Compliance and Robustness Rules
For Devices Containing Adobe Flash Access 2.0 or (Later Versions, including Adobe Access and Adobe Primetime DRM) Client Software

These Compliance and Robustness Rules shall apply as specified below to use of Flash Access, Adobe Access or Adobe Primetime DRM (for the purposes of these Compliance and Robustness Rules, collectively “Flash Access”) Licensed Software and Certificates in devices to allow decryption and consumption of content encrypted using Flash Access.

All capitalized terms not defined in Section 1 shall have the meaning defined in the relevant Adobe license agreement under which you are using the Licensed Software and Certificates (the “License Agreement”) for the foregoing purposes and are required to comply with these Compliance and Robustness Rules.

1. Definitions.

1.1. “Adobe Implementation” means the implementation of Flash Access functionality provided to Licensee as source code, binaries, technical documentation, tools, and or sample files under the License Agreement.

1.2. “Adobe Runtime” means Adobe AIR, Adobe Flash Player, a player developed using an Adobe Primetime Player SDK and any other future runtime utilizing Adobe’s Flash or Adobe Primetime Player technology distributed by Adobe or its licensees.

1.3. “Analog Component Video Output” means the set of three YPrPb consumer electronics analog connectors to a Display Device.

1.4. “Analog Computer Monitor Output” means a connector for an analog Display Device typically found and associated with a personal computer that carries uncompressed analog video signals, including but not limited to VGA, SVGA, XGA, DVI Analog.

1.5. “Analog Television Output” means typical consumer electronics analog connectors such as NTSC, PAL, SECAM, SCART, YPrPb, S-Video, and consumer RGB.

1.6. “Anti Rollback Clock” means a real-time clock that is periodically verified to have advanced since the last check.

1.7. “Authorized Analog Video Protection” means the CGMS-A, Color Stripe, AGC, and APSTB copy protection technologies.

1.8. “Authorized Digital Video Protection” means the HDCP copy protection technology.

1.9. “Content Encryption Key” means an AES private key used by a Licensee Product to decrypt Flash Access Protected Content.

1.10. “Content Samples” means small samples of Decrypted Content in compressed or decompressed form.

1.11. “Content License” means metadata (stored on a computer and/or embedded in an electronic file delivered to a Licensee Product that (i) contains an encrypted Content Encryption Key and (ii) contains or refers to usage rules for Flash Access Protected Content designed to be enforced directly through Flash Access software in a Licensee Product.


1.13. “Certificate Revocation List” (or CRL) means electronic documents published by Adobe to
identify Certificates that are no longer valid, having been revoked by Adobe.

1.14. “Circumvention Tools” means devices or technologies whether hardware or software which are designed and made available for the specific purpose of bypassing or circumventing one or more Content Protection Functions.

1.15. “Compliance Functions” means those aspects of the Licensed Software and Licensee Product that are designed to ensure compliance with the Compliance and Robustness Rules and to prevent playback, copying, modification, redistribution or other actions with respect to Flash Access Protected Content except as explicitly allowed by an applicable Content License.

1.16. “Decrypt” “Decrypted” or “Decryption” means the process of decrypting Flash Access Protected Content using a Content Encryption Key.

1.17. “Decrypted Content” means audiovisual and sound content that was Flash Access Protected Content until being Decrypted.

1.18. “Device Capabilities List” means a cryptographically signed list of device capabilities, which are certified as correctly outlining the capabilities of the Licensee Product.

1.19. “Device Key” means an RSA private key, unique to the Licensee Product model, which is generated by the Licensee for the purpose of signing requests, and decrypting responses during Individualization.

1.20. “Device Model” means a group of Licensee Products which do not materially differ in the software, hardware, and methods used by Content Protection Functions. For avoidance of doubt, Licensee Products with differing model numbers or branding can be considered part of a single Device Model if their Content Protection Functions are materially the same.

1.21. “Digital Video Output” means connectors carrying digital signals for the purpose of immediate display on a Display Device include but are not limited to the digital interface portion of the Digital Visual Interface (DVI), the digital video interface portion of HDMI, or the digital video interface portion of DisplayPort.

1.22. “Display Device” means a device the primary purpose of which is to render audiovisual or sound content for immediate consumption by a viewer and/or listener.

1.23. “DRM Certificate” means a cryptographic Certificate issued by Adobe for each device Model, which includes Device Capabilities List.

1.24. “Flash Access” means, for the purposes of these Compliance and Robustness Rules, Adobe Flash Access, Adobe Access and Adobe Primetime DRM branded software licensed by Adobe.


1.26. “Individualization Transport Certificate” means a cryptographic Certificate issued by Adobe which is used to encrypt Individualization requests.

1.27. “Licensee” shall mean the licensee responsible for complying with these Compliance and Robustness Rules under the License Agreement, however such licensee is defined under the License Agreement.

1.28. “Licensee Product” shall mean any product incorporating Licensed Software and subject to compliance with these Compliance and Robustness Rules under the License Agreement, however such product is named under the License Agreement.

1.29. “Licensed Software” shall mean the software incorporating the Adobe Implementation licensed for distribution under the License Agreement, however such software is named
under the License Agreement.


1.31. “Machine Key” means an RSA public/private key pair which is acquired during Individualization, and is used to decrypt Content Keys contained in Content Licenses.


1.33. “Pass” means to direct Decrypted Content to flow to a local Display Device or to Outputs.

1.34. “Persistent Storage” means data storage which can retain data for an indefinite period of time after device is turned off or power is withdrawn.

1.35. “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 (i) professional tools that are made available on the basis of a non-disclosure agreement, or (ii) Circumvention Tools.

1.36. “Root Public Key” means a cryptographic value embedded in the Licensed Software by Adobe that is used to establish trust between a server and a client device containing the Licensed Software.

1.37. “Secure Clock” means a hardware real-time clock which cannot be set or re-set by the user.

1.38. “Sensitive Data” means data which could be used to circumvent Compliance Functions and/or bypass restrictions on Flash Access Protected Content or Decrypted Content, and hence must be protected against being revealed, modified, deleted, and/or used without authorization, including but not limited to software code, configuration files, and Sensitive Keys provided by Adobe or created by Partner.


1.40. “Session Key” means a symmetric Key used for purposes such as, but not limited to, encryption and decryption of data in a session.

1.41. “Specialized Tools” means specialized electronic or software tools that are widely available at a reasonable price, such as memory readers and writers, debuggers, decompilers, or similar software development products, but not including Circumvention Tools.

1.42. “Time-Based Rules” means content usage rules which are predicated on the current time, including Start Date, End Date, Relative End Date, License Caching Duration, and Playback Window.

1.43. “Transitory Image” means Decrypted Content that has been stored temporarily for the sole purpose of performing a process that is permitted by these Compliance and Robustness Rules, does not persist materially after such process has been performed, and is not stored in a way that permits copying or re-streaming in a usable form for other purposes.

1.44. “Widely Available Tools” means general purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips, file editors, soldering irons, and information gathered using search engines, but not including Circumvention Tools.

2. **Compliance Rules.** These Compliance Rules set forth mandatory requirements for Licensee and Licensee Products.

2.1. **Proper Implementation.**

2.1.1. **Consistent Implementation.** Licensee Products implementing Flash Access functionality must do so in a manner consistent with the Adobe Implementation. No modification shall be made to the Adobe Implementation except as specifically required to interoperate properly with the other software and hardware elements of the Partner Product and ensure compliance with these Compliance and Robustness Rules, and such modifications must not result in material differences in behavior or result when compared to the Adobe Implementation running on desktop personal computers such as the Flash Player for Windows, Mac, and Linux distributed by Adobe at http://get.adobe.com/flashplayer/. This includes retaining proper enforcement of all restrictions on usage of Flash Access Protected Content and Decrypted Content other than usage permitted by Content Licenses.

2.1.2. **No Circumvention.** Licensee Products must not, directly or indirectly, provide access to Flash Access Protected Content or Decrypted Content in any manner inconsistent with these Compliance Rules, or otherwise circumvent restrictions on usage or other limitations in Content Licenses associated with such Flash Access Protected Content.

2.1.3. **Architecture.** Licensee Products must contain and execute the Licensed Software entirely within a single physical end user device (such as but not limited to a portable or tablet computer, smartphone, set-top box), and must not allow third-party software applications to access Decrypted Content.

2.1.3.1. **No Unauthorized Exposure of Compliance Functions.** Licensee Products shall not expose the Compliance Functions of the Licensed Software for initiation of Decryption to third party software executed on the Licensee Product or any device connected to the Licensee Product.

2.1.3.2. **No Modification of APIs.** The Licensed Software shall not be modified so as to alter the behavior of any API or to make the functionality of the Licensed Software available to software applications other than licensee’s Licensee Product.

2.1.4. **Random Numbers.** Licensee Products must implement a random number generator that is cryptographically random for all calls to the ICrypto::GetRandomNumber() function.

2.2. **Decryption for Playback.**

2.2.1. **Decryption.** Licensee Products shall be designed to perform Decryption solely as part of a process executed in its entirety within an Adobe Runtime on a single hardware device, for the purpose of immediate passing of Decrypted Content for rendering on a Display Device.

2.2.2. **Output of Decrypted Content.** Licensee Products shall not Pass, or direct to be Passed, Decrypted Content to Outputs except in a manner consistent with Section 2.3 for the purpose of immediate rendering on a Display Device.

2.2.3. **No Re-streaming.** Licensee Products shall not re-stream, or enable the re-streaming of, the video portion of Decrypted Content, by sending the Decrypted Content to any device or storage medium other than to Pass to a Digital Video Output or Analog Video Output.

2.2.4. **No Copying.** Licensee Products shall not copy, or enable the copying of Decrypted Content. For the avoidance of doubt, the creation of a Transitory Image does not violate this restriction on copying.

2.2.5. **No Content Samples.**
2.2.5.1. **No Access Via APIs.** The Licensee Product shall not include an API through which access can be gained to extract and copy Content Samples either internally or externally. For the avoidance of doubt, this rule is not intended to prevent implementation of APIs to control playback.

2.2.5.2. **Persistent Storage.** Content Samples shall not be written to Persistent Storage in any form. Buffering or caching may only be performed for Flash Access Protected Content Samples prior to Decryption.

2.3. **Output Protection.** Licensed Products which have Outputs must detect and accurately respond to any output restrictions specified in Content Licenses.

2.3.1. **Video Outputs.** Partner Products may Pass video Decrypted Content to the following local Outputs:

2.3.1.1. **Analog Component Video Outputs.** Licensee Products may Pass the video portion of decompressed Decrypted Content to Analog Component Video Outputs if all the conditions in section 2.3.3 (Output to Analog Video Outputs) are met.

2.3.1.2. **Analog Computer Monitor Outputs.** Licensee Products may Pass the video portion of decompressed Decrypted Content to Analog Computer Monitor Outputs if all the conditions in section 2.3.3 (Output to Analog Video Outputs) are met.

2.3.1.3. **Analog Television Outputs.** Licensee Products may Pass the video portion of decompressed Decrypted Content to Analog Television Outputs if all the conditions in section 2.3.3 (Output to Analog Video Outputs) are met.

2.3.1.4. **Digital Video Outputs.** Licensee Products may Pass the video and/or audio portion of decompressed Decrypted Content to Digital Video Outputs if all the conditions in section 2.3.2 (Output to Digital Video Outputs) are met.

2.3.1.5. **WirelessHD Outputs.** Licensee Products may Pass the video and/or audio portion of decompressed Decrypted Content to WirelessHD Outputs if all the conditions in section 2.3.2 (Output to Digital Video Outputs) are met.

2.3.2. **Output to Digital Video Outputs.**

2.3.2.1. **Required.** If a Content License specified Output Protection as “Required” for Digital Video Outputs, then Decrypted Content may only be Passed to authorized Digital Video Outputs with an Authorized Digital Video Protection verifiably engaged.

2.3.2.2. **Use If Available.** If a Content License specifies that Output Protection is “Use If Available” for Digital Video Outputs, then an Authorized Digital Video Protection must be engaged if available before Passing to an Digital Video Output, but clear Decrypted Content may be Passed to Digital Video Outputs if an Authorized Digital Video Protection is not available for the Output.

2.3.2.3. **No Protection.** If a Content License specifies that Output Protection is “No Protection” for Digital Video Outputs, then clear Decrypted Content may be Passed to Digital Video Outputs without restriction.

2.3.2.4. **No Playback.** If a Content License specifies “No Playback” for Digital Video Outputs, then Decrypted Content may not be Passed to any Digital Video Output.

2.3.3. **Output to Analog Video Outputs.**
2.3.3.1. **Required.** If a Content License specified Output Protection as “Required” for Analog Video Outputs, then Decrypted Content may only be Passed to authorized Analog Video Outputs with an Authorized Analog Video Protection verifiably engaged.

2.3.3.2. **Use If Available.** If a Content License specifies that Output Protection is “Use If Available” for Analog Video Outputs, then an Authorized Analog Video Protection must be engaged if available before Passing to an Analog Video Output, but clear Decrypted Content may be Passed to Analog Video Outputs if an Authorized Analog Video Protection is not available for the Output.

2.3.3.3. **No Protection.** If a Content License specifies that Output Protection is “No Protection” for a Analog Video Outputs, then clear Decrypted Content may be Passed to Analog Video Outputs without restriction.

2.3.3.4. **No Playback.** If a Content License specifies “No Playback” for Analog Video Outputs, then Decrypted Content may not be Passed to any Analog Video Output.

2.4. **Certificates.** Licensee shall not use certificates issued by parties other than Adobe to substitute for Certificates when using the functionality of the Licensed Software.

2.4.1. **DRM Certificates.** DRM Certificates must be unique for each Device Model of Licensee Products. If a Licensee Product undergoes a major hardware or firmware revision, then a separate DRM Certificate must be used for the new Device Model.

2.4.2. **Distribution of Certificates.** Certificates shall not be distributed to any entity other than the entity for which Adobe issued them, except (i) to an Authorized Contract Manufacturer in a manner consistent with the License Agreement, or (ii) as integrated into Partner Product.

2.5. **Keys.** Licensee shall comply with the following restrictions on actions involving Keys.

2.5.1. **No Extraction of Content Encryption Keys.** A Licensee shall not extract a Content Encryption Key (or data from which a Content Encryption Key could be decrypted or derived) and separately record, transcribe, reproduce or disseminate such Content Encryption Key or data in any form.

2.5.2. **No Modification or Replacement of Root Public Key.** The Root Public Key embedded in the Adobe Implementation by Adobe shall not be modified or replaced.

2.5.3. **No Modification or Replacement of Individualization Transport Certificate.** The Individualization Transport Certificate provided by Adobe shall not be modified or replaced.

2.5.4. **No Private Key Distribution.** Licensee shall not distribute a Private Key to another entity in any form, except as integrated into a Licensee Product consistent with the Robustness Rules (Section 3).

2.6. **Time-Based Rules.** Time-Based Rules must be enforced based on the current device time as reported by a Secure Clock or Anti-Rollback Clock.

2.6.1. **License State.** License State must be treated as Sensitive Data, and persisted without modification.
2.6.2 Secure Clock or Anti-Rollback Clock must be designed to maintain time accurately with clock drift not to exceed five (4) minutes per month, and maintain a minimum resolution of one (1) second.

2.7 Secure Handling of Highly Confidential Information. Licensee shall comply with the following requirements concerning access to and handling of Highly Confidential Information (Sensitive Data and Sensitive Keys), except when such Sensitive Data and Sensitive Keys are encrypted and protected for distribution with Licensed Products to end users in final form:

(i) Highly Confidential Information shall be stored and used only at Authorized Sites. The rooms within the Authorized Sites in which Highly Confidential Information is stored or used must at all times be secured by lock and key, electronic card access or similar measures, and access-controlled, such that a verifiable log of all those having access to, and the times of entering and leaving such rooms is created and preserved for a minimum of one year.

(ii) Only Authorized Employees shall have access to copies of Highly Confidential Information in permanent or temporary storage of any kind. The use of the Highly Confidential Information by the Authorized Employees shall be strictly limited to the purpose of the License Agreement under which Licensee develops and distributes Licensed Products.

(iii) When not in use, Authorized Employees shall permanently store the Highly Confidential Information only in a safe or password protected computer accessible only to Authorized Employees. Authorized Employees may remove or copy Highly Confidential Information from such permanent storage and make temporary copies onto computers or devices located within the Authorized Facilities as needed for the purposes contemplated by the License Agreement, provided that when the Highly Confidential Information is stored on such a computer or device, such computer or device shall be secure and password-protected. Authorized Employees must have a separate unique, non-trivial, non-obvious password for each permanent or temporary storage location that is changed with reasonable frequency in accordance with industry best practices. Licensee shall maintain and take reasonable security measures to preserve the integrity of log records recording the date and time at which keys are copied to or deleted from each temporary computer or device and permanent storage site, and the identify of the Authorized Employee performing such deletion or copying, such that an auditor examining such records can determine the number and location of all copies of Sensitive Keys at any point in time over the previous two years.

(iv) Authorized Employees must adhere to a “clean desk” policy at their facilities at an Authorized Site. “Clean desk” policy means the Highly Confidential Information must be completely and permanently deleted from any computer or device and stored consistent with 2.8(iii) when not in use.

(v) Licensee shall not let the Highly Confidential Information be viewed, used, copied, disseminated, or in any way circulated to any individual other than to Authorized Employees.

(vi) Adobe may inspect the Authorized Sites to verify compliance with the provisions of this Section 2.8 upon reasonable notice to Licensee, and in compliance with the reasonable policies of such Licensee relating to access.
2.8. **Distribution of Compliance and Robustness Rules.** Licensee shall provide a copy of these Compliance and Robustness Rules to each person involved in or responsible for development and testing of Licensee Products, or who handles any Sensitive Data or Sensitive Keys.

3. **Robustness Rules.** These Robustness Rules set forth mandatory processes and standards of protection for Licensee Products to prevent the compromise of the Compliance Functions and to maintain the integrity and security of Sensitive Keys and Sensitive Data.

3.1. **Construction.** Licensee Products shall be designed and manufactured in a manner clearly designed to effectively frustrate attempts to modify the behavior or the performance of Compliance Functions, or to discover, reveal, extract, modify or replace Sensitive Keys or Sensitive Data.

3.2. **Prohibited functions.** Licensee Products shall not include: switches, buttons, jumpers or software equivalents thereof, specific traces (electrical connections) that can be cut, or functions (including but not limited to secret resets, service menus and remote-control functions or keyboard, command or keystroke bypass), debuggers or debugging aids, in each case by which the Compliance Functions can be defeated.

3.3. **Extraction of Content Samples.** Licensee Products shall be designed and manufactured in a manner clearly designed to effectively frustrate attempts to extract or use Content Samples in a manner not specifically allowed by the associated Content License.

3.4. **Method of making functions robust.** Licensee Products shall be manufactured using at least the following techniques in a manner that is clearly designed to effectively frustrate attempts to defeat the requirements set forth below.

3.4.1. **Software.** Any portion of a Licensee Product that implements in software (meaning any computer program code consisting of instructions or data, other than such instructions or data that are included in Hardware) any of the Compliance Functions shall include all of the characteristics set forth in Sections 3.1 and 3.2 above. Such software portions shall also:

3.4.1.1. Protect against attempts to discover, extract, reveal, modify or replace Sensitive Keys or Sensitive Data by a reasonable method including but not limited to:
- encryption, execution of a portion of the implementation in ring zero or supervisor mode (i.e., in kernel mode) which users are not authorized to access, and/or
- embodiment in a secure physical implementation that effectively isolates Sensitive Keys and Sensitive Data from exposure by mere use of programming instructions or data (e.g., by using the values only inside a secure processor); and, in addition, using techniques of obfuscation and/or cryptographic whiteboxing technologies clearly designed to effectively disguise and hamper attempts to discover the approaches used, such that Sensitive Keys shall never exist in contiguous cleartext memory during software execution, except in dedicated decryption hardware, in cleartext in object code, or in cleartext in user accessible storage; and

3.4.1.2. Be designed so as to perform or ensure checking of the integrity of its component parts such that unauthorized modifications will be expected to result in a failure of the implementation to provide Decryption. For the purpose of this provision, a “modification” includes any change in, or disturbance or invasion of, features or characteristics, or interruption of processing, relevant to the requirements of these Robustness Rules. This provision requires at a minimum the use of signed...
code or a robust means of runtime integrity checking operating throughout the code.

3.4.2. Hardware. Any portion of a Licensee Product that implements in Hardware (meaning a physical device, including a component, that (i) does not include instructions or data other than such instructions or data that are permanently embedded in such device or component; or (ii) includes instructions or data that are not permanently embedded in such device or component where such instructions or data have been customized for such Licensee and/or can only be accessed under the control of the Licensee by authorized parties) any of the Compliance Functions shall include all of the characteristics set forth in Sections 3.1 and 3.2 above. Such products shall also be designed such that attempts to remove, replace, or reprogram Hardware elements in a way that would compromise the Compliance Functions or the integrity and security of Sensitive Keys and Sensitive Data would pose a serious risk of rendering the Licensee Products unable to Decrypt Flash Access Protected Content [or Output Decrypted Content]. By way of example, (i) a component that is soldered rather than socketed, or affixed with epoxy, or (ii) checking a signature on updateable firmware within a secure boot loader may be appropriate.

3.5. Level of Protection.

3.5.1. Protection of Highly Sensitive Keys and Data: Licensee Products shall be designed in a method clearly designed to protect against disclosure and unauthorized use or manipulation of Highly Sensitive Keys and Highly Sensitive Data including but not limited to DRM Keys, Machine Keys, and Individualization Transport Keys:

3.5.1.1. cannot be defeated or circumvented merely by using Widely Available Tools or Specialized Tools, and

3.5.1.2. can only with difficulty be defeated or circumvented using Professional Tools.

3.5.2. Protection of Sensitive Data: Licensee Products shall be designed in a method clearly designed so that (i) compliance with the requirements of Section 3.3 in the case of uncompressed Content Samples, (ii) protection against the disclosure or unauthorized use of Sensitive Data including but not limited to Content Encryption Keys, (iii) enforcement and behavior of Compliance Functions consistent with the Adobe Implementation, and (iv) binding of Machine Keys to a specific unit of Licensee Product;

3.5.2.1. cannot be defeated or circumvented merely by using Widely Available Tools; and

3.5.2.2. can only with difficulty be defeated or circumvented using Specialized Tools or Professional Tools.

3.6. Advance of Technology. Although a Licensee Product when designed and first shipped may meet the above standards, subsequent circumstances may arise which, had they existed at the time of design of such product, would have caused such product to fail to comply with these Robustness Rules (“New Circumstances”). If Licensee becomes aware of such New Circumstances, Licensee shall promptly give notice of such New Circumstances to Adobe, then within eighteen (18) months of such notice shall cease distribution of such Licensee Product and shall only distribute Licensee Products that are compliant with the Robustness Rules in view of the then-current circumstances.