known as VGA, SVGA, XGA, DVI Analog, and various non-standardized analog monitor connections which have been implemented by manufacturers, and expressly does not include such typical consumer electronics connectors as NTSC, PAL, SECAM, SCART, YPrPb, S-Video and Consumer RGB, whether or not such connectors are found on any Computer Product.
- 1.3 “Analog Protection System (APS) trigger bits (APSTB)” means the bits as specified (a) for NTSC video signals, in IEC 61880 (for inclusion of such value on Line 20) or EIA-608-B (for inclusion of such value on Line 21) or (b) for YUV (525/60 systems) signals, in IEC 61880 (for inclusion of such value on Line 20) or EIA-608-B (for inclusion of such value on Line 21).
- 1.4 “Analog Television Output” means such typical consumer electronics analog connectors as NTSC, PAL, SECAM, SCART, YPrPb, S-Video and Consumer RGB.
- 1.5 “Analog Video Content” means audiovisual works, as defined in 17 U.S.C. § 101, recorded in an analog format.
- ~~1.6 “Approved Outputs” means Analog Audio Outputs, Analog Computer Monitor Outputs, Analog Television Outputs, Digital Audio Outputs, Digital Video Outputs, Internal Video Outputs and USB Audio Outputs.~~
- 1.6 ~~1.7~~ “Audio Outputs” means Analog Audio Outputs, Digital Audio Outputs and USB Audio Outputs.

- 1.7 ~~1.8~~ “Automatic Gain Control (AGC)” means the so-named copy control system as specified (a) for NTSC, PAL, SECAM or YUV analog video signals, in the document entitled “Specification of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999,” and (b) for a 480p progressive scan analog video signal, in the document entitled “Specification of the Macrovision AGC Copy Protection Waveforms for DVD Applications with 525p (480p) Progressive Scan Outputs, Revision 1.03 (December 22, 1999).”
- 1.8 ~~1.9~~ “CGMS-A” means the Copy Generation Management System (Analog) as specified (a) for NTSC analog video signals, in IEC 61880 (for inclusion on Line 20) or in EIA-608-B (for inclusion on Line 21), (b) for PAL, SECAM or YUV analog video signals, in IEC 61880 (for inclusion on Line 20) or in EIA-608-B (for inclusion on Line 21) or in EIA-805 (for inclusion on Line 41) for YUV (525/60 systems) signals or in ETS 300924 for PAL, SECAM and YUV (625/50 systems) signals, or (c) for 480p progressive scan analog video signals, in, or adapted without material change from, EIAJ CPR1204-1 (defining the signal waveform carrying the CGMS-A) and IEC 61880 (defining the bit assignment for CGMS-A).
- 1.9 ~~1.10~~ “Certificate” means a unique WMDRM object used to assess trust.
- 1.10 ~~1.11~~ “Colorstripe” means the so-named copy control system as specified for NTSC analog video signals in the document entitled “Specification of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999.”
- 1.11 ~~1.12~~ “Company” means an entity licensed under a License Agreement to develop Licensed Products.
- 1.12 ~~1.13~~ “Company Certificate” means a Certificate issued by Microsoft and unique to Company.
- ~~1.14~~ “~~Contract Manufacturer Certificate~~” means a Certificate issued by Company and unique to a contract manufacturer for use on Company’s behalf.
- 1.13 ~~1.15~~ “Computer Product” means a device that is designed or permits the end user to install software applications thereon, including, but not limited to, personal computers, handheld “Personal Digital Assistants,” and the like.
- 1.14 ~~1.16~~ “Consistent with the Microsoft Implementation” means the Licensed Product (i) provides equivalent functionality to the Microsoft Implementation, (ii) equals or exceeds the security of the Microsoft

Implementation, and (iii) maintains compatibility and interoperability with the Microsoft Implementation.

~~1.17~~ ~~“Content Key” means a symmetric key used to decrypt WMDRM Content.~~

1.15 ~~1.18~~ “Content” means audio and/or video that are transmitted or distributed, either by broadcast, cablecast, or other means of distribution to the general public or on demand.

1.16 ~~“Content Key” means a symmetric key used to decrypt WMDRM Content.~~

1.17 ~~“Contract Manufacturer Certificate” means a Certificate issued by Company and unique to a contract manufacturer for use on Company’s behalf.~~

1.18 ~~1.19~~ “Cryptographically Random” means unpredictable, in that, ~~at no polynomial-time algorithm, given any point regardless sequence of how many preceding bits are available, can guess the probability of predicting the next~~ succeeding K bits ~~is with probability~~ greater than $\frac{1}{2}^K + \frac{1}{P(K)}$ ~~for any (positive) polynomial P and sufficiently large K.~~

1.19 ~~1.20~~ “Device Certificate” means a Certificate issued by or on behalf of Company, assigned to a Licensed Product and used, for example, to evaluate whether the Licensed Product is trusted and eligible to receive WMDRM Content.

1.20 ~~1.21~~ “Device Keys” means an associated pair of Cryptographically Random asymmetric keys generated by or on behalf of Company for inclusion in Licensed Products, comprising a “Device Public Key” and a “Device Private Key”.

1.21 ~~1.22~~ “Device Private Key” means a unique, Cryptographically Random asymmetric private key generated by or for Licensed Products for the purpose of decrypting Content Keys.

1.22 ~~1.23~~ “Device Public Key” means the public portion of the Device Keys.

1.23 ~~1.24~~ “Digital Audio Content” means sound recordings, as defined in 17 U.S.C. § 101, recorded in a digital format.

1.24 ~~1.25~~ “Digital Audio Output” means digital audio signals conforming to IEC-958, IEC-60958, or IEC-61937.

1.25 ~~1.26~~ “Digital Video Content” means audiovisual works, as defined in 17 U.S.C. § 101, recorded in a digital format.

- 1.26 ~~1.27~~ “Digital Video Output” means the digital interface portion only of Digital Visual Interface (DVI), a digital interface standard created by the Digital Display Working Group (DDWG), and the DVI digital interface portion of the High-Definition Multimedia Interface (HDMI).
- 1.27 ~~1.28~~ “Firmware Certificate” means a Certificate issued by or on behalf of Company that is unique to each model number and/or firmware revision of a Licensed Product.
- 1.28 ~~1.29~~ “HDCP” means High-Bandwidth Digital Content Protection (“HDCP”) protected ~~output~~Output. The HDCP specification and license agreement are available from Digital Content Protection, LLC at <http://www.digital-cp.com/>.
- 1.29 ~~1.30~~ “Internal Video Output” means any display that is permanently connected to the Licensed Product, including, but not limited to, a liquid crystal display (“LCD”).
- 1.30 ~~1.31~~ “License Agreement” means the agreement under which Microsoft licenses entities to develop and distribute ~~products~~WMDRM-ND Receivers that include implementations of WMDRM-ND.
- 1.31 ~~1.32~~ “Licensed Product” means a hardware device or software application (or other software component, which may be a separately identifiable subset of a software application or operating system) that (i) implements WMDRM-ND subject to a license from Microsoft and (ii) is capable of playing back WMDRM Content.
- 1.32 ~~1.33~~ “Microsoft Implementation” means the implementation of WMDRM-ND functionality provided as source code, binaries, technical documentation, tools and sample files as provided to the Company under the License Agreement.
- 1.33 “Output” means Analog Audio Outputs, Analog Computer Monitor Outputs, Analog Television Outputs, Digital Audio Outputs, Digital Video Outputs, Internal Video Outputs and USB Audio Outputs. Output does not include Streaming WMDRM Content to a WMDRM-ND Receiver.
- 1.34 “Output Protection Level” means a number included in WMDRM Policy that corresponds to the content protection that must be applied when ~~passing~~Passing WMDRM Content. The Output Protection Level may be determined and assigned by the content owner or may be assigned by the WMDRM Implementation for specific categories of WMDRM Content.

- 1.35 [“Pass” means to direct decrypted WMDRM Content to flow to Outputs, optionally \(though not necessarily\) through intermediate components such as a codec or device driver.](#)
- 1.36 ~~1.35~~ “Play” means the first decrypt of WMDRM Content.
- 1.37 ~~1.36~~ “Secure Audio Device Drivers” means audio device drivers that either 1) are not capable of being replaced by an end user or 2) are verified not to have been modified, are trusted not to expose decrypted WMDRM Content, and ensure that only the secure driver is capable of receiving the WMDRM Content through encryption or other means. For avoidance of doubt, a Licensed Product that prevents end users from upgrading the audio device drivers is considered to have Secure Audio Device Drivers.
- 1.38 ~~1.37~~ “Secure Codecs” means audio and/or video codecs that either 1) are not capable of being replaced by an end user or 2) are verified not to have been modified, are trusted not to expose decrypted WMDRM Content, and prevent intermediate software from accessing WMDRM Content. For avoidance of doubt, a Licensed Product that prevents end users from replacing the codecs is considered to have Secure Codecs.
- 1.39 ~~1.38~~ “Security Level” means a number in the WMDRM Policy associated with specific WMDRM Content that specifies the minimum security level necessary for a Licensed Product to be able to acquire a WMDRM License for the WMDRM Content.
- 1.40 [“Stream” means to transport encrypted WMDRM Content over a network, to the extent permitted by applicable WMDRM Policy, to a WMDRM-ND Receiver for Passing to an Output immediately or shortly after receipt of the WMDRM Content in the WMDRM-ND Receiver.](#)
- 1.41 ~~1.39~~ “Temporary Storage” means storage that cannot retain data for an indefinite period of time after power is withdrawn.
- 1.42 ~~1.40~~ “Unrestricted Audio Outputs” means Analog Audio Outputs and USB Audio Outputs.
- 1.43 ~~1.41~~ “USB Audio Output” means a speaker, headphones or other sound reproduction device attached that complies with the Universal Serial Bus (USB) Audio Specification available from the USB Forum.
- 1.44 ~~1.42~~ “WMDRM” means Windows Media Digital Rights Management technology.
- 1.45 ~~1.43~~ “WMDRM Content” means audio or audiovisual content that has been encrypted and recorded using WMDRM.

- 1.46 ~~1.44~~ “WMDRM License” means a data structure that contains, but is not limited to, WMDRM Policy and an encrypted Content Key associated with specific WMDRM Content.
- 1.47 ~~1.45~~ “WMDRM Policy” means the description of the actions permitted and/or required for or with WMDRM Content and restrictions on those actions as described in the WMDRM License associated with the WMDRM Content.
- 1.48 ~~1.46~~ “WMDRM-ND” means WMDRM for Network Devices.
- 1.49 ~~1.47~~ “WMDRM-ND Receiver” means a product licensed under the License Agreement for WMDRM-ND Applications that complies with the applicable Compliance Rules and may connect to WMDRM-ND Transmitters and acquire WMDRM Licenses and WMDRM Content from such WMDRM-ND Transmitters.
- 1.50 ~~1.48~~ “WMDRM-ND Transmitter” means a product or application licensed or implemented by Microsoft that complies with the applicable Compliance Rules and may connect to WMDRM-ND Receivers and issue WMDRM Licenses and WMDRM Content.

2. SCOPE. These Compliance Rules apply to Licensed Products implementing WMDRM-ND functionality and receiving content from WMDRM-ND Transmitters. These Compliance Rules set forth the requirements pursuant to which WMDRM-ND Receivers may play back and ~~output~~Output WMDRM Content.

3. REQUIREMENTS FOR WMDRM-ND APPLICATIONS

3.1 **Content Caching.** Licensed Products may store up to but no more than five (5) minutes of WMDRM Content per content stream in Temporary Storage for the sole purpose of reducing the effects of network congestion and optimizing playback performance. Licensed Products must delete the cached reference of WMDRM Content from Temporary Storage once Licensed Products begin ~~passing~~Passing a new piece of WMDRM Content.

3.2 **Serial Number.** Company or a contract manufacturer acting on Company’s behalf must assign a unique Serial Number with a minimum length of 128 bits to each Licensed Product manufactured by or on behalf of Company.

3.3 **WMDRM-ND Certificates.**

3.3.1 **Company Certificate.** Microsoft shall provide to Company the Company Certificate. Company shall use the Company Certificate to sign Firmware Certificates and/or Contract Manufacturer Certificates.

3.3.2 **Contract Manufacturer Certificates.** Contract Manufacturer Certificates are optional except that if Company uses a contract manufacturer, then Company shall issue a unique Contract Manufacturer Certificate for use by the contract manufacturer on Company's behalf. Each Contract Manufacturer Certificate must be signed with the Private Key corresponding to the Company Certificate. Contract Manufacturer Certificates must be Consistent with the Microsoft Implementation.

3.3.2.1 **SignCertificate.** Contract Manufacturer Certificates must only contain a KeyUsage right of SignCertificate.

3.3.3 **Firmware Certificates.** Firmware Certificates must be unique for each model number of a Licensed Product. If a Licensed Product undergoes a firmware revision, then each firmware version must have a unique Firmware Certificate. Firmware Certificates must be signed with the Private Key corresponding to the Company Certificate or the Contract Manufacturer Certificate. Firmware Certificates must be Consistent with the Microsoft Implementation.

3.3.3.1 **SignCertificate.** Firmware Certificates must only contain a KeyUsage right of SignCertificate.

3.3.4 **Device Certificates.** Company or a contract manufacturer acting on Company's behalf shall issue a unique Device Certificate for inclusion in each model or firmware/revision of each Licensed Product manufactured by or on behalf of Company. Device Certificates must be signed with the Private Key corresponding to the Firmware Certificate. Device Certificates must be Consistent with the Microsoft Implementation.

3.3.4.1 **EncryptKey.** Device Certificates must only contain a KeyUsage right of EncryptKey.

3.3.4.2 **Security Level.** Device Certificates must contain the appropriate Security Level as provided to Company by Microsoft.

3.3.5 **WMDRM-ND Certificate Keys.** A Cryptographically Random Public Key and Private Key must be generated by Company or a contract manufacturer acting on Company's behalf for inclusion in all WMDRM-ND Certificates. The Public Key and Private Key must be unique for each Certificate.

4. REQUIREMENTS FOR COMPLYING WITH WMDRM POLICY

The following Compliance Rule is applicable to the WMDRM Policy as specified in the WMDRM License:

4.1 **Unspecified policy.** WMDRM Policy may specify additional rights, restrictions or parameters that are not covered in these Compliance Rules. Nevertheless Licensed Products must only take action based on rights and enforce restrictions covered in this document and in a manner Consistent with the Microsoft Implementation.

5. PLAYBACK AND OUTPUT CONTROL RULES FOR LICENSED PRODUCTS

Licensed Products must comply with the following:

5.1 **Playback Control.** Licensed Products must comply with the following rules for playback control:

5.1.1 **Playback.** Licensed Products may ~~pass~~Pass decrypted WMDRM Content through the ~~outputs~~Outputs described in Sections 5.2 and 5.3 only if the right to Play is included in a WMDRM License associated with such WMDRM Content.

5.2 **Restricted Outputs.** Licensed Products must detect and accurately respond to the Output Protection Levels for WMDRM Content.

5.2.1 **Output Control for Digital Compressed Audio Content.** If a Licensed Product ~~passes~~Passes compressed Digital Audio Content, the Licensed Product must follow restrictions as specified in the WMDRM License and this Section 5.2.1. Licensed Products may ~~pass~~Pass compressed Digital Audio Content to Secure Codecs provided the decompressed Digital Audio Content is handled consistent with Section 5.2.2.

5.2.1.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may ~~pass~~Pass without restriction compressed Digital Audio Content of decrypted WMDRM Content to Audio Outputs.

5.2.1.2 **Level 101 to 200.** If the Output Protection Level specified in the WMDRM License is greater than 100 and less than or equal to 200, Licensed Products may ~~pass~~Pass, without restriction, the compressed Digital Audio Content of decrypted WMDRM Content via Secure Audio Device Drivers to Audio Outputs.

5.2.1.3 **Level 201 to 300.** If the Output Protection Level specified in the WMDRM License is greater than 200 and less than or equal to 300,

Licensed Products may ~~pass~~Pass compressed Digital Audio Content of decrypted WMDRM Content via Secure Audio Device Drivers to Unrestricted Audio Outputs.

5.2.1.4 **Level 301 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not ~~pass~~Pass compressed Digital Audio Content of decrypted WMDRM Content.

5.2.2 **Output Control for Digital Uncompressed Audio Content.** If a Licensed Product ~~passes~~Passes uncompressed Digital Audio Content, the Licensed Products must follow restrictions as specified in the WMDRM License and this Section 5.2.2.

5.2.2.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may ~~pass~~Pass without restriction digital uncompressed Digital Audio Content of decrypted WMDRM Content to Audio Outputs.

5.2.2.2 **Level 101 to 200.** If the Output Protection Level specified in the WMDRM License is greater than 100 and less than or equal to 200, Licensed Products may ~~pass~~Pass, without restriction, the uncompressed Digital Audio Content of decrypted WMDRM Content via Secure Audio Device Drivers to Audio Outputs.

5.2.2.3 **Level 201 to 300.** If the Output Protection Level specified in the WMDRM License is greater than 200 and less than or equal to 300, Licensed Products may ~~pass~~Pass uncompressed Digital Audio Content of decrypted WMDRM Content via Secure Audio Device Drivers to Unrestricted Audio Outputs.

5.2.2.4 **Level 301 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not ~~pass~~Pass uncompressed Digital Audio Content of decrypted WMDRM Content.

5.2.3 **Output Control for Digital Compressed Video Content.** Licensed Products must not ~~pass~~Pass ~~decrypted~~ compressed Digital Video Content to any ~~output~~Output, except that a Licensed Product may Pass Content marked with the ATSC Standard A/65B Redistribution Control descriptor (rc descriptor()) to any Output protected by a digital content protection technology approved by the Federal Communications Commission (or otherwise approved in accordance with applicable Federal Communications Commission rules) for use with such Content. Licensed Products may ~~pass~~Pass compressed Digital Video Content to Secure Codecs provided that the decompressed Digital Video Content is handled consistent with Section 5.2.4.

5.2.4 **Output Control for Digital Uncompressed Video Content.** If a Licensed Product ~~passes~~Passes uncompressed Digital Video Content, the Licensed Product must follow restrictions as specified in the WMDRM License and this Section 5.2.4.

5.2.4.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may ~~pass~~Pass, without restriction, the uncompressed Digital Video Content of decrypted WMDRM Content on Video Outputs.

5.2.4.2 **Level 101 to 300.** If the Output Protection Level specified in the WMDRM License is greater than 100 and less than or equal to 300 and Licensed Product is ~~passing~~Passing Digital Video Content to Digital Video Outputs, the Licensed Product must engage HDCP to protect the uncompressed Digital Video Content of decrypted WMDRM Content. Licensed Products must verify that the HDCP Source Function is engaged and able to deliver protected content, which means HDCP encryption is operational on such ~~output~~Output.

5.2.4.3 **Level 301 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not ~~pass~~Pass uncompressed Digital Video Content of decrypted WMDRM Content on Digital Video Outputs.

5.2.5 **Output Control for Analog Video Content.** If a Licensed Product ~~passes~~Passes the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs, the Licensed Product must follow restrictions as specified in the WMDRM License and this Section 5.2.5. Additional restrictions may be required as specified in Section 5.2.6.

5.2.5.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may ~~pass~~Pass without restriction the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs.

5.2.5.2 **Level 101 to 200.** If the Output Protection Level specified in the WMDRM Licenses is greater than 100 but less than or equal to 200 and the Licensed Product is ~~passing~~Passing the Analog Video Content of decrypted WMDRM Content to the Analog Television Outputs, the Licensed Product must engage CGMS-A with the CGMS field in the copy set to '11' ("no more copies").

5.2.5.3 **Level 201 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 200, Licensed Products must not ~~pass~~Pass the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs.

5.2.6 **Output Control for Extended Analog Video Content.** If a Licensed Product ~~passes~~Passes the video portion of Decrypted WMDRM Content to Analog Television Outputs, the Licensed Product must follow restrictions as specified in the WMDRM License and this Section 5.2.6. Additional restrictions may be required as specified in Section 5.2.5.

5.2.6.1 **Automatic Gain Control and ColorStripe.** If Extended Analog Video Protection List in the WMDRM License includes “C3FD11C6-F8B7-4d20-B008-1DB17D61F2DA”, Licensed Products must engage Automatic Gain Control and ColorStripe and set the APSTB field as based on the Extended Analog Video Protection Configuration Data included in the WMDRM License. Additional technologies and restrictions may be required as specified in Section 5.2.5. For avoidance of doubt, the permitted APSTB values in the WMDRM License are as follows:

APSTB values	Description	NTSC	PAL
00	AGC and ColorStripe is disabled	Disabled <u>Off</u>	Disable <u>Off</u>
01	AGC Only	APS1	APS1
10	AGC and 2 line ColorStripe	APS2	APS1
11	AGC and 4 line ColorStripe	APS3	APS1

5.3 **Unrestricted Outputs.** Unless otherwise specified in Section 5.2, Licensed Products may ~~pass~~Pass without restriction WMDRM Content to the following ~~outputs~~Outputs provided the requirements in Section 5.1.1 are met.

5.3.1 **Analog Audio Outputs.** Licensed Products may ~~pass~~Pass without restriction the Analog Audio Content of decrypted WMDRM Content to Analog Audio Outputs.

5.3.2 **USB Audio Outputs.** Licensed Products may ~~pass~~Pass without restriction the uncompressed Digital Audio Content of decrypted WMDRM Content to USB Audio Outputs.

5.3.3 **Analog Computer Monitor Outputs.** Licensed Products may ~~pass~~Pass without restriction the uncompressed Analog Video Content of decrypted WMDRM Content to Analog Computer Monitor Outputs.

5.3.4 **Internal Video Outputs.** Licensed Products may ~~pass~~Pass without restriction the uncompressed Digital Video Content of decrypted WMDRM Content to Internal Video Outputs.

EXHIBIT 5

COMPLIANCE RULES FOR WMDRM FOR PORTABLE DEVICES PLATFORMS

1. DEFINITIONS

The following terms have the meanings set forth below. Other initially capitalized terms not defined in these Compliance Rules have the meanings ascribed to them in the License Agreement, the Compliance Rules for WMDRM for Portable Devices Applications, or the Microsoft Implementation.

- 1.1 “Anti-Rollback Clock” means a real time clock that is verified to have continued to advance each time WMDRM is executed.
- 1.2 “Certificate” means a unique WMDRM object used to assess trust.
- 1.3 “Clock Rollback Event” means the detection by WMDRM that the current date and time precedes the date and time last recorded by WMDRM.
- 1.4 “Company” means an entity licensed under a License Agreement to develop Licensed Products.
- 1.5 “Consistent with the Microsoft Implementation” means the Licensed Product (i) provides equivalent functionality to the Microsoft Implementation, (ii) equals or exceeds the security of the Microsoft Implementation, and (iii) maintains compatibility and interoperability with the Microsoft Implementation.
- 1.6 “Content” means audio and/or video that are transmitted or distributed, either by broadcast, cablecast, or other means of distribution to the general public or on demand.
- 1.7 “Content Key” means a symmetric key used to decrypt WMDRM Content.
- 1.8 “Copy” means to transport encrypted WMDRM Content over a USB connection, to the extent permitted by applicable WMDRM Policy, to a Licensed Product for Passing to Outputs at any time and/or for as many times as permitted by applicable WMDRM Policy.
- 1.9 “Cryptographic Keys” means Content Key, Device Keys, Device Certificate Signing Keys, Fallback Keys, and Privacy Key.
- 1.10 “Cryptographically Random” means unpredictable, in that no polynomial-time algorithm, given any sequence of bits, can guess the succeeding K bits with probability greater than $\frac{1}{2}^K + 1/P(K)$ for any (positive) polynomial P and sufficiently large K.

- 1.11 “Device Certificate” means a Certificate issued by Company or contract manufacturer on Company’s behalf, assigned to each Licensed Product and used, for example, to evaluate whether the Licensed Product is trusted and eligible to receive WMDRM Content.
- 1.12 “Device Certificate Signing Keys” means an associated pair of Cryptographically Random asymmetric keys generated by Company for each of its Licensed Products, comprising: “Device Certificate Signing Public Key”; and “Device Certificate Signing Private Key”.
- 1.13 “Device Certificate Signing Private Key” means the private portion of the Device Certificate Signing Keys.
- 1.14 “Device Certificate Signing Public Key” means the public portion of the Device Certificate Signing Keys.
- 1.15 “Device Key” means unique Cryptographically Random key or keys generated by Company for each of its Licensed Products for the purpose of decrypting Content Keys.
- 1.16 “Digital Audio Content” means sound recordings, as defined in 17 U.S.C. § 101, recorded in a digital format.
- 1.17 “Digital Video Content” means audiovisual works, as defined in 17 U.S.C. § 101, recorded in a digital format.
- 1.18 “Direct License Acquisition” or “DLA” means the process of acquiring a WMDRM license directly from a WMDRM Server.
- 1.19 “Fallback Keys” means an associated pair of keys for Licensed Products for the purpose of Direct License Acquisition from WMDRM Servers.
- 1.20 “ILA Receiver” means Licensed Products that may connect to ILA Transmitters and acquire WMDRM Licenses.
- 1.21 “ILA Transmitter” means Licensed Products that may connect to ILA Receivers and issue WMDRM Licenses.
- 1.22 “Indirect License Acquisition” or “ILA” means the process of acquiring a WMDRM license via an ILA Transmitter using the MTP or RAPI protocol over USB.
- 1.23 “License Acquisition” means acquiring a WMDRM License from an ILA Transmitter or WMDRM Server.

- 1.24 “License Agreement” means the agreement under which Microsoft licenses entities to develop and distribute products that include implementations of WMDRM-PD.
- 1.25 “License Evaluation” means, but is not limited to, the process of parsing the WMDRM License, verifying the signature and evaluating the syntax for the purpose of determining the WMDRM Policy and the Content Key.
- 1.26 “Licensed Product” means a hardware device or software application (or other software component, which may be a separately identifiable subset of a software application or operating system), that (i) implements WMDRM-PD subject to a license from Microsoft and (ii) is capable of playing back WMDRM Content.
- 1.27 “Media Transfer Protocol” or “MTP” means Microsoft’s Media Transfer Protocol for device control, metadata exchange and media transfer, which is only supported over USB 1.0 or later.
- 1.28 “Metering” is a feature of WMDRM-PD designed to securely collect and report content usage information.
- 1.29 “Microsoft Implementation” means the implementation of WMDRM-PD functionality provided as source code, binaries, technical documentation, tools and/or sample files as provided to the Company under the License Agreement.
- 1.30 “Optional Features” includes, but is not limited to: Direct License Acquisition; License Synchronization; Metering; Secure Clock; and Anti-Rollback Clock.
- 1.31 “Output” means Analog Audio Outputs, Analog Computer Monitor Outputs, Analog Television Outputs, Digital Audio Outputs, Digital Video Outputs, Internal Video Outputs and USB Audio Outputs. Output does not include Copying WMDRM Content to a Licensed Product over a USB connection.
- 1.32 “Pass” means to direct decrypted WMDRM Content to flow to Outputs, optionally (though not necessarily) through intermediate components such as a codec or device driver.
- 1.33 “Persistent Storage” means storage that can retain data for an indefinite period of time after power is withdrawn.
- 1.34 “Play” means the first decrypt of WMDRM Content.

- 1.35 “Privacy Key” means an asymmetric public key provided by Microsoft for the purpose of encrypting sensitive communication sent over a public network.
- 1.36 “Remote Application Programming Interface” or “RAPI” means Microsoft’s implementation of RAPI protocol on Microsoft Windows Mobile.
- 1.37 “Secure Clock” means a hardware real time clock that has been secured from unauthorized access.
- 1.38 “Secure Clock Service” means an Internet service authorized by Microsoft for the purpose of providing the current UTC date and time through a secure protocol.
- 1.39 “Security Level” means a number in the WMDRM Policy associated with specific WMDRM Content that specifies the minimum security level necessary for a Licensed Product to be able to acquire a WMDRM License for the WMDRM Content.
- 1.40 “Temporary Storage” means storage that cannot retain data for an indefinite period of time after power is withdrawn.
- 1.41 “UTC” means Universal Time Coordinated.
- 1.42 “WMDRM” means Windows Media Digital Rights Management technology.
- 1.43 “WMDRM Content” means audio or audiovisual content that has been encrypted and recorded using WMDRM.
- 1.44 “WMDRM Data Stores” means the secure databases required for mandatory and optional WMDRM features. This includes, but is not limited to, License store, Secure store, Metering store and License Synchronization store as defined in the Microsoft Implementation.
- 1.45 “WMDRM License” means a data structure that contains, but is not limited to, WMDRM Policy and an encrypted Content Key associated with specific WMDRM Content.
- 1.46 “WMDRM Policy” means the description of the actions permitted and/or required for or with WMDRM Content and restrictions on those actions as described in the WMDRM License associated with the WMDRM Content.
- 1.47 “WMDRM Server” means a Licensed Product capable of issuing WMDRM Licenses over a network connection.

- 1.48 “WMDRM-PD” means WMDRM for Portable Devices.
- 1.49 “WMDRM-PD MTP Extensions Technical Documentation” means the Technical Documentation, included in the Microsoft Implementation, that describes how to call WMDRM-PD from MTP.

2. SCOPE. These Compliance Rules apply to Licensed Products implementing WMDRM-PD functionality, including without limitation Windows CE. These Compliance Rules set forth the requirements pursuant to which Licensed Products must enforce the WMDRM controls applicable to the transfer, playback or rendering, and output of WMDRM Content on Licensed Products implementing WMDRM-PD functionality.

3. REQUIREMENTS FOR WMDRM PD IMPLEMENTATIONS

3.1 **Functionality.** When a Licensed Product implements any WMDRM functionality, it must do so in a manner Consistent with the Microsoft Implementation of that same functionality. This requirement is in addition to all of the specific Compliance Rules set forth in this document. In the event of a conflict between how the Microsoft Implementation implements a given WMDRM functionality and how a specific compliance rule in this document describes how such implementation must be accomplished, the Compliance Rules are controlling.

3.2 **Optional Features.** Licensed Products may implement optional features of WMDRM-PD provided that any chosen optional features are implemented in accordance with the applicable Compliance and Robustness Rules. The only optional features are Direct License Acquisition, License Synchronization, Metering, Secure Clock and Anti-Rollback Clock.

3.3 **Mandatory Features.** All features not listed as optional in Section 3.2 are mandatory features. Licensed Products must implement all mandatory features.

3.4 **Random Number Generator.** Licensed Products must implement and make use of a random number generator that is Cryptographically Random. For the avoidance of doubt, linear congruential random number generators are not acceptable.

3.5 **Device Certificate.** Licensed Products must implement Device Certificate signing procedures.

3.6 **Data Stores.** Licensed Products must implement support for WMDRM Data Stores. If optional features are implemented, the corresponding Data Stores must be supported.

3.7 **License Acquisition.** Licensed Products must support one or both of the following methods of License Acquisition.

3.7.1 **Indirect License Acquisition.** Licensed Products that implement receiving WMDRM Licenses from an ILA Transmitter must support all mandatory features and supported optional features via the MTP protocol as specified in the WMDRM-PD MTP Extensions Technical Documentation or RAPI protocol.

3.7.2 **Direct License Acquisition.** Licensed Products that support acquiring WMDRM Licenses from WMDRM Servers must implement Direct License Acquisition functionality.

3.8 **License Evaluation.** Licensed Products must implement License Evaluation.

3.9 **Cryptographic Keys**

3.9.1 **Device Key.** A Cryptographically Random Device Key must be generated by the Company for each Licensed Product. The Device Key must be unique for each Licensed Product manufactured by Company.

3.9.2 **Device Certificate Signing Keys.** A Cryptographically Random Device Certificate Signing Public and Private Key must be generated by the Company for Licensed Products. The Device Certificate Signing Public and Private Key must be unique for each Licensed Product with different functionality, for example for two different model numbers or revisions.

3.9.3 **Privacy Public Key.** All DLA transmissions must be encrypted with the Privacy Public Key.

3.9.4 **Fallback Keys.** If a Licensed Product supports the optional feature DLA, the Licensed Product may store Fallback Keys.

3.10 **Real Time Clock.** Licensed Products that support use of WMDRM Licenses including expiration, as described in Section 4.3, must implement a Real Time Clock. The Real Time Clock must be capable of maintaining time accurately with a clock drift no more than two minutes per month and a minimum resolution of one second. Licensed Products may implement either an Anti-Rollback Clock or Secure Clock as described below.

3.10.1 **Anti-Rollback Clock.** Anti-Rollback Clock, if supported, must be implemented as follows.

3.10.1.1 **Clock Reset.** When power is lost to the Licensed Product, the clock must be automatically reset in such a way that the reset date and time after reset precedes by one year the day on which the device was manufactured. Before playing WMDRM Content, the Licensed Product must set the initial date and time to no

later than 1/1/2000 at 12:00:00 AM and require the user to set a date and time subsequent to the last date and time recorded by WMDRM to be valid.

3.10.1.2 **Clock Rollback.** When a Licensed Product detects a Clock Rollback Event, it must iterate through all WMDRM Licenses stored in the WMDRM License Store and take the appropriate actions as specified in Section 4.3.5 and 4.3.6 respectively.

3.10.2 **Secure Clock.** Secure Clock, if supported, must be implemented as follows.

3.10.2.1 **Authorized Service.** Licensed Products must connect only to a Secure Clock Service.

3.10.2.2 **Clock Reset.** When power is lost to a Licensed Product, the clock must be reset such that when power is regained, the Licensed Product must detect the loss of power and set the state of the Secure Clock to an unset or unsecured state.

3.10.2.3 **Grace Period.** Licensed Products must implement support for Grace Period.

4. REQUIREMENTS FOR COMPLYING WITH WMDRM POLICY

The following Compliance Rules are applicable to the WMDRM Policy as specified in the WMDRM License.

4.1 **Security Level.** A Licensed Product must decrypt WMDRM Content using only WMDRM Licenses that have a Security Level less than or equal to the Security Level for such Licensed Product.

4.2 **Unspecified Policy.** WMDRM Policy may specify additional rights, restrictions or parameters that are not covered in these Compliance Rules. Nevertheless Licensed Products must only take action based on rights and enforce restrictions covered in this document and Consistent with the Microsoft Implementation. To the extent that WMDRM Policy (or a particular WMDRM License) describes additional rights, restrictions or parameters that are not described in these Compliance Rules, Licensed Products must ignore such additional rights, restrictions or parameters.

4.3 **Expiration.** Licensed Devices that support a Clock must implement expiration support as follows:

4.3.1 **Begin Date.** If specified in the WMDRM License, Licensed Products must not allow the associated WMDRM Content to be Passed before the specified date and time.

4.3.2 **End Date.** If specified in the WMDRM License, Licensed Products must not allow the associated WMDRM Content to be Passed after the specified date and time.

4.3.3 **ExpirationAfterFirstUse.** If specified in the WMDRM License, upon first use of the associated WMDRM Content, the specified number of hours must be added to the current date and time and the sum stored in the Secure Store. This sum must then be evaluated as specified in Section 4.3.2.

4.3.4 **ExpirationOnStore.** If specified in the WMDRM License, upon storing the WMDRM License the specified number of hours must be added to the current date and time and the sum stored in the Secure Store. This sum must then be evaluated as specified in Section 4.3.2.

4.3.5 **DisableOnClockRollback.** If a Licensed Product implements Anti-Rollback Clock and detects and processes a Clock Rollback Event, the Licensed Product must make inaccessible any WMDRM License specifying DisableOnClockRollback. When a Licensed Product detects that the current date and time exceeds the last known good date and time, it must re-enable access to any WMDRM License that specifies DisableOnClockRollback.

4.3.6 **DeleteOnClockRollback.** If a Licensed Product implements Anti-Rollback Clock and detects and processes a Clock Rollback Event, WMDRM must delete any WMDRM License that specifies DeleteOnClockRollback.

4.4 **Metering.** Metering, if supported, must be implemented as follows:

4.4.1 **Implementation.** Each time a WMDRM License that includes a Metering ID is used to decrypt and Pass WMDRM Content, the Licensed Products must update the WMDRM Metering Store.

4.4.2 **Metering Update.** When accessing WMDRM Content with an associated WMDRM License that requires Metering, the Metering Store must be updated when the associated WMDRM Content is first decrypted and Passed. For Licensed Products first introduced prior to June 30, 2005, the update to the Metering Store may be postponed, provided that reasonable steps are taken to update the Metering Store before the next time the Licensed Product communicates with an ILA Transmitter or Network.

4.4.3 **Insufficient Storage.** If a Licensed Product does not have Persistent Storage available to persist updates to Metering, it must not decrypt and Pass WMDRM Content using any WMDRM License specifying a Metering ID.

4.4.4 **Delayed Updates.** If a Licensed Product caches WMDRM Content including only Audio Content in Temporary Storage and Persistent Storage is currently unavailable, caching Metering updates is permitted until Persistent Storage thereafter becomes available to record Metering updates, provided that the Licensed

Product (i) confirms prior to decrypting WMDRM Content that sufficient Persistent Storage will be available to record Metering updates and (ii) records any Metering updates cached in temporary storage after Passing no more than thirty (30) minutes of WMDRM Content or ten (10) WMDRM Content files, whichever occurs first. Licensed Products first introduced after June 30, 2005 must not delay updates but must record updates directly in Persistent Storage.

4.5 **Play Count.** A Play count, if present in the WMDRM License, specifies the number of times that the WMDRM License may be used to decrypt and Pass WMDRM Content. Licensed Products must implement Play count as follows:

4.5.1 **Implementation.** If Play count is specified in the WMDRM License, Licensed Products must limit the number of Plays to the specified maximum number. A Play count is decremented when WMDRM Content is first decrypted and Passed.

4.5.2 **Insufficient Storage.** If a Licensed Product does not have available Persistent Storage to record Play count, it must not decrypt WMDRM Content using any WMDRM License that specifies a Play count.

4.5.3 **Delayed Updates.** If a Licensed Product caches WMDRM Content including only Audio Content in Temporary Storage and Persistent Storage is currently unavailable, caching Play count updates is permitted until Persistent Storage is available to record Play count updates, provided that the Licensed Product (i) confirms, prior to decrypting additional WMDRM Content, that sufficient Persistent Storage will be available to record Play count updates and Play counts remaining for WMDRM Content, and (ii) records any Play count updates cached in Temporary Storage after Passing no more than thirty (30) minutes of WMDRM Content or ten (10) WMDRM content files, whichever occurs first. Licensed Products first introduced after June 30, 2005 must not delay updates but must record updates directly in Persistent Storage.

COMPLIANCE RULES FOR WMDRM FOR PORTABLE DEVICES PLATFORMS

1. DEFINITIONS

The following terms have the meanings set forth below. Other initially capitalized terms not defined in these Compliance Rules have the meanings ascribed to them in the License Agreement, [the Compliance Rules for WMDRM for Portable Devices Applications](#), or the Microsoft Implementation.

- 1.1 “Anti-Rollback Clock” means a real time clock that is verified to have continued to advance each time WMDRM is executed.
- 1.2 “Certificate” means a unique WMDRM object used to assess trust.
- 1.3 “Clock Rollback Event” means the detection by WMDRM that the current date and time precedes the date and time last recorded by WMDRM.
- 1.4 “Company” means an entity licensed under a License Agreement to develop Licensed Products.
- 1.5 “Consistent with the Microsoft Implementation” means the Licensed Product (i) provides equivalent functionality to the Microsoft Implementation, (ii) equals or exceeds the security of the Microsoft Implementation, and (iii) maintains compatibility and interoperability with the Microsoft Implementation.
- ~~1.6~~ “Content Key” means a symmetric key used to decrypt WMDRM Content.
- 1.6 ~~1.7~~ “Content” means audio and/or video that are transmitted or distributed, either by broadcast, cablecast, or other means of distribution to the general public or on demand.
- 1.7 “Content Key” means a symmetric key used to decrypt WMDRM Content.
- 1.8 “Copy” means to transport encrypted WMDRM Content over a USB connection, to the extent permitted by applicable WMDRM Policy, to a Licensed Product for Passing to Outputs at any time and/or for as many times as permitted by applicable WMDRM Policy.
- 1.9 ~~1.8~~ “Cryptographic Keys” means Content Key, Device Keys, Device Certificate Signing Keys, Fallback Keys, and Privacy Key.
- 1.10 ~~1.9~~ “Cryptographically Random” means unpredictable, in that, ~~at any point regardless of how many preceding~~ no polynomial-time

algorithm, given any sequence of bits ~~are available~~, can guess the ~~probability of predicting the next~~ succeeding K bits is with probability greater than $\frac{1}{2}^K + \frac{1}{P(K)}$ for any (positive) polynomial P and sufficiently large K.

- 1.11 ~~1.10~~ “Device Certificate” means a Certificate issued by Company or contract manufacturer on Company’s behalf, assigned to each Licensed Product and used, for example, to evaluate whether the Licensed Product is trusted and eligible to receive WMDRM Content.
- 1.12 ~~1.11~~ “Device Certificate Signing Keys” means an associated pair of Cryptographically Random asymmetric keys generated by Company for each of its Licensed Products, comprising: “Device Certificate Signing Public Key”; and “Device Certificate Signing Private Key”.
- 1.13 ~~1.12~~ “Device Certificate Signing Private Key” means the private portion of the Device Certificate Signing Keys.
- 1.14 ~~1.13~~ “Device Certificate Signing Public Key” means the public portion of the Device Certificate Signing Keys.
- 1.15 ~~1.14~~ “Device Key” means unique Cryptographically Random key or keys generated by Company for each of its Licensed Products for the purpose of decrypting Content Keys.
- 1.16 ~~1.15~~ “Digital Audio Content” means sound recordings, as defined in 17 U.S.C. § 101, recorded in a digital format.
- 1.17 ~~1.16~~ “Digital Video Content” means audiovisual works, as defined in 17 U.S.C. § 101, recorded in a digital format.
- 1.18 ~~1.17~~ “Direct License Acquisition” or “DLA” means the process of acquiring a WMDRM license directly from a WMDRM Server.
- 1.19 ~~1.18~~ “Fallback Keys” means an associated pair of keys for Licensed Products for the purpose of Direct License Acquisition from WMDRM Servers.
- 1.20 ~~1.19~~ “ILA Receiver” means Licensed Products that may connect to ILA Transmitters and acquire WMDRM Licenses.
- 1.21 ~~1.20~~ “ILA Transmitter” means Licensed Products that may connect to ILA ~~Transmitters~~ Receivers and ~~acquire~~ issue WMDRM Licenses.
- 1.22 ~~1.21~~ “Indirect License Acquisition” or “ILA” means the process of acquiring a WMDRM license via an ILA Transmitter using the MTP or RAPI protocol over USB.

- 1.23** ~~1.22~~ “License Acquisition” means acquiring a WMDRM License from an ILA Transmitter or WMDRM Server.
- 1.24** ~~1.23~~ “License Agreement” means the agreement under which Microsoft licenses entities to develop and distribute products that include implementations of WMDRM-PD.
- 1.25** ~~1.24~~ “License Evaluation” means, but is not limited to, the process of parsing the WMDRM License, verifying the signature and evaluating the syntax for the purpose of determining the WMDRM Policy and the Content Key.
- 1.26** ~~1.25~~ “Licensed Product” means a hardware device or software application (or other software component, which may be a separately identifiable subset of a software application or operating system), that (i) implements WMDRM-PD subject to a license from Microsoft and (ii) is capable of playing back WMDRM Content.
- 1.27** ~~1.26~~ “Media Transfer Protocol” or “MTP” means Microsoft’s Media Transfer Protocol for device control, metadata exchange and media transfer, which is only supported over USB 1.0 or later.
- 1.28** ~~1.27~~ “Metering” is a feature of WMDRM-PD designed to securely collect and report content usage information.
- 1.29** ~~1.28~~ “Microsoft Implementation” means the implementation of WMDRM-PD functionality provided as source code, binaries, technical documentation, tools and/or sample files as provided to the Company under the License Agreement.
- 1.30** ~~1.29~~ “Optional Features” includes, but is not limited to: Direct License Acquisition; License Synchronization; Metering; Secure Clock; and Anti-Rollback Clock.
- 1.31** “Output” means Analog Audio Outputs, Analog Computer Monitor Outputs, Analog Television Outputs, Digital Audio Outputs, Digital Video Outputs, Internal Video Outputs and USB Audio Outputs. Output does not include Copying WMDRM Content to a Licensed Product over a USB connection.
- 1.32** “Pass” means to direct decrypted WMDRM Content to flow to Outputs, optionally (though not necessarily) through intermediate components such as a codec or device driver.
- 1.33** ~~1.30~~ “Persistent Storage” means storage that can retain data for an indefinite period of time after power is withdrawn.

- [1.34](#) ~~1.31~~ “Play” means the first decrypt of WMDRM Content.
- [1.35](#) ~~1.32~~ “Privacy Key” means an asymmetric public key provided by Microsoft for the purpose of encrypting sensitive communication sent over a public network.
- [1.36](#) ~~1.33~~ “Remote Application Programming Interface” or “RAPI” means Microsoft’s implementation of RAPI protocol on Microsoft Windows Mobile.
- [1.37](#) ~~1.34~~ “Secure Clock” means a hardware real time clock that has been secured from unauthorized access.
- [1.38](#) ~~1.35~~ “Secure Clock Service” means an Internet service authorized by Microsoft for the purpose of providing the current UTC date and time through a secure protocol.
- [1.39](#) ~~1.36~~ “Security Level” means a number in the WMDRM Policy associated with specific WMDRM Content that specifies the minimum security level necessary for a Licensed Product to be able to acquire a WMDRM License for the WMDRM Content.
- [1.40](#) ~~1.37~~ “Temporary Storage” means storage that cannot retain data for an indefinite period of time after power is withdrawn.
- [1.41](#) ~~1.38~~ “UTC” means Universal Time Coordinated.
- [1.42](#) ~~1.39~~ “WMDRM” means Windows Media Digital Rights Management technology.
- [1.43](#) ~~1.40~~ “WMDRM Content” means audio or audiovisual content that has been encrypted and recorded using WMDRM.
- [1.44](#) ~~1.41~~ “WMDRM Data Stores” means the secure databases required for mandatory and optional WMDRM features. This includes, but is not limited to, License store, Secure store, Metering store and License Synchronization store as defined in the Microsoft Implementation.
- [1.45](#) ~~1.42~~ “WMDRM License” means a data structure that contains, but is not limited to, WMDRM Policy and an encrypted Content Key associated with specific WMDRM Content.
- [1.46](#) ~~1.43~~ “WMDRM Policy” means the description of the actions permitted and/or required for or with WMDRM Content and restrictions on those actions as described in the WMDRM License associated with the WMDRM Content.

- 1.47 ~~1.44~~ “WMDRM Server” means a Licensed Product capable of issuing WMDRM Licenses over a network connection.
- 1.48 ~~1.45~~ “WMDRM-PD” means WMDRM for Portable Devices.
- 1.49 ~~1.46~~ “WMDRM-PD MTP Extensions Technical Documentation” means the Technical Documentation, included in the Microsoft Implementation, that describes how to call WMDRM-PD from MTP.

2. SCOPE. These Compliance Rules apply to Licensed Products implementing WMDRM-PD functionality, including without limitation Windows CE. These Compliance Rules set forth the requirements pursuant to which Licensed Products must enforce the WMDRM controls applicable to the transfer, playback or rendering, and output of WMDRM Content on Licensed Products implementing WMDRM-PD functionality.

3. REQUIREMENTS FOR WMDRM PD IMPLEMENTATIONS

3.1 **Functionality.** When a Licensed Product implements any WMDRM functionality, it must do so in a manner Consistent with the Microsoft Implementation of that same functionality. This requirement is in addition to all of the specific Compliance Rules set forth in this document. In the event of a conflict between how the Microsoft Implementation implements a given WMDRM functionality and how a specific compliance rule in this document describes how such implementation must be accomplished, the Compliance Rules are controlling.

3.2 **Optional Features.** Licensed Products may implement optional features of WMDRM-PD provided that any chosen optional features are implemented in accordance with the applicable Compliance and Robustness Rules. The only optional features are Direct License Acquisition, License Synchronization, Metering, Secure Clock and Anti-Rollback Clock.

3.3 **Mandatory Features.** All features not listed as optional in Section 3.2 are mandatory features. Licensed Products must implement all mandatory features.

3.4 **Random Number Generator.** Licensed Products must implement and make use of a random number generator that is Cryptographically Random. For the avoidance of doubt, linear congruential random number generators are not acceptable.

3.5 **Device Certificate.** Licensed Products must implement Device Certificate signing procedures.

3.6 **Data Stores.** Licensed Products must implement support for WMDRM Data Stores. If optional features are implemented, the corresponding Data Stores must be supported.

3.7 **License Acquisition.** Licensed Products must support one or both of the following methods of License Acquisition.

3.7.1 **Indirect License Acquisition.** Licensed Products that implement receiving WMDRM Licenses from an ILA Transmitter must support all mandatory features and supported optional features via the MTP protocol as specified in the WMDRM-PD MTP Extensions Technical Documentation or RAPI protocol.

3.7.2 **Direct License Acquisition.** Licensed Products that support acquiring WMDRM Licenses from WMDRM Servers must implement Direct License Acquisition functionality.

3.8 **License Evaluation.** Licensed Products must implement License Evaluation.

3.9 **Cryptographic Keys**

3.9.1 **Device Key.** A Cryptographically Random Device Key must be generated by the Company for each Licensed Product. The Device Key must be unique for each Licensed Product manufactured by Company.

3.9.2 **Device Certificate Signing Keys.** A Cryptographically Random Device Certificate Signing Public and Private Key must be generated by the Company for Licensed Products. The Device Certificate Signing Public and Private Key must be unique for each Licensed Product with different functionality, for example for two different model numbers or revisions.

3.9.3 **Privacy Public Key.** All DLA transmissions must be encrypted with the Privacy Public Key.

3.9.4 **Fallback Keys.** If a Licensed Product supports the optional feature DLA, the Licensed Product may store Fallback Keys.

3.10 **Real Time Clock.** Licensed Products that support use of WMDRM Licenses including expiration, as described in Section 4.3, must implement a Real Time Clock. The Real Time Clock must be capable of maintaining time accurately with a clock drift no more than two minutes per month and a minimum resolution of one second. Licensed Products may implement either an Anti-Rollback Clock or Secure Clock as described below.

3.10.1 **Anti-Rollback Clock.** Anti-Rollback Clock, if supported, must be implemented as follows.

3.10.1.1 **Clock Reset.** When power is lost to the Licensed Product, the clock must be automatically reset in such a way that the reset date and time after reset precedes by one year the day on which the device was manufactured. Before playing WMDRM Content, the Licensed Product must set the initial date and time to no later than 1/1/2000 at 12:00:00 AM and require the user to set a date and time subsequent to the last date and time recorded by WMDRM to be valid.

3.10.1.2 **Clock Rollback.** When a Licensed Product detects a Clock Rollback Event, it must iterate through all WMDRM Licenses stored in the WMDRM License Store and take the appropriate actions as specified in Section 4.3.5 and 4.3.6 respectively.

3.10.2 **Secure Clock.** Secure Clock, if supported, must be implemented as follows.

3.10.2.1 **Authorized Service.** Licensed Products must connect only to a Secure Clock Service.

3.10.2.2 **Clock Reset.** When power is lost to a Licensed Product, the clock must be reset such that when power is regained, the Licensed Product must detect the loss of power and set the state of the Secure Clock to an unset or unsecured state.

3.10.2.3 **Grace Period.** Licensed Products must implement support for Grace Period.

4. REQUIREMENTS FOR COMPLYING WITH WMDRM POLICY

The following Compliance Rules are applicable to the WMDRM Policy as specified in the WMDRM License.

4.1 **Security Level.** A Licensed Product must decrypt WMDRM Content using only WMDRM Licenses that have a Security Level less than or equal to the Security Level for such Licensed Product.

4.2 **Unspecified Policy.** WMDRM Policy may specify additional rights, restrictions or parameters that are not covered in these Compliance Rules. Nevertheless Licensed Products must only take action based on rights and enforce restrictions covered in this document and Consistent with the Microsoft Implementation. To the extent that WMDRM Policy (or a particular WMDRM License) describes additional rights, restrictions or parameters that are not described in these Compliance Rules, Licensed Products must ignore such additional rights, restrictions or parameters.

4.3 **Expiration.** Licensed Devices that support a Clock must implement expiration support as follows:

4.3.1 **Begin Date.** If specified in the WMDRM License, Licensed Products must not allow the associated WMDRM Content to be ~~passed~~Passed before the specified date and time.

4.3.2 **End Date.** If specified in the WMDRM License, Licensed Products must not allow the associated WMDRM Content to be ~~passed~~Passed after the specified date and time.

4.3.3 **ExpirationAfterFirstUse.** If specified in the WMDRM License, upon first use of the associated WMDRM Content, the specified number of hours must be added to the current date and time and the sum stored in the Secure Store. This sum must then be evaluated as specified in Section 4.3.2.

4.3.4 **ExpirationOnStore.** If specified in the WMDRM License, upon storing the WMDRM License the specified number of hours must be added to the current date and time and the sum stored in the Secure Store. This sum must then be evaluated as specified in Section 4.3.2.

4.3.5 **DisableOnClockRollback.** If a Licensed Product implements Anti-Rollback Clock and detects and processes a Clock Rollback Event, the Licensed Product must make inaccessible any WMDRM License specifying DisableOnClockRollback. When a Licensed Product detects that the current date and time exceeds the last known good date and time, it must re-enable access to any WMDRM License that specifies DisableOnClockRollback.

4.3.6 **DeleteOnClockRollback.** If a Licensed Product implements Anti-Rollback Clock and detects and processes a Clock Rollback Event, WMDRM must delete any WMDRM License that specifies DeleteOnClockRollback.

4.4 **Metering.** Metering, if supported, must be implemented as follows:

4.4.1 **Implementation.** Each time a WMDRM License that includes a Metering ID is used to decrypt and ~~pass~~Pass WMDRM Content, the Licensed Products must update the WMDRM Metering Store.

4.4.2 **Metering Update.** When accessing WMDRM Content with an associated WMDRM License that requires Metering, the Metering Store must be updated when the associated WMDRM Content is first decrypted and ~~passed~~Passed. For Licensed Products first introduced prior to June 30, 2005, the update to the Metering Store may be postponed, provided that reasonable steps are taken to update the Metering Store before the next time the Licensed Product communicates with an ILA Transmitter or Network.

4.4.3 **Insufficient Storage.** If a Licensed Product does not have Persistent Storage available to persist updates to Metering, it must not decrypt and ~~pass~~Pass WMDRM Content using any WMDRM License specifying a Metering ID.

4.4.4 Delayed Updates. If a Licensed Product caches WMDRM Content including only Audio Content in Temporary Storage and Persistent Storage is currently unavailable, caching Metering updates is permitted until Persistent Storage thereafter becomes available to record Metering updates, provided that the Licensed Product (i) confirms prior to decrypting WMDRM Content that sufficient Persistent Storage will be available to record Metering updates and (ii) records any Metering updates cached in temporary storage after ~~passing~~Passing no more than thirty (30) minutes of WMDRM Content or ten (10) WMDRM Content files, whichever occurs first. Licensed Products first introduced after June 30, 2005 must not delay updates but must record updates directly in Persistent Storage.

4.5 Play Count. A Play count, if present in the WMDRM License, specifies the number of times that the WMDRM License may be used to decrypt and ~~pass~~Pass WMDRM Content. Licensed Products must implement Play count as follows:

4.5.1 Implementation. If Play count is specified in the WMDRM License, Licensed Products must limit the number of Plays to the specified maximum number. A Play count is decremented when WMDRM Content is first decrypted and ~~passed~~Passed.

4.5.2 Insufficient Storage. If a Licensed Product does not have available Persistent Storage to record Play count, it must not decrypt WMDRM Content using any WMDRM License that specifies a Play count.

4.5.3 Delayed Updates. If a Licensed Product caches WMDRM Content including only Audio Content in Temporary Storage and Persistent Storage is currently unavailable, caching Play count updates is permitted until Persistent Storage is available to record Play count updates, provided that the Licensed Product (i) confirms, prior to decrypting additional WMDRM Content, that sufficient Persistent Storage will be available to record Play count updates and Play counts remaining for WMDRM Content, and (ii) records any Play count updates cached in Temporary Storage after ~~passing~~Passing no more than thirty (30) minutes of WMDRM Content or ten (10) WMDRM content files, whichever occurs first. Licensed Products first introduced after June 30, 2005 must not delay updates but must record updates directly in Persistent Storage.

EXHIBIT 6

COMPLIANCE RULES FOR WMDRM FOR PORTABLE DEVICES APPLICATIONS

1. DEFINITIONS

The following terms have the meanings set forth below. Other initially capitalized terms not defined in these Compliance Rules have the meanings ascribed to them in the License Agreement or the Microsoft Implementation.

- 1.1 “Analog Audio Outputs” means a connector for an analog sound reproduction device such as a speaker or headphones. For avoidance of doubt, this includes both external jacks to connect speakers and/or headphones and built-in speakers and/or headphones.
- 1.2 “Analog Computer Monitor Output” means a connector for an analog monitor typically found and associated with a Computer Product and that carries uncompressed analog video signals. The term expressly includes those outputs known as VGA, SVGA, XGA, DVI Analog, and various non-standardized analog monitor connections which have been implemented by manufacturers, and expressly does not include such typical consumer electronics connectors as NTSC, PAL, SECAM, SCART, YPrPb, S-Video and Consumer RGB, whether or not such connectors are found on any Computer Product.
- 1.3 “Analog Protection System (APS) trigger bits (APSTB)” means the bits as specified (a) for NTSC video signals, in IEC 61880 (for inclusion of such value on Line 20) or EIA-608-B (for inclusion of such value on Line 21) or (b) for YUV (525/60 systems) signals, in IEC 61880 (for inclusion of such value on Line 20) or EIA-608-B (for inclusion of such value on Line 21).
- 1.4 “Analog Television Output” means such typical consumer electronics analog connectors as NTSC, PAL, SECAM, SCART, YPrPb, S-Video and Consumer RGB.
- 1.5 “Analog Video Content” means audiovisual works, as defined in 17 U.S.C. § 101, recorded in an analog format.
- 1.6 “Audio Outputs” means Analog Audio Outputs, Digital Audio Outputs and USB Audio Outputs.
- 1.7 “Automatic Gain Control (AGC)” means the so-named copy control system as specified (a) for NTSC, PAL, SECAM or YUV analog video signals, in the document entitled “Specification of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999,” and (b) for a 480p progressive scan analog video signal, in the

document entitled “Specification of the Macrovision AGC Copy Protection Waveforms for DVD Applications with 525p (480p) Progressive Scan Outputs, Revision 1.03 (December 22, 1999).”

- 1.8 “CGMS-A” means the Copy Generation Management System (Analog) as specified (a) for NTSC analog video signals, in IEC 61880 (for inclusion on Line 20) or in EIA-608-B (for inclusion on Line 21), (b) for PAL, SECAM or YUV analog video signals, in IEC 61880 (for inclusion on Line 20) or in EIA-608-B (for inclusion on Line 21) or in EIA-805 (for inclusion on Line 41) for YUV (525/60 systems) signals or in ETS 300924 for PAL, SECAM and YUV (625/50 systems) signals, or (c) for 480p progressive scan analog video signals, in, or adapted without material change from, EIAJ CPR1204-1 (defining the signal waveform carrying the CGMS-A) and IEC 61880 (defining the bit assignment for CGMS-A).
- 1.9 “Certificate” means a unique WMDRM object used to assess trust.
- 1.10 “Colorstripe” means the so-named copy control system as specified for NTSC analog video signals in the document entitled “Specification of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999.”
- 1.11 “Company” means an entity licensed under a License Agreement to develop Licensed Products.
- 1.12 “Computer Product” means a device that is designed or permits the end user to install software applications thereon, including, but not limited to, personal computers, handheld “Personal Digital Assistants,” and the like.
- 1.13 “Consistent with the Microsoft Implementation” means the Licensed Product (i) provides equivalent functionality to the Microsoft Implementation, (ii) equals or exceeds the security of the Microsoft Implementation, and (iii) maintains compatibility and interoperability with the Microsoft Implementation.
- 1.14 “Content” means audio and/or video that are transmitted or distributed, either by broadcast, cablecast, or other means of distribution to the general public or on demand.
- 1.15 “Content Key” means a symmetric key used to decrypt WMDRM Content.
- 1.16 “Copy” means to transport encrypted WMDRM Content over a USB connection, to the extent permitted by applicable WMDRM Policy, to a Licensed Product for Passing to Outputs at any time and/or for as many times as permitted by applicable WMDRM Policy.

- 1.17 “Cryptographically Random” means unpredictable, in that no polynomial-time algorithm, given any sequence of bits, can guess the succeeding K bits with probability greater than $\frac{1}{2}^K + 1/P(K)$ for any (positive) polynomial P and sufficiently large K.
- 1.18 “Device Authorization Certificate” means a digital certificate, used for example to verify whether a Device Certificate Template is authentic.
- 1.19 “Device Certificate Signing Keys” means an associated pair of Cryptographically Random asymmetric keys generated by Company for each of its Licensed Products, consisting of a “Device Certificate Signing Public Key” and a “Device Certificate Signing Private Key”.
- 1.20 “Device Certificate Signing Private Key” means the private portion of the Device Certificate Signing Keys.
- 1.21 “Device Certificate Signing Public Key” means the public portion of the Device Certificate Signing Keys.
- 1.22 “Device Certificate Template” means a digital certificate, unique to each Licensed Product, used for example to create a Device Certificate for use with WMDRM-PD.
- 1.23 “Device Certificate” means a Certificate issued by Company or contract manufacturer on Company’s behalf, assigned to each Licensed Product and used, for example, to evaluate whether the Licensed Product is trusted and eligible to receive WMDRM Content.
- 1.24 “Digital Audio Content” means sound recordings, as defined in 17 U.S.C. § 101, recorded in a digital format.
- 1.25 “Digital Audio Output” means digital audio signals conforming to IEC-958, IEC-60958, or IEC-61937.
- 1.26 “Digital Video Content” means audiovisual works, as defined in 17 U.S.C. § 101, recorded in a digital format.
- 1.27 “Digital Video Output” means the digital interface portion only of Digital Visual Interface (DVI), a digital interface standard created by the Digital Display Working Group (DDWG), and the DVI digital interface portion of the High-Definition Multimedia Interface (HDMI).
- 1.28 “Direct License Acquisition” or “DLA” means the process of acquiring a WMDRM License directly from a WMDRM Server.

- 1.29 “Fallback Keys” means an associated pair of keys generated by Microsoft for Licensed Products for the purpose of Direct License Acquisition from WMDRM Servers.
- 1.30 “HDCP” means High-Bandwidth Digital Content Protection (“HDCP”) protected Output. The HDCP specification and license agreement are available from Digital Content Protection, LLC at <http://www.digital-cp.com/>.
- 1.31 “Internal Video Output” means any display that is permanently connected to the Licensed Product, including, but not limited to, a liquid crystal display (“LCD”).
- 1.32 “License Agreement” means the agreement under which Microsoft licenses entities to develop and distribute products that include implementations of WMDRM-PD.
- 1.33 “Licensed Product” means a hardware device or software application (or other software component, which may be a separately identifiable subset of a software application or operating system), that (i) implements WMDRM-PD subject to a license from Microsoft and (ii) is capable of playing back WMDRM Content.
- 1.34 “Media Transfer Protocol” or “MTP” means Microsoft’s Media Transfer Protocol for device control, metadata exchange and media transfer which is only supported over USB 1.0 or later.
- 1.35 “Metering” is a feature of WMDRM-PD designed to securely collect and report content usage information.
- 1.36 “Microsoft Implementation” means the implementation of WMDRM-PD functionality provided as source code, binaries, technical documentation, tools and/or sample files as provided to the Company under the License Agreement.
- 1.37 “Output” means Analog Audio Outputs, Analog Computer Monitor Outputs, Analog Television Outputs, Digital Audio Outputs, Digital Video Outputs, Internal Video Outputs and USB Audio Outputs. Output does not include Copying WMDRM Content to a Licensed Product over a USB connection.
- 1.38 “Output Protection Level” means a number included in WMDRM Policy that corresponds to the content protection that must be applied when Passing WMDRM Content. The Output Protection Level may be determined and assigned by the content owner or may be assigned by the WMDRM Implementation for specific categories of WMDRM Content.

- 1.39 “Pass” means to direct decrypted WMDRM Content to flow to Outputs, optionally (though not necessarily) through intermediate components such as a codec or device driver.
- 1.40 “Play” means the first decrypt of WMDRM Content.
- 1.41 “Privacy Key” means an asymmetric public key provided by Microsoft for the purpose of encrypting sensitive communication sent over a public network.
- 1.42 “Secure Audio Device Drivers” means audio device drivers that either (1) are not capable of being replaced by an end user or (2) are verified not to have been modified, are trusted not to expose decrypted WMDRM Content, and ensure that only the secure driver is capable of receiving the WMDRM Content through encryption or other means. For avoidance of doubt, a Licensed Product that prevents end users from upgrading the audio device drivers is considered to have Secure Audio Device Drivers.
- 1.43 “Secure Codecs” means audio and/or video codecs that either (1) are not capable of being replaced by an end user or (2) are verified not to have been modified, are trusted not to expose decrypted WMDRM Content, and prevent intermediate software from accessing WMDRM Content. For avoidance of doubt, a Licensed Product that prevents end users from replacing the codecs is considered to have Secure Codecs.
- 1.44 “Secure Video Device Drivers” means video device drivers that either (1) are not capable of being replaced by an end user or (2) are trusted not to expose decrypted WMDRM Content and provide a secure mechanism for signaling required content protection on Digital Video Outputs. For avoidance of doubt, a Licensed Product that prevents end users from upgrading the video device drivers is considered to have Secure Video Device Drivers.
- 1.45 “Stream” means to transport encrypted WMDRM Content over a network, to the extent permitted by applicable WMDRM Policy, to a WMDRM-ND Receiver for Passing to an Output immediately or shortly after receipt of the WMDRM Content in the WMDRM-ND Receiver.
- 1.46 “Unrestricted Audio Outputs” means Analog Audio Outputs and USB Audio Outputs.
- 1.47 “USB Audio Output” means a speaker, headphones or other sound reproduction device attached that complies with the Universal Serial Bus (USB) Audio Specification available from the USB Forum.

- 1.48 “Video Outputs” means Analog Television Outputs, Digital Video Outputs and Internal Video Outputs.
- 1.49 “WMDRM Content” means audio or audiovisual content that has been encrypted and recorded using WMDRM.
- 1.50 “WMDRM License” means a data structure that contains, but is not limited to, WMDRM Policy and an encrypted Content Key associated with specific WMDRM Content.
- 1.51 “WMDRM Policy” means the description of the actions permitted and/or required for or with WMDRM Content and restrictions on those actions as described in the WMDRM License associated with the WMDRM Content.
- 1.52 “WMDRM Server” means a Licensed Product capable of issuing WMDRM Licenses over a network connection.
- 1.53 “WMDRM” means Windows Media Digital Rights Management technology.
- 1.54 “WMDRM-PD” means WMDRM for Portable Devices.

2. SCOPE. These Compliance Rules apply to Licensed Products implementing WMDRM-PD functionality, including without limitation Portable Media Devices, Wireless Handsets and Portable Digital Assistants. These Compliance Rules set forth the requirements pursuant to which Licensed Products may play back and Output WMDRM Content.

3. REQUIREMENTS FOR WMDRM-PD APPLICATIONS

3.1 **Serial Number.** Company shall assign a unique serial number with a minimum length of 128 bits to each Licensed Product manufactured by Company.

3.2 **Device Certificate Template.** Licensed Products must implement a Device Certificate Template that includes accurate metadata. Each Device Certificate Template must include the following information: manufacturer name, model number and hardware revision, and may include the major firmware revision. Each Device Certificate Template must be signed with the Device Authorization Certificate private key provided by Microsoft.

3.3 **Device Authorization Certificate.** Company shall use a unique Device Authorization Certificate for each Licensed Product manufactured by the Company and employing a hardware and/or software configuration that differs materially from the Company’s other Licensed Products.

4. REQUIREMENTS FOR COMPLYING WITH WMDRM POLICY

The following Compliance Rule is applicable to WMDRM Policy specified in the WMDRM License:

4.1 **Unspecified policy.** WMDRM Policy may specify additional rights, restrictions or parameters that are not covered in these Compliance Rules. Nevertheless Licensed Products must only take action based on rights and enforce restrictions covered in these Compliance Rules. To the extent that WMDRM Policy (or a particular WMDRM License) describes additional rights, restrictions or parameters that are not described in these Compliance Rules, Licensed Products must ignore such additional rights, restrictions or parameters.

5. PLAYBACK AND OUTPUT CONTROL RULES FOR LICENSED PRODUCTS

Licensed Products must comply with the following:

5.1 **Playback Control.** Licensed Products must comply with the following rules for playback control:

5.1.1 **Playback.** Licensed Products may Pass decrypted WMDRM Content through the Outputs described in Sections 5.2 and 5.3 only if the right to Play is included in a WMDRM License associated with such WMDRM Content.

5.2 **Restricted Outputs.** Licensed Products must detect and accurately respond to the Output Protection Levels for WMDRM Content.

5.2.1 **Output Control for Digital Compressed Audio Content.** If a Licensed Product Passes compressed Digital Audio Content, the Licensed Product must follow restrictions as specified in the WMDRM License and this Section 5.2.1. Licensed Products may Pass compressed Digital Audio Content to Secure Codecs provided the decompressed Digital Audio Content is handled consistent with Section 5.2.2.

5.2.1.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may Pass without restriction compressed Digital Audio Content of decrypted WMDRM Content to Audio Outputs.

5.2.1.2 **Level 101 to 200.** If the Output Protection Level specified in the WMDRM License is greater than 100 and less than or equal to 200, Licensed Products may Pass, without restriction, the compressed Digital Audio Content of decrypted WMDRM Content via Secure Audio Device Drivers to Audio Outputs.

5.2.1.3 **Level 201 to 300.** If the Output Protection Level specified in the WMDRM License is greater than 200 and less than or equal to 300,

Licensed Products may Pass compressed Digital Audio Content of decrypted WMDRM Content via Secure Audio Device Drivers to Unrestricted Audio Outputs.

5.2.1.4 **Level 301 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not Pass compressed Digital Audio Content of decrypted WMDRM Content.

5.2.2 **Output Control for Digital Uncompressed Audio Content.** If a Licensed Product Passes uncompressed Digital Audio Content, the Licensed Products must follow restrictions as specified in the WMDRM License and this Section 5.2.2.

5.2.2.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may Pass without restriction digital uncompressed Digital Audio Content of decrypted WMDRM Content to Audio Outputs.

5.2.2.2 **Level 101 to 200.** If the Output Protection Level specified in the WMDRM License is greater than 100 and less than or equal to 200, Licensed Products may Pass, without restriction, the uncompressed Digital Audio Content of decrypted WMDRM Content via Secure Audio Device Drivers to Audio Outputs.

5.2.2.3 **Level 201 to 300.** If the Output Protection Level specified in the WMDRM License is greater than 200 and less than or equal to 300, Licensed Products may Pass uncompressed Digital Audio Content of decrypted WMDRM Content via Secure Audio Device Drivers to Unrestricted Audio Outputs.

5.2.2.4 **Level 301 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not Pass uncompressed Digital Audio Content of decrypted WMDRM Content.

5.2.3 **Output Control for Digital Compressed Video Content.** Licensed Products must not Pass decrypted compressed Digital Video Content to any Output, except that a Licensed Product may Pass Content marked with the ATSC Standard A/65B Redistribution Control descriptor (rc_descriptor()) to any Output protected by a digital content protection technology approved by the Federal Communications Commission (or otherwise approved in accordance with applicable Federal Communications Commission rules) for use with such Content. Licensed Products may Pass compressed Digital Video Content to Secure Codecs provided that the decompressed Digital Video Content is handled consistent with Section 5.2.4.

5.2.4 **Output Control for Digital Uncompressed Video Content.** If a Licensed Product Passes uncompressed Digital Video Content, the Licensed Product must follow restrictions as specified in the WMDRM License and this Section 5.2.4.

5.2.4.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may Pass, without restriction, the uncompressed Digital Video Content of decrypted WMDRM Content on Video Outputs.

5.2.4.2 **Level 101 to 300.** If the Output Protection Level specified in the WMDRM License is greater than 100 and less than or equal to 300 and Licensed Product is Passing Digital Video Content to Digital Video Outputs, the Licensed Product must engage HDCP to protect the uncompressed Digital Video Content of decrypted WMDRM Content. Licensed Products must verify that the HDCP Source Function is engaged and able to deliver protected content, which means HDCP encryption is operational on such Output.

5.2.4.3 **Level 301 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not Pass uncompressed Digital Video Content of decrypted WMDRM Content on Digital Video Outputs.

5.2.5 **Output Control for Analog Video Content.** If a Licensed Product Passes the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs, the Licensed Product must follow restrictions as specified in the WMDRM License and this Section 5.2.5. Additional restrictions may be required as specified in Section 5.2.6.

5.2.5.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may Pass without restriction the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs.

5.2.5.2 **Level 101 to 200.** If the Output Protection Level specified in the WMDRM Licenses is greater than 100 but less than or equal to 200 and the Licensed Product is Passing the Analog Video Content of decrypted WMDRM Content to the Analog Television Outputs, the Licensed Product must engage CGMS-A with the CGMS field in the copy set to '11' ("no more copies").

5.2.5.3 **Level 201 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 200, Licensed Products must not Pass the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs.

5.2.6 **Output Control for Extended Analog Video Content.** If a Licensed Product Passes the video portion of Decrypted WMDRM Content to Analog Television Outputs, the Licensed Product must follow restrictions as specified in the WMDRM License and this Section 5.2.6. Additional restrictions may be required as specified in Section 5.2.5.

5.2.6.1 Automatic Gain Control and ColorStripe. If Extended Analog Video Protection List in the WMDRM License includes “C3FD11C6-F8B7-4d20-B008-1DB17D61F2DA”, Licensed Products must engage Automatic Gain Control and ColorStripe and set the APSTB field as based on the Extended Analog Video Protection Configuration Data included in the WMDRM License. Additional technologies and restrictions may be required as specified in Section 5.2.5. For avoidance of doubt, the permitted APSTB values in the WMDRM License are as follows:

APSTB values	Description	NTSC	PAL
00	AGC and ColorStripe	Off	Off
01	AGC Only	APS1	APS1
10	AGC and 2 line ColorStripe	APS2	APS1
11	AGC and 4 line ColorStripe	APS3	APS1

5.3 Unrestricted Outputs. Unless otherwise specified in Section 5.2, Licensed Products may Pass without restriction WMDRM Content to the following Outputs provided the requirements in Section 5.1.1 are met.

5.3.1 Analog Audio Outputs. Licensed Products may Pass without restriction the Analog Audio Content of decrypted WMDRM Content to Analog Audio Outputs.

5.3.2 USB Audio Outputs. Licensed Products may Pass without restriction the uncompressed Digital Audio Content of decrypted WMDRM Content to USB Audio Outputs.

5.3.3 Analog Computer Monitor Outputs. Licensed Products may Pass without restriction the uncompressed Analog Video Content of decrypted WMDRM Content to Analog Computer Monitor Outputs.

5.3.4 Internal Video Outputs. Licensed Products may Pass without restriction the uncompressed Digital Video Content of decrypted WMDRM Content to Internal Video Outputs.

COMPLIANCE RULES FOR WMDRM FOR PORTABLE DEVICES APPLICATIONS

1. DEFINITIONS

The following terms have the meanings set forth below. Other initially capitalized terms not defined in these Compliance Rules have the meanings ascribed to them in the License Agreement or the Microsoft Implementation.

- 1.1 “Analog Audio Outputs” means a connector for an analog sound reproduction device such as a speaker or headphones. For avoidance of doubt, this includes both external jacks to connect speakers and/or headphones and built-in speakers and/or headphones.
- 1.2 “Analog Computer Monitor Output” means a connector for an analog monitor typically found and associated with a Computer Product and that carries uncompressed analog video signals. The term expressly includes those outputs known as VGA, SVGA, XGA, DVI Analog, and various non-standardized analog monitor connections which have been implemented by manufacturers, and expressly does not include such typical consumer electronics connectors as NTSC, PAL, SECAM, SCART, YPrPb, S-Video and Consumer RGB, whether or not such connectors are found on any Computer Product.
- 1.3 “Analog Protection System (APS) trigger bits (APSTB)” means the bits as specified (a) for NTSC video signals, in IEC 61880 (for inclusion of such value on Line 20) or EIA-608-B (for inclusion of such value on Line 21) or (b) for YUV (525/60 systems) signals, in IEC 61880 (for inclusion of such value on Line 20) or EIA-608-B (for inclusion of such value on Line 21).
- 1.4 “Analog Television Output” means such typical consumer electronics analog connectors as NTSC, PAL, SECAM, SCART, YPrPb, S-Video and Consumer RGB.
- 1.5 “Analog Video Content” means audiovisual works, as defined in 17 U.S.C. § 101, recorded in an analog format.
- ~~1.6 “Approved Outputs” means Analog Audio Outputs, Analog Computer Monitor Outputs, Analog Television Outputs, Digital Audio Outputs, Digital Video Outputs, Internal Video Outputs and USB Audio Outputs.~~
- 1.6 ~~1.7~~ “Audio Outputs” means Analog Audio Outputs, Digital Audio Outputs and USB Audio Outputs.

- 1.7** ~~**1.8**~~ “Automatic Gain Control (AGC)” means the so-named copy control system as specified (a) for NTSC, PAL, SECAM or YUV analog video signals, in the document entitled “Specification of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999,” and (b) for a 480p progressive scan analog video signal, in the document entitled “Specification of the Macrovision AGC Copy Protection Waveforms for DVD Applications with 525p (480p) Progressive Scan Outputs, Revision 1.03 (December 22, 1999).”
- ~~**1.9**~~ “Certificate” means a unique WMDRM object used to assess trust.
- 1.8** ~~**1.10**~~ “CGMS-A” means the Copy Generation Management System (Analog) as specified (a) for NTSC analog video signals, in IEC 61880 (for inclusion on Line 20) or in EIA-608-B (for inclusion on Line 21), (b) for PAL, SECAM or YUV analog video signals, in IEC 61880 (for inclusion on Line 20) or in EIA-608-B (for inclusion on Line 21) or in EIA-805 (for inclusion on Line 41) for YUV (525/60 systems) signals or in ETS 300924 for PAL, SECAM and YUV (625/50 systems) signals, or (c) for 480p progressive scan analog video signals, in, or adapted without material change from, EIAJ CPR1204-1 (defining the signal waveform carrying the CGMS-A) and IEC 61880 (defining the bit assignment for CGMS-A).
- 1.9** “Certificate” means a unique WMDRM object used to assess trust.
- 1.10** ~~**1.11**~~ “Colorstripe” means the so-named copy control system as specified for NTSC analog video signals in the document entitled “Specification of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999.”
- 1.11** ~~**1.12**~~ “Company” means an entity licensed under a License Agreement to develop Licensed Products.
- 1.12** ~~**1.13**~~ “Computer Product” means a device that is designed or permits the end user to install software applications thereon, including, but not limited to, personal computers, handheld “Personal Digital Assistants,” and the like.
- 1.13** ~~**1.14**~~ “Consistent with the Microsoft Implementation” means the Licensed Product (i) provides equivalent functionality to the Microsoft Implementation, (ii) equals or exceeds the security of the Microsoft Implementation, and (iii) maintains compatibility and interoperability with the Microsoft Implementation.
- ~~**1.15**~~ “Content Key” means a symmetric key used to decrypt WMDRM Content.

- 1.14 ~~1.16~~ “Content” means audio and/or video that are transmitted or distributed, either by broadcast, cablecast, or other means of distribution to the general public or on demand.
- 1.15 “Content Key” means a symmetric key used to decrypt WMDRM Content.
- 1.16 “Copy” means to transport encrypted WMDRM Content over a USB connection, to the extent permitted by applicable WMDRM Policy, to a Licensed Product for Passing to Outputs at any time and/or for as many times as permitted by applicable WMDRM Policy.
- 1.17 “Cryptographically Random” means unpredictable, in that, ~~at no polynomial-time algorithm, given~~ any ~~point regardless of how many preceding sequence of~~ bits ~~are available~~, can guess the ~~probability of predicting the next~~ succeeding K bits is with probability greater than $\frac{1}{2^{K+1}}$ for any (positive) polynomial P and sufficiently large K.
- 1.18 “Device Authorization Certificate” means a digital certificate, used for example to verify whether a Device Certificate Template is authentic.
- 1.19 “Device Certificate Signing Keys” means an associated pair of Cryptographically Random asymmetric keys generated by Company for each of its Licensed Products, consisting of a “Device Certificate Signing Public Key” and a “Device Certificate Signing Private Key”.
- 1.20 “Device Certificate Signing Private Key” means the private portion of the Device Certificate Signing Keys.
- 1.21 “Device Certificate Signing Public Key” means the public portion of the Device Certificate Signing Keys.
- 1.22 “Device Certificate Template” means a digital certificate, unique to each Licensed Product, used for example to create a Device Certificate for use with WMDRM-PD.
- 1.23 “Device Certificate” means a Certificate issued by Company or contract manufacturer on Company’s behalf, assigned to each Licensed Product and used, for example, to evaluate whether the Licensed Product is trusted and eligible to receive WMDRM Content.
- 1.24 “Digital Audio Content” means sound recordings, as defined in 17 U.S.C. § 101, recorded in a digital format.
- 1.25 “Digital Audio Output” means digital audio signals conforming to IEC-958, IEC-60958, or IEC-61937.

- 1.26 “Digital Video Content” means audiovisual works, as defined in 17 U.S.C. § 101, recorded in a digital format.
- 1.27 “Digital Video Output” means the digital interface portion only of Digital Visual Interface (DVI), a digital interface standard created by the Digital Display Working Group (DDWG), and the DVI digital interface portion of the High-Definition Multimedia Interface (HDMI).
- 1.28 “Direct License Acquisition” or “DLA” means the process of acquiring a WMDRM License directly from a WMDRM Server.
- 1.29 “Fallback Keys” means an associated pair of keys generated by Microsoft for Licensed Products for the purpose of Direct License Acquisition from WMDRM Servers.
- 1.30 “HDCP” means High-Bandwidth Digital Content Protection (“HDCP”) protected ~~output~~Output. The HDCP specification and license agreement are available from Digital Content Protection, LLC at <http://www.digital-cp.com/>.
- 1.31 “Internal Video Output” means any display that is permanently connected to the Licensed Product, including, but not limited to, a liquid crystal display (“LCD”).
- 1.32 “License Agreement” means the agreement under which Microsoft licenses entities to develop and distribute products that include implementations of WMDRM-PD.
- 1.33 “Licensed Product” means a hardware device or software application (or other software component, which may be a separately identifiable subset of a software application or operating system), that (i) implements WMDRM-PD subject to a license from Microsoft and (ii) is capable of playing back WMDRM Content.
- 1.34 “Media Transfer Protocol” or “MTP” means Microsoft’s Media Transfer Protocol for device control, metadata exchange and media transfer which is only supported over USB 1.0 or later.
- 1.35 “Metering” is a feature of WMDRM-PD designed to securely collect and report content usage information.
- 1.36 “Microsoft Implementation” means the implementation of WMDRM-PD functionality provided as source code, binaries, technical documentation, tools and/or sample files as provided to the Company under the License Agreement.

- 1.37 “Output” means Analog Audio Outputs, Analog Computer Monitor Outputs, Analog Television Outputs, Digital Audio Outputs, Digital Video Outputs, Internal Video Outputs and USB Audio Outputs. Output does not include Copying WMDRM Content to a Licensed Product over a USB connection.
- 1.38 “Output Protection Level” means a number included in WMDRM Policy that corresponds to the content protection that must be applied when ~~passing~~Passing WMDRM Content. The Output Protection Level may be determined and assigned by the content owner or may be assigned by the WMDRM Implementation for specific categories of WMDRM Content.
- 1.39 “Pass” means to direct decrypted WMDRM Content to flow to Outputs, optionally (though not necessarily) through intermediate components such as a codec or device driver.
- 1.40 ~~1.38~~ “Play” means the first decrypt of WMDRM Content.
- 1.41 ~~1.39~~ “Privacy Key” means an asymmetric public key provided by Microsoft for the purpose of encrypting sensitive communication sent over a public network.
- 1.42 ~~1.40~~ “Secure Audio Device Drivers” means audio device drivers that either (1) are not capable of being replaced by an end user or (2) are verified not to have been modified, are trusted not to expose decrypted WMDRM Content, and ensure that only the secure driver is capable of receiving the WMDRM Content through encryption or other means. For avoidance of doubt, a Licensed Product that prevents end users from upgrading the audio device drivers is considered to have Secure Audio Device Drivers.
- 1.43 ~~1.41~~ “Secure Codecs” means audio and/or video codecs that either (1) are not capable of being replaced by an end user or (2) are verified not to have been modified, are trusted not to expose decrypted WMDRM Content, and prevent intermediate software from accessing WMDRM Content. For avoidance of doubt, a Licensed Product that prevents end users from replacing the codecs is considered to have Secure Codecs.
- 1.44 ~~1.42~~ “Secure Video Device Drivers” means video device drivers that either (1) are not capable of being replaced by an end user or (2) are trusted not to expose decrypted WMDRM Content and provide a secure mechanism for signaling required content protection on ~~Approved~~Digital Video Outputs. For avoidance of doubt, a Licensed Product that prevents end users from upgrading the video device drivers is considered to have Secure Video Device Drivers.

- 1.45 [“Stream” means to transport encrypted WMDRM Content over a network, to the extent permitted by applicable WMDRM Policy, to a WMDRM-ND Receiver for Passing to an Output immediately or shortly after receipt of the WMDRM Content in the WMDRM-ND Receiver.](#)
- 1.46 ~~1.43~~ [“Unrestricted Audio Outputs”](#) means Analog Audio Outputs and USB Audio Outputs.
- 1.47 ~~1.44~~ [“USB Audio Output”](#) means a speaker, headphones or other sound reproduction device attached that complies with the Universal Serial Bus (USB) Audio Specification available from the USB Forum.
- 1.48 ~~1.45~~ [“Video Outputs”](#) means Analog Television Outputs, Digital Video Outputs and Internal Video Outputs.
- 1.49 ~~1.46~~ [“WMDRM Content”](#) means audio or audiovisual content that has been encrypted and recorded using WMDRM.
- 1.50 ~~1.47~~ [“WMDRM License”](#) means a data structure that contains, but is not limited to, WMDRM Policy and an encrypted Content Key associated with specific WMDRM Content.
- 1.51 ~~1.48~~ [“WMDRM Policy”](#) means the description of the actions permitted and/or required for or with WMDRM Content and restrictions on those actions as described in the WMDRM License associated with the WMDRM Content.
- 1.52 ~~1.49~~ [“WMDRM Server”](#) means a Licensed Product capable of issuing WMDRM Licenses over a network connection.
- 1.53 ~~1.50~~ [“WMDRM”](#) means Windows Media Digital Rights Management technology.
- 1.54 ~~1.51~~ [“WMDRM-PD”](#) means WMDRM for Portable Devices.

2. SCOPE. These Compliance Rules apply to Licensed Products implementing WMDRM-PD functionality, including without limitation Portable Media Devices, Wireless Handsets and Portable Digital Assistants. These Compliance Rules set forth the requirements pursuant to which Licensed Products may play back and ~~output~~Output WMDRM Content.

3. REQUIREMENTS FOR WMDRM-PD APPLICATIONS

3.1 **Serial Number.** Company shall assign a unique serial number with a minimum length of 128 bits to each Licensed Product manufactured by Company.

3.2 **Device Certificate Template.** Licensed Products must implement a Device Certificate Template that includes accurate metadata. Each Device Certificate Template must include the following information: manufacturer name, model number and hardware revision, and may include the major firmware revision. Each Device Certificate Template must be signed with the Device Authorization Certificate private key provided by Microsoft.

3.3 **Device Authorization Certificate.** Company shall use a unique Device Authorization Certificate for each Licensed Product manufactured by the Company and employing a hardware and/or software configuration that differs materially from the Company's other Licensed Products.

4. REQUIREMENTS FOR COMPLYING WITH WMDRM POLICY

The following Compliance Rule is applicable to WMDRM Policy specified in the WMDRM License:

4.1 **Unspecified policy.** WMDRM Policy may specify additional rights, restrictions or parameters that are not covered in these Compliance Rules. Nevertheless Licensed Products must only take action based on rights and enforce restrictions covered in these Compliance Rules. To the extent that WMDRM Policy (or a particular WMDRM License) describes additional rights, restrictions or parameters that are not described in these Compliance Rules, Licensed Products must ignore such additional rights, restrictions or parameters.

5. PLAYBACK AND OUTPUT CONTROL RULES FOR LICENSED PRODUCTS

Licensed Products must comply with the following:

5.1 **Playback Control.** Licensed Products must comply with the following rules for playback control:

5.1.1 **Playback.** Licensed Products may ~~pass~~Pass decrypted WMDRM Content through the ~~outputs~~Outputs described in Sections 5.2 and 5.3 only if the right to Play is included in a WMDRM License associated with such WMDRM Content.

5.2 **Restricted Outputs.** Licensed Products must detect and accurately respond to the Output Protection Levels for WMDRM Content.

5.2.1 **Output Control for Digital Compressed Audio Content.** If a Licensed Product ~~passes~~Passes compressed Digital Audio Content, the Licensed Product must follow restrictions as specified in the WMDRM License and this Section 5.2.1.

Licensed Products may ~~pass~~Pass compressed Digital Audio Content to Secure Codecs provided the decompressed Digital Audio Content is handled consistent with Section 5.2.2.

5.2.1.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may ~~pass~~Pass without restriction compressed Digital Audio Content of decrypted WMDRM Content to Audio Outputs.

5.2.1.2 **Level 101 to 200.** If the Output Protection Level specified in the WMDRM License is greater than 100 and less than or equal to 200, Licensed Products may ~~pass~~Pass, without restriction, the compressed Digital Audio Content of decrypted WMDRM Content via Secure Audio Device Drivers to Audio Outputs.

5.2.1.3 **Level 201 to 300.** If the Output Protection Level specified in the WMDRM License is greater than 200 and less than or equal to 300, Licensed Products may ~~pass~~Pass compressed Digital Audio Content of decrypted WMDRM Content via Secure Audio Device Drivers to Unrestricted Audio Outputs.

5.2.1.4 **Level 301 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not ~~pass~~Pass compressed Digital Audio Content of decrypted WMDRM Content.

5.2.2 **Output Control for Digital Uncompressed Audio Content.** If a Licensed Product ~~passes~~Passes uncompressed Digital Audio Content, the Licensed Products must follow restrictions as specified in the WMDRM License and this Section 5.2.2.

5.2.2.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may ~~pass~~Pass without restriction digital uncompressed Digital Audio Content of decrypted WMDRM Content to Audio Outputs.

5.2.2.2 **Level 101 to 200.** If the Output Protection Level specified in the WMDRM License is greater than 100 and less than or equal to 200, Licensed Products may ~~pass~~Pass, without restriction, the uncompressed Digital Audio Content of decrypted WMDRM Content via Secure Audio Device Drivers to Audio Outputs.

5.2.2.3 **Level 201 to 300.** If the Output Protection Level specified in the WMDRM License is greater than 200 and less than or equal to 300, Licensed Products may ~~pass~~Pass uncompressed Digital Audio Content of decrypted WMDRM Content via Secure Audio Device Drivers to Unrestricted Audio Outputs.

5.2.2.4 **Level 301 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not ~~pass~~Pass uncompressed Digital Audio Content of decrypted WMDRM Content.

5.2.3 **Output Control for Digital Compressed Video Content.** Licensed Products must not ~~pass~~Pass decrypted compressed Digital Video Content to any ~~output~~. ~~Licensed Products may pass~~Output, except that a Licensed Product may Pass Content marked with the ATSC Standard A/65B Redistribution Control descriptor (rc descriptor()) to any Output protected by a digital content protection technology approved by the Federal Communications Commission (or otherwise approved in accordance with applicable Federal Communications Commission rules) for use with such Content. ~~Licensed Products may Pass~~ compressed Digital Video Content to Secure Codecs provided that the decompressed Digital Video Content is handled consistent with Section 5.2.4.

5.2.4 **Output Control for Digital Uncompressed Video Content.** If a Licensed Product ~~passes~~Passes uncompressed Digital Video Content, the Licensed Product must follow restrictions as specified in the WMDRM License and this Section 5.2.4.

5.2.4.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100, Licensed Products may ~~pass~~Pass, without restriction, the uncompressed Digital Video Content of decrypted WMDRM Content on Video Outputs.

5.2.4.2 **Level 101 to 300.** If the Output Protection Level specified in the WMDRM License is greater than 100 and less than or equal to 300 and Licensed Product is ~~passing~~Passing Digital Video Content to Digital Video Outputs, the Licensed Product must engage HDCP to protect the uncompressed Digital Video Content of decrypted WMDRM Content. Licensed Products must verify that the HDCP Source Function is engaged and able to deliver protected content, which means HDCP encryption is operational on such ~~output~~Output.

5.2.4.3 **Level 301 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 300, Licensed Products must not ~~pass~~Pass uncompressed Digital Video Content of decrypted WMDRM Content on Digital Video Outputs.

5.2.5 **Output Control for Analog Video Content.** If a Licensed Product ~~passes~~Passes the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs, the Licensed Product must follow restrictions as specified in the WMDRM License and this Section 5.2.5. Additional restrictions may be required as specified in Section 5.2.6.

5.2.5.1 **Level 0 to 100.** If the Output Protection Level is not specified or the level specified in the WMDRM License is less than or equal to 100,

Licensed Products may **pass**Pass without restriction the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs.

5.2.5.2 **Level 101 to 200.** If the Output Protection Level specified in the WMDRM Licenses is greater than 100 but less than or equal to 200 and the Licensed Product is **passing**Passing the Analog Video Content of decrypted WMDRM Content to the Analog Television Outputs, the Licensed Product must engage CGMS-A with the CGMS field in the copy set to '11' ("no more copies").

5.2.5.3 **Level 201 or greater.** If the Output Protection Level specified in the WMDRM License exceeds 200, Licensed Products must not **pass**Pass the Analog Video Content of decrypted WMDRM Content to Analog Television Outputs.

5.2.6 **Output Control for Extended Analog Video Content.** If a Licensed Product **passes**Passes the video portion of Decrypted WMDRM Content to Analog Television Outputs, the Licensed Product must follow restrictions as specified in the WMDRM License and this Section 5.2.6. Additional restrictions may be required as specified in Section 5.2.5.

5.2.6.1 **Automatic Gain Control and ColorStripe.** If Extended Analog Video Protection List in the WMDRM License includes "C3FD11C6-F8B7-4d20-B008-1DB17D61F2DA", Licensed Products must engage Automatic Gain Control and ColorStripe and set the APSTB field as based on the Extended Analog Video Protection Configuration Data included in the WMDRM License. Additional technologies and restrictions may be required as specified in Section 5.2.5. For avoidance of doubt, the permitted APSTB values in the WMDRM License are as follows:

APSTB values	Description	NTSC	PAL
00	AGC and ColorStripe is disabled	Disabled <u>Off</u>	Disable <u>dOff</u>
01	AGC Only	APS1	APS1
10	AGC and 2 line ColorStripe	APS2	APS1
11	AGC and 4 line ColorStripe	APS3	APS1

5.3 **Unrestricted Outputs.** Unless otherwise specified in Section 5.2, Licensed Products may **pass**Pass without restriction WMDRM Content to the following **outputs**Outputs provided the requirements in Section 5.1.1 are met.

5.3.1 **Analog Audio Outputs.** Licensed Products may **passPass** without restriction the Analog Audio Content of decrypted WMDRM Content to Analog Audio Outputs.

5.3.2 **USB Audio Outputs.** Licensed Products may **passPass** without restriction the uncompressed Digital Audio Content of decrypted WMDRM Content to USB Audio Outputs.

5.3.3 **Analog Computer Monitor Outputs.** Licensed Products may **passPass** without restriction the uncompressed Analog Video Content of decrypted WMDRM Content to Analog Computer Monitor Outputs.

5.3.4 **Internal Video Outputs.** Licensed Products may **passPass** without restriction the uncompressed Digital Video Content of decrypted WMDRM Content to Internal Video Outputs.

EXHIBIT 7

ROBUSTNESS RULES FOR WINDOWS MEDIA FORMAT SDK APPLICATIONS

0. DEFINITIONS

The following terms have the meanings set forth below. Other initially capitalized terms not defined in these Compliance Rules have the meanings ascribed to them in the License Agreement or the Microsoft Implementation.

- 0.1 “Application” means software applications running on the Windows Media Format SDK and making use of WMDRM functionality.
- 0.2 “Application Secrets” means, collectively, the WMDRM stub library provided to the Company and secrets that reside in the Application binary and in the process space of the Application.
- 0.3 “Certificate” means a unique WMDRM object used to assess trust, specifically whether or not a device or application has been revoked.
- 0.4 “Certificate Revocation List” means a list of Certificates that have been revoked.
- 0.5 “Certified Output Protection Protocol” or “COPP” enables a robust signaling and content delivery mechanism between the Application and video device drivers.
- 0.6 “Circumvention Device” means a hardware, software or hybrid entity whose primary purpose is the circumvention of Security Functions.
- 0.7 “Collaborative Play-enabled Licensed Products” means Licensed Products that implement Collaborative Play as prescribed by the Compliance Rules.
- 0.8 “Collaborative Session Secrets” means secrets pertaining to the execution of Collaborative Play as prescribed by the Compliance Rules, including without limitation recompressed content encryption keys or assets used by the Licensed Product to secure the exchange of these keys.
- 0.9 “Company” means an entity licensed under a License Agreement to develop Licensed Products.
- 0.10 “Compliance Rules” means the Compliance Rules for the licensed WMDRM Technology, as such Compliance Rules may be amended from time to time.
- 0.11 “Compliant Product” refers to a Licensed Product that is in compliance with all applicable Robustness and Compliance Rules.

- 0.12 “Content Key” means a symmetric key used to decrypt WMDRM Content.
- 0.13 “COPP Session Assets” means the sequence numbers and protection settings for a given COPP session, as described in the Technical Documentation.
- 0.14 “COPP Session Key” means the data integrity key for a given COPP Session as described in the Technical Documentation.
- 0.15 “Debugging Aids” means software/hardware components supporting debugging and profiling tools and/or technologies, including without limitation debugging symbols in software.
- 0.16 “License Agreement” means the agreement under which Microsoft licenses entities to develop and distribute products that include and use the WMDRM components contained in the Windows Media Format SDK redistributable components.
- 0.17 “Licensed Product” means a software application (or other software component, which may be a separately identifiable subset of a software application or operating system) that (i) implements WMDRM subject to a license from Microsoft, (ii) may be capable of passing WMDRM Content and (iii) may make use of WMDRM functionality.
- 0.18 “Licensed Technology” means the WMF SDK.
- 0.19 “Media-enabled Licensed Products” means Licensed Products that are required to enforce output protection on audio and/or video data, as prescribed by the Compliance Rules.
- 0.20 “Microsoft Implementation of WMDRM-ND” means the implementation of WMDRM-ND functionality provided as source code, binaries, technical documentation, tools and/or sample files as provided to Company under the License Agreement.
- 0.21 “Output Protection Level” means a number included in WMDRM Policy that corresponds to the content protection that must be applied when passing WMDRM Content. The Output Protection Level may be determined and assigned by the content owner or may be assigned by the WMDRM Implementation for specific categories of WMDRM Content.
- 0.22 “Output Protection Level Constants” means characterizing information related to interpretation and enforcement of Output Protection Levels as prescribed by the Compliance Rules, including without limitation the OPL designation of the Licensed Product and the correlation between an OPL index and its characteristics.

- 0.23 “Public Cryptography Constants” means all applicable public keys in the public key cryptography sense that are used to validate certificates and/or signatures as prescribed in the Compliance Rules. Public Cryptography Constants include the root public key used to authenticate the WMF SDK API at run time, the Microsoft root public key used to verify a COPP certificate, and the Microsoft root public key used to verify a Certificate Revocation List.
- 0.24 “Robustness Rules” means the rules and requirements set out in this document, as they may be amended from time to time by Microsoft.
- 0.25 “Security Functions” means functions related to protection of content as prescribed by the Technical Documentation and the Compliance Rules, including without limitation transfer of WMDRM Content to WMDRM-ND Receivers, COPP execution including without limitation verification of Certificates, enforcement of the Certificate Revocation List, commanding protection and periodically verifying protection status as prescribed by the Technical Documentation, and WMDRM-ND transmission including without limitation enforcement of maximum number of WMDRM-ND Receivers concurrently receiving WMDRM Content as prescribed by the Technical Documentation.
- 0.26 “Technical Documentation” means, collectively, the WMF SDK Technical Documentation and the Microsoft Implementation of WMDRM-ND.
- 0.27 “Unprotected WMDRM Content” means audio and/or video content that is governed by WMDRM Policy, in a form that is inconsistent with such WMDRM Policy, as described by the Microsoft Implementation and the Compliance Rules.
- 0.28 “Video-enabled Licensed Products” means Licensed Products that are required to enforce output protection on video data, as prescribed by the Compliance Rules.
- 0.29 “WMDRM” means Windows Media Digital Rights Management technology.
- 0.30 “WMDRM Content” means audio or audiovisual content that has been encrypted and recorded using WMDRM whose usage is governed by a WMDRM License.
- 0.31 “WMDRM License” means a data structure that contains, but is not limited to, WMDRM Policy and an encrypted Content Key associated with specific WMDRM Content.
- 0.32 “WMDRM Policy” means the description of the actions permitted and/or required for or with WMDRM Content and restrictions on those actions

as described in the WMDRM License associated with the WMDRM Content.

- 0.33 “WMDRM Technology” means the methods for local decryption and renewability developed by Microsoft for use with Windows Media Digital Rights Management.
- 0.34 “WMDRM-ND” means WMDRM for Networked Devices.
- 0.35 “WMDRM-ND Receiver” means a device, licensed by Microsoft, to connect to WMDRM-ND Transmitters and acquire WMDRM Licenses and WMDRM Content.
- 0.36 “WMDRM-ND Session Assets” means the bookkeeping assets maintained by the WMDRM-ND Transmitter to fulfill requirements of the Technical Documentation and the Compliance Rules; for example, without limitation, the number of devices being served at the current time.
- 0.37 “WMDRM-ND Transmitter” means a product licensed under the License Agreement for WMDRM-ND Platforms that complies with the applicable Compliance Rules and may connect to WMDRM-ND Receivers and issue WMDRM Licenses and WMDRM Content.
- 0.38 “WMDRM-ND Transmitter-enabled Licensed Products” means Licensed Products that implement WMDRM-ND Transmitter functions, as prescribed by the Compliance Rules.
- 0.39 “WMF SDK” means Windows Media Format Software Development Kit.
- 0.40 “WMF SDK Technical Documentation” means documentation provided with the WMF SDK.

1. CONSTRUCTION

- 1.1 **Generally.** Licensed Products as shipped must meet the applicable Robustness and Compliance Rules and be designed and manufactured so as to resist attempts to modify such products so as to defeat the functions of the Technical Documentation, as more specifically described herein.
- 1.2 **Defeating Functions and Features.** Licensed Products must not include control functions means, software switches, backdoors, bypasses, end-user selectable options, debuggers or Debugging Aids, or mechanisms for self-tampering or delayed loading by which the Security Functions may be defeated. Licensed Products must not use, incorporate, call or enable any software that modifies the behavior of the Licensed Product

in a manner that causes it to violate the Compliance Rules. This Section 1.2 does not prohibit Company from designing and implementing its products incorporating means used by Company or professionals to analyze or debug deployed products, or to design its products incorporating software protection techniques such as obfuscation or fragilization, provided, however, that such means do not provide a pretext for inducing consumers to defeat or circumvent mandatory provisions of the Technical Documentation, Robustness Rules or Compliance Rules.

1.3 Keep Secrets. Licensed Products must be designed and manufactured such that they resist attempts to each and all of the following:

- 1.3.1 Use or replace without authority the Application Secrets. For this Section 1.3.1, ‘use without authority’ refers to direct or indirect use or leverage of the Application Secrets by a software entity other than the Licensed Product, by which the Security Functions may be defeated;
- 1.3.2 Replace without authority the Public Cryptographic Constants;
- 1.3.3 For Media-enabled Licensed Products, replace without authority Output Protection Level Constants;
- 1.3.4 For Video-enabled Licensed Products, discover, reveal or replace without authority the COPP Session Key;
- 1.3.5 For Video-enabled Licensed Products, replace without authority the COPP Session Assets;
- 1.3.6 For WMDRM-ND Transmitter-enabled Licensed Products, replace without authority the WMDRM-ND Session Assets;
- 1.3.7 For Collaborative Play-enabled Licensed Products, discover, reveal, replace or use without authority the Collaborative Session Secrets.

2. ACCESSIBILITY OF CONTENT. Company must design and develop Licensed Products such that Unprotected WMDRM Content must not be available as output or via unrestricted application APIs, and must not travel or otherwise be placed outside the application process except as allowed by the Compliance Rules.

3. METHODS OF MAKING FUNCTIONS ROBUST

Licensed Products must use at least the following techniques to be designed to effectively frustrate efforts to circumvent or defeat all applicable Security Functions and protections specified in the Compliance and Robustness Rules:

- 3.1 The Licensed Product must include all of the characteristics set forth in Sections 1 and 2 of these Robustness Rules. In addition, the Licensed Product must:
 - 3.1.1 Achieve compliance with Sections 1 and 2 of these Robustness Rules, to the extent required by Section 4, by reasonable and effective methods, which may include use of techniques of obfuscation to disguise and hamper attempts to discover the approaches used and/or secrets concealed within the software, and/or self-checking of integrity in such a manner as to result in a failure to execute Security Functions in the event of unauthorized modification.
 - 3.1.2 Be implemented such that the failure of a Security Function would cause the implementation to cease further processing and explicitly fail safely, as prescribed by the Technical Documentation.

4. REQUIRED LEVELS OF ROBUSTNESS

- 4.1 The Security Functions and the characteristics set forth in Sections 1.3.1, 1.3.2 and if applicable 1.3.3 must be implemented so that it is reasonably certain that they:
 - 4.1.1 Cannot be defeated or circumvented using Widely Available Tools or Specialized Tools.
- 4.2 The Security Functions and the characteristics set forth in Sections 1.3.4, 1.3.5, 1.3.6, and 1.3.7, wherever applicable, must be implemented so that it is reasonably certain that they:
 - 4.2.1 Cannot be defeated or circumvented using Widely Available Tools.
 - 4.2.2 Can only with difficulty be defeated or circumvented using Specialized Tools.
- 4.3 “Widely Available Tools” means unrestricted application APIs and general-purpose tools or software that are widely available at a reasonable price, such as file readers, file editors, file comparison utilities and internet traffic analyzers, other than Circumvention Devices.
- 4.4 “Specialized Tools” means specialized tools, equipment or software that are widely available at a reasonable price, such as page file scanners, kernel mode code, and memory readers and writers, other than Circumvention Devices.

5. NEW CIRCUMSTANCES. If a Licensed Product when designed and shipped complies with the Robustness Rules 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 Robustness Rules ("New Circumstances"), then upon becoming aware of such New Circumstances, Company shall promptly redesign the affected Licensed Product(s) or make available upgrades to its affected Licensed Product(s) to make such Licensed Products compliant with the Robustness Rules under the New Circumstances, 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 Licensed Product(s), or if such redesign or upgrades are not possible or practical, cease manufacturing such affected Licensed Product(s) and cease selling such affected Licensed Product(s).

ROBUSTNESS RULES FOR WINDOWS MEDIA FORMAT SDK APPLICATIONS

0. DEFINITIONS

The following terms have the meanings set forth below. Other initially capitalized terms not defined in these Compliance Rules have the meanings ascribed to them in the License Agreement or the Microsoft Implementation.

- 0.1 “Application” means software applications running on the Windows Media Format SDK and making use of WMDRM functionality.
- 0.2 “Application Secrets” means, collectively, the WMDRM stub library provided to the Company and secrets that reside in the Application binary and in the process space of the Application.
- 0.3 “Certificate” means a unique WMDRM object used to assess trust, specifically whether or not a device or application has been revoked.
- 0.4 “Certificate Revocation List” means a list of Certificates that have been revoked.
- 0.5 “Certified Output Protection Protocol” or “COPP” enables a robust signaling and content delivery mechanism between the Application and video device drivers.
- 0.6 “Circumvention Device” means a hardware, software or hybrid entity whose primary purpose is the circumvention of Security Functions.
- 0.7 “Collaborative Play-enabled Licensed Products” means Licensed Products that implement Collaborative Play as prescribed by the Compliance Rules.
- 0.8 “Collaborative Session Secrets” means secrets pertaining to the execution of Collaborative Play as prescribed by the Compliance Rules, including without limitation recompressed content encryption keys or assets used by the Licensed Product to secure the exchange of these keys.
- 0.9 “Company” means an entity licensed under a License Agreement to develop Licensed Products.
- 0.10 “Compliance Rules” means the Compliance Rules for the licensed WMDRM Technology, as such Compliance Rules may be amended from time to time.

- 0.11 “Compliant Product” refers to a Licensed Product that is in compliance with all applicable Robustness and Compliance Rules.
- 0.12 “Content Key” ~~means~~ means a symmetric key used to decrypt WMDRM Content.
- 0.13 “COPP Session Assets” means the sequence numbers and protection settings for a given COPP session, as described in the Technical Documentation.
- 0.14 “COPP Session Key” means the data integrity key for a given COPP Session as described in the Technical Documentation.
- 0.15 “Debugging Aids” means software/hardware components supporting debugging and profiling tools and/or technologies, including without limitation debugging symbols in software.
- 0.16 “License Agreement” means the agreement under which Microsoft licenses entities to develop and distribute products that include and use the WMDRM components contained in the Windows Media Format SDK redistributable components.
- 0.17 “Licensed Product” means a software application (or other software component, which may be a separately identifiable subset of a software application or operating system) that (i) implements WMDRM subject to a license from Microsoft, (ii) may be capable of passing WMDRM Content and (iii) may make use of WMDRM functionality.
- 0.18 “Licensed Technology” means the WMF SDK.
- 0.19 “Media-enabled Licensed Products” means Licensed Products that are required to enforce output protection on audio and/or video data, as prescribed by the Compliance Rules.
- 0.20 “Microsoft Implementation of WMDRM-ND” means the implementation of WMDRM-ND functionality provided as source code, binaries, technical documentation, tools and/or sample files as provided to Company under the License Agreement.
- 0.21 “Output Protection Level” means a number included in WMDRM Policy that corresponds to the content protection that must be applied when passing WMDRM Content. The Output Protection Level may be determined and assigned by the content owner or may be assigned by the WMDRM Implementation for specific categories of WMDRM Content.

- 0.22 “Output Protection Level Constants” means characterizing information related to interpretation and enforcement of Output Protection Levels as prescribed by the Compliance Rules, including without limitation the OPL designation of the Licensed Product and the correlation between an OPL index and its characteristics.
- 0.23 “Public Cryptography Constants” means all applicable public keys in the public key cryptography sense that are used to validate certificates and/or signatures as prescribed in the Compliance Rules. Public Cryptography Constants include the root public key used to authenticate the WMF SDK API at run time, the Microsoft root public key used to verify a COPP certificate, and the Microsoft root public key used to verify a Certificate Revocation List.
- 0.24 “Robustness Rules” means the rules and requirements set out in this document, as they may be amended from time to time by Microsoft.
- 0.25 “Security Functions” means functions related to protection of content as prescribed by the Technical Documentation and the Compliance Rules, including without limitation transfer of WMDRM Content to WMDRM-ND Receivers, COPP execution including without limitation verification of Certificates, enforcement of the Certificate Revocation List, commanding protection and periodically verifying protection status as prescribed by the Technical Documentation, and WMDRM-ND transmission including without limitation enforcement of maximum number of WMDRM-ND Receivers concurrently receiving WMDRM Content as prescribed by the Technical Documentation.
- 0.26 “Technical Documentation” means, collectively, the WMF SDK Technical Documentation and the Microsoft Implementation of WMDRM-ND.
- 0.27 “Unprotected WMDRM Content” means audio and/or video content that is governed by WMDRM Policy, in a form that is inconsistent with such WMDRM Policy, as described by the Microsoft Implementation and the Compliance Rules.
- 0.28 “Video-enabled Licensed Products” means Licensed Products that are required to enforce output protection on video data, as prescribed by the Compliance Rules.
- 0.29 “WMDRM” means Windows Media Digital Rights Management technology.
- 0.30 “WMDRM Content” means audio or audiovisual content that has been encrypted and recorded using WMDRM whose usage is governed by a WMDRM License.

- 0.31 “WMDRM License” means a data structure that contains, but is not limited to, WMDRM Policy and an encrypted Content Key associated with specific WMDRM Content.
- 0.32 “WMDRM Policy” means the description of the actions permitted and/or required for or with WMDRM Content and restrictions on those actions as described in the WMDRM License associated with the WMDRM Content.
- 0.33 “WMDRM Technology” means the methods for local decryption and renewability developed by Microsoft for use with Windows Media Digital Rights Management.
- 0.34 “WMDRM-ND” means WMDRM for Networked Devices.
- 0.35 “WMDRM-ND Receiver” means a device, licensed by Microsoft, to connect to WMDRM-ND Transmitters and acquire WMDRM Licenses and WMDRM Content.
- 0.36 “WMDRM-ND Session Assets” means the bookkeeping assets maintained by the WMDRM-ND Transmitter to fulfill requirements of the Technical Documentation and the Compliance Rules; for example, without limitation, the number of devices being served at the current time.
- 0.37 “WMDRM-ND Transmitter” means a product licensed under the License Agreement for WMDRM-ND Platforms that complies with the applicable Compliance Rules and may connect to WMDRM-ND Receivers and issue WMDRM Licenses and WMDRM Content.
- 0.38 “WMDRM-ND Transmitter-enabled [Licensed Products](#)” means Licensed Products that implement WMDRM-ND Transmitter functions, as prescribed by the Compliance Rules.
- 0.39 “WMF SDK” means Windows Media Format Software Development Kit.
- 0.40 “WMF SDK Technical Documentation” means documentation provided with the WMF SDK.

1. CONSTRUCTION

- 1.1 **Generally.** Licensed Products as shipped must meet the applicable Robustness and Compliance Rules and be designed and manufactured so as to resist attempts to modify such products so as

to defeat the functions of the Technical Documentation, as more specifically described herein.

1.2 **Defeating Functions and Features.** Licensed Products must not include control functions, means, software switches, backdoors, bypasses, end-user selectable options, debuggers or Debugging Aids, or mechanisms for self-tampering or delayed loading by which the Security Functions may be defeated. Licensed Products must not use, incorporate, call or enable any software that modifies the behavior of the Licensed Product in a manner that causes it to violate the Compliance Rules. This Section 1.2 does not prohibit Company from designing and implementing its products incorporating means used by Company or professionals to analyze or debug deployed products, or to design its products incorporating software protection techniques such as obfuscation or fragilization, provided, however, that such means do not provide a pretext for inducing consumers to defeat or circumvent mandatory provisions of the Technical Documentation, Robustness Rules or Compliance Rules.

1.3 **Keep Secrets.** Licensed Products must be designed and manufactured such that they resist attempts to each and all of the following:

- 1.3.1 Use or replace without authority the Application Secrets. For this Section 1.3.1, 'use without authority' refers to direct or indirect use or leverage of the Application Secrets by a software entity other than the Licensed Product, by which the Security Functions may be defeated;
- 1.3.2 Replace without authority the Public Cryptographic Constants;
- 1.3.3 For Media-enabled Licensed Products, replace without authority Output Protection Level Constants;
- 1.3.4 For Video-enabled Licensed Products, discover, reveal or replace without authority the COPP Session Key;
- 1.3.5 For Video-enabled Licensed Products, replace without authority the COPP Session Assets;
- 1.3.6 For WMDRM-ND Transmitter-enabled Licensed Products, replace without authority the WMDRM-ND Session Assets;
- 1.3.7 For Collaborative Play-enabled Licensed Products, discover, reveal, replace or use without authority the Collaborative Session Secrets.

2. ACCESSIBILITY OF CONTENT. Company must design and develop Licensed Products such that Unprotected WMDRM Content must not be available as output or via unrestricted application APIs, and must not travel or otherwise be placed outside the application process except as allowed by the Compliance Rules.

3. METHODS OF MAKING FUNCTIONS ROBUST

Licensed Products must use at least the following techniques to be designed to effectively frustrate efforts to circumvent or defeat all applicable Security Functions and protections specified in the Compliance and Robustness Rules:

3.1 The Licensed Product must include all of the characteristics set forth in Sections 1 and 2 of these Robustness Rules. In addition, the Licensed Product must:

3.1.1 Achieve compliance with Sections 1 and 2 of these Robustness Rules, to the extent required by Section 4, by reasonable and effective methods, which may include use of techniques of obfuscation to disguise and hamper attempts to discover the approaches used and/or secrets concealed within the software, and/or self-checking of integrity in such a manner as to result in a failure to execute Security Functions in the event of unauthorized modification.

3.1.2 Be implemented such that the failure of a Security Function would cause the implementation to cease further processing and explicitly fail safely, as prescribed by the Technical Documentation.

4. REQUIRED LEVELS OF ROBUSTNESS

4.1 The Security Functions and the characteristics set forth in Sections 1.3.1, 1.3.2 and if applicable 1.3.3 must be implemented so that it is reasonably certain that they:

4.1.1 Cannot be defeated or circumvented using Widely Available Tools or Specialized Tools.

4.2 The Security Functions and the characteristics set forth in Sections 1.3.4, 1.3.5, 1.3.6, and 1.3.7, wherever applicable, must be implemented so that it is reasonably certain that they:

4.2.1 Cannot be defeated or circumvented using Widely Available Tools.

4.2.2 Can only with difficulty be defeated or circumvented using Specialized Tools.

4.3 “Widely Available Tools” means unrestricted application APIs and general-purpose tools or software that are widely available at a reasonable price, such as file readers, file editors, file comparison utilities and internet traffic analyzers, other than Circumvention Devices.

4.4 “Specialized Tools” means specialized tools, equipment or software that are widely available at a reasonable price, such as page file scanners, kernel mode code, and memory readers and writers, other than Circumvention Devices.

5. NEW CIRCUMSTANCES. If a Licensed Product when designed and shipped complies with the Robustness Rules 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 Robustness Rules (“New Circumstances”), then upon becoming aware of such New Circumstances, Company shall promptly redesign the affected Licensed Product(s) or make available upgrades to its affected Licensed Product(s) to make such Licensed Products compliant with the Robustness Rules under the New Circumstances, 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 Licensed Product(s), or if such redesign or upgrades are not possible or practical, cease manufacturing such affected Licensed Product(s) and cease selling such affected Licensed Product(s).

EXHIBIT 8

**ROBUSTNESS RULES
FOR WMDRM-NETWORK DEVICES AND WMDRM-PORTABLE DEVICES**

0. DEFINITIONS

Initially capitalized terms not defined below have the meanings ascribed to them elsewhere in these Robustness Rules.

- 0.1 “Certificate” means a unique WMDRM object used to assess trust, specifically whether or not a device or application has been revoked.
- 0.2 “Certificate Signing Private Key” means an asymmetric private key generated by Company.
- 0.3 “Company” means an entity licensed under a License Agreement to develop Licensed Products.
- 0.4 “Compliance Rules” means the Compliance Rules for the licensed WMDRM Technology, as such Compliance Rules may be amended from time to time.
- 0.5 “Confidential User Information” means information about the end users’ use of WMDRM-PD, including but not limited to Metering Data.
- 0.6 “Consistent with the Microsoft Implementation” means the Licensed Product (i) provides equivalent functionality to the Microsoft Implementation, (ii) equals or exceeds the security of the Microsoft Implementation, and (iii) maintains compatibility and interoperability with the Microsoft Implementation.
- 0.7 “Content Key” means a symmetric key used to decrypt WMDRM Content.
- 0.8 “Cryptographically Random” means unpredictable, in that, at any point regardless of how many preceding bits are available, the probability of predicting the next succeeding K bits is greater than $\frac{1}{2}^K$.
- 0.9 “Debugging Aids” means software/hardware components supporting debugging and profiling tools and/or technologies, including without limitation debugging symbols in software.
- 0.10 “Device Certificate” means a digital certificate assigned to a Licensed Product and used for example to evaluate whether the Licensed Product is trusted and eligible to receive WMDRM Content.
- 0.11 “Device Key” means an associated pair of Cryptographically Random keys generated by Company for each of its Licensed Products, consisting of a “Device Public Key” and a “Device Private Key”.

- 0.12 “Device Private Key” means a unique, Cryptographically Random asymmetric private key generated by or for Licensed Products for the purpose of decrypting Content Keys.
- 0.13 “Device Public Key” means the public portion of the Device Keys.
- 0.14 “Device Secrets” means, for WMDRM-ND, the Device Private Key, and for WMDRM-PD, the Device Private Key, the Fallback Keys and the Certificate Signing Private Key.
- 0.15 “Direct License Acquisition” or “DLA” means the process of acquiring a WMDRM license directly from a WMDRM Server.
- 0.16 “Fallback Keys” means an associated pair of keys for Licensed Products for the purpose of Direct License Acquisition from WMDRM Servers.
- 0.17 “License Agreement” means the agreement under which Microsoft licenses entities to develop and distribute products that include implementations of WMDRM-ND and/or WMDRM-PD.
- 0.18 “Licensed Product” means a hardware device or software application (or other software component, which may be a separately identifiable subset of a software application or operating system) that (i) implements WMDRM subject to a license from Microsoft, (ii) may be capable of passing WMDRM Content and (iii) may make use of WMDRM functionality.
- 0.19 “Metering Data” means the stored content usage information collected and reported upon by the WMDRM Metering feature.
- 0.20 “Microsoft Implementation” means the implementation of WMDRM-ND and/or WMDRM-PD functionality provided as source code, binaries, technical documentation, tools and/or sample files as provided to Company under the License Agreement.
- 0.21 “Robustness Rules” means the rules and requirements set out in this document, as they may be amended from time to time by Microsoft.
- 0.22 “Secure Clock State” means the date and time information stored within the Secure Clock.
- 0.23 “Secure Clock” means a hardware real time clock that has been secured from unauthorized access.
- 0.24 “Serial Number” means an identifier with a minimum length of 128 bits that must be unique to each Licensed Product manufactured by or on behalf of Company.

- 0.25 “Specifically Set Serial Number” means to set the serial number of a Licensed Product in such a manner as to violate the condition of uniqueness of the serial number as prescribed by the Compliance Rules.
- 0.26 “Unprotected WMDRM Content” means audio and/or video content that is governed by WMDRM Policy, in a form that is inconsistent with such WMDRM Policy, as described by the Microsoft Implementation and the Compliance Rules.
- 0.27 “WMDRM” means Windows Media Digital Rights Management technology.
- 0.28 “WMDRM Content” means audio or audiovisual content that has been encrypted and recorded using WMDRM and whose usage is governed by a WMDRM License.
- 0.29 “WMDRM Content Keys” means, for WMDRM-ND, the WMDRM-ND Session Keys, and for WMDRM-PD, the Content Keys.
- 0.30 “WMDRM Data Stores” means the secure databases required for mandatory and optional WMDRM features. This includes, but is not limited to, License store, Secure store, Metering store and License Synchronization store as defined in the Microsoft Implementation.
- 0.31 “WMDRM License” means a data structure that contains, but is not limited to, WMDRM Policy and an encrypted Content Key associated with specific WMDRM Content.
- 0.32 “WMDRM Policy” means the description of the actions permitted and/or required for or with WMDRM Content and restrictions on those actions as described in the WMDRM License associated with the WMDRM Content.
- 0.33 “WMDRM Server” means a Licensed Product capable of issuing WMDRM Licenses over a network connection.
- 0.34 “WMDRM Technology” means the methods for local decryption and renewability developed by Microsoft for use with Windows Media Digital Rights Management.
- 0.35 “WMDRM-ND Session Keys” means, for a given WMDRM-ND session, (1) the data security key used to encrypt media data, and (2) the data integrity key used to sign messages such as the policy message.
- 0.36 “WMDRM-ND” means WMDRM for Network Devices.
- 0.37 “WMDRM-PD” means WMDRM for Portable Devices.

1. CONSTRUCTION

- 1.1 **Generally.** Licensed Products as shipped must meet the applicable Robustness and Compliance Rules and be designed and manufactured so as to resist attempts to modify such products so as to defeat the functions of the Microsoft Implementation, as more specifically described herein.
- 1.2 **Defeating Functions and Features.** Licensed Products must 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), debuggers or Debugging Aids or software equivalents of any of the foregoing by which content protection technologies or other mandatory provisions of the Microsoft Implementation, Robustness Rules or Compliance Rules may be defeated or by which Unprotected WMDRM Content may be exposed to unauthorized copying, usage or distribution. This Section 1.2 does not prohibit Company from designing and manufacturing its products incorporating means, such as test points, used by Company or professionals to analyze or repair products, provided, however, that such means do not provide a pretext for inducing consumers to defeat or circumvent mandatory provisions of the Microsoft Implementation, Robustness Rules or Compliance Rules.
- 1.3 **Keep Secrets.** Licensed Products must be designed and manufactured such that they resist attempts to each and all of the following:
 - 1.3.1 Discover, reveal, or use or replace without authority the Device Secrets;
 - 1.3.2 Discover or reveal the WMDRM Content Keys;
 - 1.3.3 Specifically Set the Serial Number;
 - 1.3.4 For Licensed Products implementing a WMDRM-PD Secure Clock, replace the Secure Clock State without authority.
- 1.4 **Keep Confidential.** Licensed Products that implement WMDRM-PD must be designed and manufactured such that they resist unauthorized attempts to discover Confidential User Information. Company is deemed to be in compliance with Section 1.4 if it complies with Section 4.3 below.

2. ACCESSIBILITY OF CONTENT. Company must design and develop Licensed Products such that Unprotected WMDRM Content is not available on device outputs other than those device outputs expressly specified (and in the form specified) in these Robustness and Compliance Rules. Within Licensed Products, decrypted compressed video data must be protected by a robust method when transiting a User Accessible Bus.

- 2.1 “User Accessible Bus” means a data bus that is designed for end user upgrades or access, such as PCMCIA, device bay, IEEE 1394, PCI buses with user accessible sockets or Cardbus, but not graphics buses, memory buses, CPU buses, internal PCI buses or other point-to-point buses, and similar portions of a device's internal architecture. This Section 2.1 does not prohibit Company from designing and manufacturing its products incorporating means, such as test points, used by Company or professionals to analyze or repair products, provided, however, that such means do not provide a pretext for inducing consumers to obtain ready and unobstructed access to internal connectors.
- 2.2 “Security Functions” means:
- 2.2.1 For Licensed Products implementing WMDRM-PD, functions related to authentication, encryption, decryption, Device Certificate signing, output protection, metering, Secure Clock, content revocation, key management, and rights enforcement and storing/updating information in the WMDRM Data Stores as such terms are described and required in the Microsoft Implementation, to the extent such functions are implemented in a Licensed Product implementing WMDRM-PD.
- 2.2.2 For Licensed Products implementing WMDRM-ND, functions related to decryption, WMDRM-ND protocol and output protection as described and required in the Microsoft Implementation.
- 2.2.3 For Licensed Products implementing both WMDRM-PD and WMDRM-ND, all functions listed in Sections 2.2.1 and 2.2.2.

3. METHODS OF MAKING FUNCTIONS ROBUST

Licensed Products must use at least the following techniques to be designed to effectively frustrate efforts to circumvent or defeat the functions and protections specified in the Compliance and Robustness Rules:

- 3.1 **Robustness Requirements Applicable to Software Implementations.** Any portion of a Licensed Product that implements one or more of the Security Functions in software must include all of the characteristics set forth in Sections 1 and 2 of these Robustness Rules. In addition, such implementations must:
- 3.1.1 Comply with Section 1.3 and, if applicable as defined by the Compliance Rules, Section 1.4 of these Robustness Rules, by reasonable and effective methods, which may include, but are not limited to: encryption, execution of a portion of the implementation in kernel mode, embodiment in a secure physical

implementation, using techniques of obfuscation to disguise and hamper attempts to discover the approaches used or secrets concealed within the software, and/or self-checking of integrity in such a manner as to result in a failure to execute Security Functions in the event of unauthorized modification.

3.1.2 Be implemented such that the failure of a Security Function would cause the implementation to cease further processing Consistent with the Microsoft Implementation.

3.2 Robustness Requirements Applicable to Hardware Implementations.
Any portion of the Licensed Product that implements one or more Security Functions in hardware must include all of the characteristics set forth in Sections 1 and 2 of these Robustness Rules. The fact that a software implementation operates on a hardware computing platform does not, in and of itself, cause such hardware computer platform to be subject to the requirements set forth in Sections 3.2 and 3.3. If, however, the software implementation relies on hardware or any hardware component to satisfy any of these Robustness Rules, then such hardware or hardware component must satisfy all of the Robustness Rules set forth in this Section 3.2 for hardware implementations. In addition, such implementation must:

3.2.1 Comply with Section 1.3 and, if applicable as defined by the Compliance Rules, Section 1.4 of these Robustness Rules, by reasonable and effective means including, but not limited to: embedding secrets in silicon circuitry or firmware that cannot reasonably be read or replaced, or the techniques described in Section 3.1 for software.

3.3 Robustness Requirements Applicable to Hybrid Implementations.
The interfaces between hardware and software portions of a Licensed Product must be designed so that the hardware portions comply with the level of robustness that is required for a pure hardware implementation and the software portions comply with the level of robustness that is required for a pure software implementation.

4. REQUIRED LEVELS OF ROBUSTNESS

4.1 The Security Functions and the characteristics set forth in Section 1.3.1 must be implemented so that it is reasonably certain that they:

4.1.1 Cannot be defeated or circumvented using Widely Available Tools or Specialized Tools.

4.1.2 Can only with difficulty be defeated or circumvented using Professional Tools.

- 4.2 The Security Functions and the characteristics set forth in Sections 1.3.2, 1.3.3, and, if applicable as defined by the Compliance Rules, Section 1.3.4, must be implemented so that it is reasonably certain that they:
 - 4.2.1 Cannot be defeated or circumvented using Widely Available Tools.
 - 4.2.2 Can only with difficulty be defeated or circumvented using Specialized Tools or Professional Tools.
- 4.3 If applicable as defined by the Compliance Rules, the characteristics set forth in Section 1.4 must be implemented so that it is reasonably certain that they:
 - 4.3.1 Can only with difficulty be defeated or circumvented using Widely Available Tools.
- 4.4 “Widely Available Tools” means general-purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips, file editors, and soldering irons, but does not include 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 Microsoft Implementation (“Circumvention Devices”).
- 4.5 “Specialized Tools” means 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 Circumvention Devices.
- 4.6 “Professional Tools” means professional tools or equipment, such as logic analyzers, chip disassembly systems, in-circuit emulators and their software equivalents, disassemblers, loaders, or patchers, such as would be used primarily by persons of professional skill and training, but not including either professional tools or equipment that are made available on the basis of a non-disclosure agreement or Circumvention Devices.

5. NEW CIRCUMSTANCES. If a Licensed Product when designed and shipped complies with the Robustness Rules 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 Robustness Rules (“New Circumstances”), then upon becoming aware of such New Circumstances, Company shall promptly redesign the affected Licensed Product(s) or make available upgrades to its affected Licensed Product(s) to make such Licensed Products compliant with the Robustness Rules under the New Circumstances, 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 Licensed Product(s), or if such redesign or upgrades are not possible or

practical, cease manufacturing such affected Licensed Product(s) and cease selling such affected Licensed Product(s).

ROBUSTNESS RULES FOR WMDRM-NETWORK DEVICES AND WMDRM-PORTABLE DEVICES

0. DEFINITIONS

Initially capitalized terms not defined below have the meanings ascribed to them elsewhere in these Robustness Rules.

- 0.1 “Certificate” means a unique WMDRM object used to assess trust, specifically whether or not a device or application has been revoked.
- 0.2 “Certificate Signing Private Key” means an asymmetric private key generated by Company.
- ~~0.3 “Certified Output Protection Protocol” or “COPP” enables robust signaling and content delivery mechanism between applications and video device drivers.~~
- ~~0.3~~ 0.4 “Company” means an entity licensed under a License Agreement to develop Licensed Products.
- ~~0.4~~ 0.5 “Compliance Rules” means the Compliance Rules for the licensed WMDRM Technology, as such Compliance Rules may be amended from time to time.
- ~~0.5~~ 0.6 “Confidential User Information” means information about the end users’ use of WMDRM-PD, including but not limited to Metering Data.
- ~~0.6~~ 0.7 “Consistent with the Microsoft Implementation” means the Licensed Product (i) provides equivalent functionality to the Microsoft Implementation, (ii) equals or exceeds the security of the Microsoft Implementation, and (iii) maintains compatibility and interoperability with the Microsoft Implementation.
- ~~0.7~~ 0.8 “Content Key” means a symmetric key used to decrypt WMDRM Content.
- ~~0.8~~ 0.9 “Cryptographically Random” means unpredictable, in that, at any point regardless of how many preceding bits are available, the probability of predicting the next succeeding K bits is greater than $\frac{1}{2}^K$.
- ~~0.9~~ 0.10 “Debugging Aids” means software/hardware components supporting debugging and profiling tools and/or technologies, including without limitation debugging symbols in software.
- ~~0.10~~ 0.11 “Device Certificate” means a digital certificate assigned to a Licensed ~~Products~~Product and used for example to evaluate whether

~~a~~the Licensed Product is trusted and eligible to receive WMDRM Content.

- 0.11 ~~0.12~~ “Device Key” means an associated pair of Cryptographically Random keys generated by Company for each of its Licensed Products, consisting of a “Device Public Key” and a “Device Private Key”.
- 0.12 ~~0.13~~ “Device Private Key” means a unique, Cryptographically Random asymmetric private key generated by or for Licensed Products for the purpose of decrypting Content Keys.
- 0.13 ~~0.14~~ “Device Public Key” means the public portion of the Device Keys.
- 0.14 ~~0.15~~ “Device Secrets” means, for WMDRM-ND, the Device Private Key, and for WMDRM-PD, the Device Private Key, the Fallback Keys and the Certificate Signing Private Key.
- 0.15 ~~0.16~~ “Direct License Acquisition” or “DLA” means the process of acquiring a WMDRM license directly from a WMDRM Server.
- 0.16 ~~0.17~~ “Fallback Keys” means an associated pair of keys for Licensed Products for the purpose of Direct License Acquisition from WMDRM Servers.
- 0.17 ~~0.18~~ “License Agreement” means the agreement under which Microsoft licenses entities to develop and distribute products that include implementations of WMDRM-ND and/or WMDRM-PD.
- 0.18 ~~0.19~~ “Licensed Product” means a hardware device or software application (or other software component, which may be a separately identifiable subset of a software application or operating system) that (i) implements WMDRM subject to a license from Microsoft, (ii) may be capable of passing WMDRM Content and (iii) may make use of WMDRM functionality.
- 0.19 ~~0.20~~ “Metering Data” means the stored content usage information collected and reported upon by the WMDRM Metering feature.
- 0.20 ~~0.21~~ “Microsoft Implementation” means the implementation of WMDRM-ND and/or WMDRM-PD functionality provided as source code, binaries, technical documentation, tools and/or sample files as provided to Company under the License Agreement.
- 0.21 ~~0.22~~ “Robustness Rules” means the rules and requirements set out in this document, as they may be amended from time to time by Microsoft.
- 0.22 ~~0.23~~ “Secure Clock State” means the date and time information stored within the Secure Clock.

- 0.23** ~~0.24~~ “Secure Clock” means a hardware real time clock that has been secured from unauthorized access.
- 0.24** ~~0.25~~ “Serial Number” means an identifier with a minimum length of 128 bits that must be unique to each Licensed Product manufactured by or on behalf of Company.
- 0.25** ~~0.26~~ “Specifically Set Serial Number” means to set the serial number of a Licensed Product in such a manner as to violate the condition of uniqueness of the serial number as prescribed by the Compliance Rules.
- 0.26** ~~0.27~~ “Unprotected WMDRM Content” means audio and/or video content that is governed by WMDRM Policy, in a form that is inconsistent with such WMDRM Policy, as described by the Microsoft Implementation and the Compliance Rules.
- 0.27** ~~0.28~~ “WMDRM” means Windows Media Digital Rights Management technology.
- 0.28** ~~0.29~~ “WMDRM Content” means audio or audiovisual content that has been encrypted and recorded using WMDRM and whose usage is governed by a WMDRM License.
- 0.29** ~~0.30~~ “WMDRM Content Keys” means, for WMDRM-ND, the WMDRM-ND Session Keys, and for WMDRM-PD, the Content Keys.
- 0.30** ~~0.31~~ “WMDRM Data Stores” means the secure databases required for mandatory and optional WMDRM features. This includes, but is not limited to, License store, Secure store, Metering store and License Synchronization store as defined in the Microsoft Implementation.
- 0.31** ~~0.32~~ “WMDRM License” means a data structure that contains, but is not limited to, WMDRM Policy and an encrypted Content Key associated with specific WMDRM Content.
- 0.32** ~~0.33~~ “WMDRM Policy” means the description of the actions permitted and/or required for or with WMDRM Content and restrictions on those actions as described in the WMDRM License associated with the WMDRM Content.
- 0.33** ~~0.34~~ “WMDRM Server” means a Licensed Product capable of issuing WMDRM Licenses over a network connection.
- 0.34** ~~0.35~~ “WMDRM Technology” means the methods for local decryption and renewability developed by Microsoft for use with Windows Media Digital Rights Management.

0.35 ~~0.36~~ “WMDRM-ND Session Keys” means, for a given WMDRM-ND session, (1) the data security key used to encrypt media data, and (2) the data integrity key used to sign messages such as the policy message.

0.36 ~~0.37~~ “WMDRM-ND” means WMDRM for Network Devices.

0.37 ~~0.38~~ “WMDRM-PD” means WMDRM for Portable Devices.

1. CONSTRUCTION

- 1.1 **Generally.** Licensed Products as shipped must meet the applicable Robustness and Compliance Rules and be designed and manufactured so as to resist attempts to modify such products so as to defeat the functions of the Microsoft Implementation, as more specifically described herein.
- 1.2 **Defeating Functions and Features.** Licensed Products must 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), debuggers or Debugging Aids or software equivalents of any of the foregoing by which content protection technologies or other mandatory provisions of the Microsoft Implementation, Robustness Rules or Compliance Rules may be defeated or by which Unprotected WMDRM Content may be exposed to unauthorized copying, usage or distribution. This Section 1.2 does not prohibit Company from designing and manufacturing its products incorporating means, such as test points, used by Company or professionals to analyze or repair products, provided, however, that such means do not provide a pretext for inducing consumers to defeat or circumvent mandatory provisions of the Microsoft Implementation, Robustness Rules or Compliance Rules.
- 1.3 **Keep Secrets.** Licensed Products must be designed and manufactured such that they resist attempts to each and all of the following:
 - 1.3.1 Discover, reveal, or use or replace without authority the Device Secrets;
 - 1.3.2 Discover or reveal the ~~Controlled~~WMDRM Content Keys;
 - 1.3.3 Specifically Set the Serial Number;
 - 1.3.4 For Licensed Products implementing a WMDRM-PD Secure Clock, replace the Secure Clock State without authority;
- 1.4 **Keep Confidential.** Licensed Products that implement WMDRM-PD must be designed and manufactured such that they resist unauthorized attempts to discover Confidential User Information. Company is deemed to be in compliance with Section 1.4 if it complies with Section 4.3 below.

2. ACCESSIBILITY OF CONTENT. Company must design and develop Licensed Products such that Unprotected WMDRM Content is not available on device outputs other than those device outputs expressly specified (and in the form specified) in these Robustness and Compliance Rules. Within Licensed Products, decrypted compressed video data must be protected by a robust method when transiting a User Accessible Bus.

2.1 “User Accessible Bus” means a data bus that is designed for end user upgrades or access, such as PCMCIA, device bay, IEEE 1394, PCI buses with user accessible sockets or Cardbus, but not graphics buses, memory buses, CPU buses, internal PCI buses or other point-to-point buses, and similar portions of a device's internal architecture. This Section 2.1 does not prohibit Company from designing and manufacturing its products incorporating means, such as test points, used by Company or professionals to analyze or repair products, provided, however, that such means do not provide a pretext for inducing consumers to obtain ready and unobstructed access to internal connectors.

2.2 “Security Functions” means:

2.2.1 For Licensed Products implementing WMDRM-PD, functions related to authentication, encryption, decryption, Device Certificate signing, output protection, metering, Secure Clock, content revocation, key management, and rights enforcement and storing/updating information in the WMDRM Data Stores as such terms are described and required in the Microsoft Implementation, to the extent such functions are implemented in a Licensed Product implementing WMDRM-PD.

2.2.2 For Licensed Products implementing WMDRM-ND, functions related to decryption, WMDRM-ND protocol and output protection as described and required in the Microsoft Implementation.

2.2.3 For Licensed Products implementing both WMDRM-PD and WMDRM-ND, all functions listed in Sections 2.2.1 and 2.2.2.

3. METHODS OF MAKING FUNCTIONS ROBUST

Licensed Products must use at least the following techniques to be designed to effectively frustrate efforts to circumvent or defeat the functions and protections specified in the Compliance and Robustness Rules:

3.1 **Robustness Requirements Applicable to Software Implementations.** Any portion of a Licensed Product that implements one or more of the Security Functions in software must include all of the characteristics set

forth in Sections 1 and 2 of these Robustness Rules. In addition, such implementations must:

- 3.1.1 Comply with Section 1.3 and, if applicable as defined by the Compliance Rules, Section 1.4 of these Robustness Rules, by reasonable and effective methods, which may include, but are not limited to: encryption, execution of a portion of the implementation in kernel mode, embodiment in a secure physical implementation, using techniques of obfuscation to disguise and hamper attempts to discover the approaches used or secrets concealed within the software, and/or self-checking of integrity in such a manner as to result in a failure to execute Security Functions in the event of unauthorized modification.
- 3.1.2 Be implemented such that the failure of a Security Function would cause the implementation to cease further processing Consistent with the Microsoft Implementation.

- 3.2 **Robustness Requirements Applicable to Hardware Implementations.** Any portion of the Licensed Product that implements one or more Security Functions in hardware must include all of the characteristics set forth in Sections 1 and 2 of these Robustness Rules. The fact that a software implementation operates on a hardware computing platform does not, in and of itself, cause such hardware computer platform to be subject to the requirements set forth in Sections 3.2 and 3.3. If, however, the software implementation relies on hardware or any hardware component to satisfy any of these Robustness Rules, then such hardware or hardware component must satisfy all of the Robustness Rules set forth in this Section 3.2 for hardware implementations. In addition, such implementation must:

- 3.2.1 Comply with Section 1.3 and, if applicable as defined by the Compliance Rules, Section 1.4 of these Robustness Rules, by reasonable and effective means including, but not limited to: embedding secrets in silicon circuitry or firmware that cannot reasonably be read or replaced, or the techniques described in Section 3.1 for software.

- 3.3 **Robustness Requirements Applicable to Hybrid Implementations.** The interfaces between hardware and software portions of a Licensed Product must be designed so that the hardware portions comply with the level of robustness that is required for a pure hardware implementation and the software portions comply with the level of robustness that is required for a pure software implementation.

4. REQUIRED LEVELS OF ROBUSTNESS

- 4.1 The Security Functions and the characteristics set forth in Section 1.3.1 must be implemented so that it is reasonably certain that they:
 - 4.1.1 Cannot be defeated or circumvented using Widely Available Tools or Specialized Tools.
 - 4.1.2 Can only with difficulty be defeated or circumvented using Professional Tools.
- 4.2 The Security Functions and the characteristics set forth in ~~Section~~[Sections](#) 1.3.2, 1.3.3, and, if applicable as defined by the Compliance Rules, Section 1.3.4, must be implemented so that it is reasonably certain that they:
 - 4.2.1 Cannot be defeated or circumvented using Widely Available Tools.
 - 4.2.2 Can only with difficulty be defeated or circumvented using ~~or~~ Specialized Tools or Professional Tools.
- 4.3 If applicable as defined by the Compliance Rules, the characteristics set forth in Section 1.4 must be implemented so that it is reasonably certain that they:
 - 4.3.1 Can only with difficulty be defeated or circumvented using Widely Available Tools.
- 4.4 “Widely Available Tools” means general-purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips, file editors, and soldering irons, but does not include 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 Microsoft Implementation (“Circumvention Devices”).
- 4.5 “Specialized Tools” means 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 Circumvention Devices.
- 4.6 “Professional Tools” means professional tools or equipment, such as logic analyzers, chip disassembly systems, in-circuit emulators and their software equivalents, disassemblers, loaders, or patchers, such as would be used primarily by persons of professional skill and training, but not including either professional tools or equipment that are made available on the basis of a non-disclosure agreement or Circumvention Devices.

5. NEW CIRCUMSTANCES. If a Licensed Product when designed and shipped complies with the Robustness Rules 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 Robustness Rules ("New Circumstances"), then upon becoming aware of such New Circumstances, Company shall promptly redesign the affected Licensed Product(s) or make available upgrades to its affected Licensed Product(s) to make such Licensed Products compliant with the Robustness Rules under the New Circumstances, 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 Licensed Product(s), or if such redesign or upgrades are not possible or practical, cease manufacturing such affected Licensed Product(s) and cease selling such affected Licensed Product(s).