



PSLT- Adobe Primetime Cloud Multi-DRM: Powered By ExpossPlay (2017v1)

1. Additional Licenses.

- 1.1 **Access to the On-demand Service.** Adobe will, on a non-exclusive basis during the License Term, allow Customer to access and use the On-demand Service. Customer may use the On-demand Service only for the purpose of allowing Consumers to obtain Content Licenses for Protected Content and Managed Content.
- 1.2 **On-premise Software.** Adobe grants to Customer a non-exclusive, non-transferable, license to install and use the On-premise Software in accordance with the Documentation for the purpose of creating, protecting and distributing Protected Content via a Customer Player and creating Content Policies for Customer's own account.

2. License Restrictions and Customer's Obligations.

- 2.1 **Transaction Volume Increases.** Customer will notify Adobe, and Adobe will notify ICSC, for those periods during which Customer believes that the initial transaction volume thresholds provided in the Sales Order will be exceeded by more than 200%, and will provide Customer's best estimate of whether and when such periods will recur.

2.2 Adobe Access DRM Restrictions and Obligations.

- (A) **Adobe Access Compliance and Robustness Rules; Verification Rights.** Customer must ensure that the Licensed Product complies with the Adobe Access Compliance and Robustness Rules at all times. If Adobe posts changes to the Adobe Access Compliance and Robustness Rules, Customer is required to comply with such changes as soon as commercially practicable, but in any event no later than six months after the date the changes were posted. Customer is responsible for checking the web site listed in section 9.2 of this PSLT periodically to be aware of any changes. Adobe will send notice of the change(s) to the designated Certificate Administrator (as last provided by Customer), and notice will be considered received upon delivery to a properly addressed email. Lack of receipt of such notification will not exempt Customer from the obligation to comply with the then-current rules within the required period. Adobe's right of audit under the License Compliance section of the General Terms Adobe may also inspect of Customer's books, records, procedures and facilities necessary to verify Customer's compliance with the Adobe Access Compliance and Robustness Rules.
- (B) **Prohibited Use.** Except as expressly authorized under this PSLT, Customer is prohibited from using the On-demand Service or On-premise Software to (i) create or maintain a License Server, or to create or generate Content Licenses; or (ii) protect any other formats or media other than Content.
- (C) **Content Protection Updates.** If Adobe delivers a Content Protection Update to Customer, Customer will apply such update to the On-premise Software, and discontinue using copies of the On-premise Software that have not been updated, as soon as reasonably possible and will provide notice to Adobe if this will take more than 90 calendar days.

- (D) **Use of Current Certificate.** Each Certificate for commercial use will expire two years from the date it is generated by Adobe. Each Certificate for evaluation use will expire one year from the date it is generated by Adobe. Customer will be required to place an order for new Certificates, as needed.
- (E) **No Circumvention.** No element of the On-demand Service or the On-premise Software may be used to circumvent or defeat the Content Protection Functions or other security requirements of the On-demand Service or the On-premise Software and related technical specifications, provided hereunder. Customer will not (i) use Confidential Information or Highly Confidential Information to circumvent the Content Protection Functions of either the On-demand Service or the On-premise Software or any related Adobe technology that is used to encrypt or decrypt digital content for authorized consumption by users of the On-premise Software or On-demand Service; or (ii) develop or distribute products that are designed to circumvent the Content Protection Functions of the On-demand Service or the On-premise Software or the content protection functions of any related Adobe technology that is used to encrypt or decrypt digital content for authorized consumption by users of the On-demand Service or the On-premise Software.
- (F) **Open Source Software.** Customer will not directly or indirectly grant, to any third party any rights or immunities to Adobe's intellectual property or proprietary rights in the On-premise Software that will subject the On-premise Software to an open source license or scheme that requires, or could be interpreted as requiring, as a condition of use, modification and/or distribution of such open source software, that the On-premise Software be: (i) disclosed or distributed in source code form; (ii) licensed for the purpose of making derivative works; or (iii) redistributable at no charge. Any violation of the foregoing provision will immediately terminate all of Customer's licenses and other rights to the On-premise Software granted under the Agreement.
- (G) **Confidential Treatment of Content Encryption Keys.** Content Encryption Keys are Confidential Information. However, Customer will have no further responsibility for Content Encryption Keys that have been distributed to Consumers in Content Licenses.

2.3 Microsoft PlayReady Restrictions and Obligations.

- (A) Customer's right and license to use PlayReady through the On-demand Service is subject to (i) Customer providing Adobe an accurately-filled out version of Appendix A prior to Adobe's commencement of its provision of PlayReady through the On-Demand Service to Customer; (ii) Customer promptly revising the current version of Appendix A as necessary to render it complete and accurate at all times; and (iii) Microsoft consenting to Customer's use of PlayReady through the On-demand Service, which such consent Microsoft may withhold or withdraw at any time, without prior notice, in Microsoft's sole discretion, and which shall be subject to suspension in Microsoft's discretion. Customer shall provide Adobe any other items of information as Microsoft may require in order to grant such consent, and consents to Adobe's transmittal of such information to its suppliers of PlayReady, and by those entities to Microsoft. Adobe does not guarantee that Microsoft shall consent to providing PlayReady to Customer, either at all or for any period of time, and disclaims any liability related to Microsoft's determination not to consent to Customer's use of PlayReady through the On-Demand Service or to Microsoft's withdrawal of any such consent previously given.
- (B) All of Customer's use of PlayReady through the On-demand Service must comply at all times with the PlayReady Compliance Rules then in effect. If and when the PlayReady Compliance Rules are modified by Microsoft, Customer must promptly take such actions, if any, as shall be necessary to bring its Customer Service(s) into compliance with such modified PlayReady Compliance Rules. Customer shall at all times maintain documentation detailing how its Customer Service(s) conform to the current PlayReady Compliance Rules, and provide such documentation to Adobe within two Business Days of Customer's receipt of a request from Adobe for such documentation. Customer

grants Adobe the right to share such documentation with its suppliers of PlayReady services and for those entities to share that documentation with Microsoft.

- (C) If Customer uses PlayReady through the On-demand Service, Customer must post the following notice within the terms of use that apply to its websites and Customer Services:

Content owners use Microsoft PlayReady™ content access technology to protect their intellectual property, including copyrighted content. This service uses PlayReady technology to protect certain content. If the PlayReady technology fails to protect the content, content owners may require the service to restrict or prevent the delivery of protected content to specified devices or PC software applications. In certain cases, you may be required to upgrade the PlayReady technology to continue to access the service's content. If you decline such an upgrade, you will not be able to access content that requires the upgrade.

- 2.4 **MTMO Restrictions.** Customer acknowledges that, in delivering the service, Adobe and its suppliers are obligated to implement MTMO security directives which may restrict devices from rendering Marlin Managed Content.

3. Additional Terms for Highly Confidential Information and Authentication Credentials.

- 3.1 **Handling of Highly Confidential Information.** Private Keys for Adobe Access DRM are subject to requirements applicable to Highly Confidential Information contained in the Adobe Access Compliance and Robustness Rules and any updates thereto, together with the following provisions (the “**Security Requirements**”).

- (A) All Authorized Employees must sign, or have signed, confidentiality agreements with Customer containing terms at least as restrictive as those in this Section 3.1 and the Security Requirements, either as a condition of their employment or before they are granted access to the Highly Confidential Information. Customer will ensure that all Authorized Employees are made aware of their obligation to comply with the Security Requirements. Customer will promptly provide Adobe with copies of such confidentiality agreements signed by the Authorized Employees, if requested as part of any security verification permitted under section 2.1, above. Customer is fully responsible for the conduct of its employees (including Authorized Employees) who may in any way breach this PSLT. Customer will, upon request of Adobe, take all reasonable steps necessary to recover any Highly Confidential Information and will bear the cost of such steps. Customer agrees to notify Adobe in the event of any breach of the terms of this section 3.1(A) including breaches in its security. Customer must cause each Authorized Employee to strictly abide by their obligations under this section 3 and the Security Requirements. Customer must use the same efforts to enforce the confidentiality obligations of each Authorized Employee after the termination of his/her employment as Customer uses to enforce its own confidential information, such efforts of enforcement not to be less than reasonable efforts.
- (B) Without limitation to any requirement of this section 3.1(B) and the Security Requirements, Customer agrees that it will treat the Highly Confidential Information with at least the same degree of care as it gives to the protection of its most sensitive confidential information, if any, and Customer represents that it exercises at least a high degree of care to protect its own sensitive confidential information.
- (C) Customer’s obligations with respect to the Highly Confidential Information are in effect in perpetuity. Customer's obligations not to disclose Highly Confidential Information will not be subject to any of the exceptions set forth in the section containing the definition of Confidential Information or the Confidentiality section of the General Terms, with the exception of the sub-

section titled Permitted Disclosure under the Confidentiality section of the General Terms regarding disclosure required by law or the order of a court or similar judicial or administrative body.

3.2 Commercial DRM Authentication Credentials. Customer must securely store and protect all Authentication Credentials from unauthorized disclosure or use. Customer shall be responsible for all actions taken by any person who uses Customer's Authentication Credentials to interact with the On-demand Service, including when those Authentication Credentials are used without authorization. In the event that Customer's Authentication Credentials are lost, stolen, or otherwise used without authorization, Customer shall be responsible for changing its Authentication Credentials using its ExpressPlay account in the On-Demand Service to prevent further unauthorized activity.

3.3 Content Keys. Customer will covenant that it will use commercially reasonable methods to prevent unauthorized access, disclosure or distribution of Content Keys.

4. Adobe Access Certificate Administration. Customer must provide Adobe with the name of one employee to serve as the "**Certificate Administrator**" responsible for administering the names of those Authorized Employees of Customer who are permitted to request Certificates from Adobe on behalf of the Customer. No Certificates will be delivered until a Certificate Administrator has been designated and Authorized Employees have been identified. The Certificate Administrator is prohibited from requesting Certificates. Customer may update the name of the Contract Administrator from time to time during the Term, but no more than 3 times in a 12-month period, unless expressly approved by Adobe.

5. Remedies, Revocation, and Suspension.

5.1 Revocation of Certificates. Adobe will have the right to take measures to revoke Certificates issued to Customer if Adobe obtains or becomes aware of evidence satisfactory, in Adobe's sole discretion, to establish that one or more of the following criteria are met:

- (A) such Certificate or the Public Key associated with it is being used without authorization by a party other than the Customer to which it was issued by Adobe;
- (B) the Private Key corresponding to a Public Key for which Adobe has issued a Certificate has been made public, lost, stolen, intercepted or otherwise misdirected, disclosed;
- (C) revocation has been ordered by a court or similar judicial or administrative body of any government;
- (D) the PSLT has expired or been terminated by either party; or
- (E) Customer has requested or consented in writing to such expiration.

5.2 Revocation Process. If Adobe determines that any of the prior criteria have been met, Adobe will take reasonable steps to consult with Customer prior to initiating such revocation to determine if Customer can present evidence satisfactory to Adobe, in Adobe's sole discretion, that the relevant criteria have not been met and/or that revocation is not necessary to prevent any material compromise to the security of Protected Content or of the Content Protection Functions of the On-premise Software, or the content protection capabilities of any other Adobe licensed software as applied to any digital content. Adobe will not initiate such revocation prior to 30 days following notice of such consultation unless Adobe determines, in its sole discretion, that immediate or earlier revocation is necessary to mitigate ongoing and material harm to the interests of distributors of digital content protected using Adobe licensed software.

5.3 Injunctive Relief. In addition to the Injunctive Relief section of the General Terms, Customer agrees that certain breaches of this PSLT, including but not limited to breaches of sections 2, 3.1 and 4, of

this PSLT and breaches of the Adobe Access Compliance and Robustness Rules, may compromise the Content Protection Functions of the On-premise Software and cause unique and lasting harm to the interests of Adobe and owners of Content that rely on such Content Protection Functions, and that monetary damages will be inadequate to compensate fully for such harm. Therefore, Customer further agrees that Adobe will be entitled to obtain timely injunctive relief to prevent or limit the harm caused by such breaches, in addition to monetary damages or other remedies available at law.

5.4 **Suspension; Termination of Commercial DRM access.**

(A) **MTMO and Commercial DRM Provider Events.** Adobe may suspend its provision of, and Customer's right to use some or all of the On-demand Service or terminate the Customer Agreement in the event that a provider of a Commercial DRM (i) terminates any relevant agreement it has with ICSC or any of its Affiliates (such as the Marlin Service Provider Agreement) or (ii) withdraws any right necessary for ICSC or any of ICSC's Affiliates to provide any of the On-demand Service to Customer.

(B) **Suspension of Adobe's Provision of the On-Demand.** Adobe may suspend its provision of some or all of the On-demand Service on one (1) days' notice in the event that Customer breaches its obligations under sections 2.3 of this PSLT. If Customer's breaches of sections 2.3(A) or 2.3(B) of this PSLT are not cured within thirty (30) days of Customer's receipt of the foregoing notice, Adobe may terminate the Agreement pursuant to the Termination for Cause section of the General Terms.

6. **Additional Warranties.** Customer represents, warrants that it has entered into and will comply with all agreements required by the Commercial DRM providers for the Commercial DRMs that Customer accesses via the On-demand Service, and all such agreements will remain in full force and effect for so long as they are applicable.

7. **Changes to Commercial DRM.** Customer acknowledges that Adobe may amend the Agreement on thirty (30) days' notice at any time as necessary to reflect changes due to (A) third party license obligations, including required changes to the content protection technologies; or (B) Adobe or ICSC's loss of rights to provide certain DRM technologies as part of the On-demand Service.

8. **Third Party Beneficiary.** Customer acknowledges that ICSC is an intended third party beneficiary of the Agreement to the extent applicable to the Commercial DRM and the On-demand service and ICSC may enforce the terms relating to Commercial DRM and corresponding use of such DRM in the On-demand Service directly against Customer regardless of the extent to which Adobe may or may not have previously undertaken to enforce the terms of the Agreement.

9. **Definitions.**

9.1 **"Ad(s)"** means a graphic or multi-media file served in adjacent to or otherwise in connection with Customer Content, including, without limitation, overlays, companion banners, pre-roll/mid-roll/post-roll, video and display.

9.2 **"Adobe Access Compliance and Robustness Rules"** means the document setting forth compliance and robustness rules for the use of the On-premise Software and Certificates located at <http://www.adobe.com/go/FlashAccessComplianceandRobustnessRules> or a successor web site thereto.

9.3 **"Adobe Access DRM SDK"** means:

- (A) the SDK and documentation provided to Customer by Adobe under this PSLT that combines Object Code, Sample Source and Certificates for the sole purposes of creating Protected Content, Content Licenses and Content Policies in conjunction with the On-demand Service;
 - (B) any updates and fix releases thereto that Adobe may provide to Customer under this PSLT; and
 - (C) any other documentation or source or object code provided by Adobe under this PSLT that is intended to assist Customer in development of the Licensed Product.
- 9.4 **“Adobe Primetime TVSDK”** means Adobe’s proprietary SDK for creating desktop and mobile application players of Content and Ads, licensed under a separate written terms.
- 9.5 **“Apple”** means Apple Inc. and its affiliates.
- 9.6 **“Authentication Credentials”** means a credential generated by any of the Commercial DRM and that is provided to Customers to submit to the On-demand Service so that the On-demand Service may confirm the authenticity of a request for acquisition of a secure instruction.
- 9.7 **“Authorized Employees”** means only the individuals authorized to place or approve orders for Certificates through the online registration process for Certificate ordering described in the Documentation, all of whom must at all times be full-time employees of Customer with a strict need to have access to Highly Confidential Information in order to perform Customer’s obligations or exercise Customer’s rights under this PSLT.
- 9.8 **“Authorized Site(s)”** means those Customer owned or controlled sites identified in a Sales Order where Customer may use and store Highly Confidential Information, subject to the terms of this PSLT and the General Terms.
- 9.9 **“Certificates”** means electronic documents provided by Adobe for the use with Adobe Access DRM under this PSLT that incorporate a digital signature that associates a public key with an entity (including server, client) and can be used to establish a chain of trust.
- 9.10 **“Certificate Revocation List (or CRL)”** means electronic documents published by Adobe to identify Certificates that are no longer valid, having been revoked by Adobe.
- 9.11 **“Commercial DRM”** means FairPlay Streaming, Marlin, PlayReady and/or Widevine Modular, as applicable.
- 9.12 **“Consumer”** means an individual end user that receives Protected Content or Managed Content and obtains a Content License in order to obtain access to and view the Protected Content or Managed Content on a supported Customer Player.
- 9.13 **“Content”** for the purposes of this PSLT, means audio, video, multimedia, text, images, documents, computer programs, data and any other information or materials. The definition of Content does not include Ads.
- 9.14 **“Content Encryption Key”** means a cryptographic value for use in encrypting Customer Content for secure distribution and for use by Customer Player to decrypt Protected Content for access and use in accordance with a Content License.
- 9.15 **“Content Key”** means the cryptographic key required to decrypt Managed Content.
- 9.16 **“Content License(s)”** means metadata (stored on a computer and/or embedded in an electronic file delivered to a Customer Player) that:

- (A) contains an encrypted Content Encryption Key for the corresponding DRM client technology; and
- (B) which may contain or refer to usage rules for Protected Content or Managed Content designed to be enforced directly through the corresponding DRM client in the Customer Player.
- 9.17 **“Content Policy”** means metadata that contains usage rules for Protected Content.
- 9.18 **“Content Protection Functions”** means those aspects of the On-premise Software that are designed to implement requirements of the Adobe Access Compliance and Robustness Rules and/or prevent unauthorized access to Private Keys, Content Encryption Keys and Certificates or unauthorized access to or use of Protected Content inconsistent with the access and usage rules contained in a Content License or Content Policy associated with such Protected Content.
- 9.19 **“Content Protection Update”** means an update to the On-premise Software that is designated as such by Adobe because it alters the prior means for providing the Content Protection Functions in the On-premise Software.
- 9.20 **“Customer Content”** for the purposes of this PSLT, means HDS and HLS audio, video or data Content that is:
- (A) made available or provided by Customer and/or other third parties or
- (B) is uploaded by or on behalf of Customer in connection with Customer’s use of the On-demand Services, in each case to be distributed on or through the Customer Player.
- 9.21 **“Customer Player”** means the video player(s) that Customer creates using the Adobe Primetime TVSDK under a valid license from Adobe.
- 9.22 **“Customer Service”** means a Customer service that utilizes the On-demand Service to deliver Managed Content to a Customer Player.
- 9.23 **“Deliver or Delivery”** means to deliver or otherwise make available, directly or indirectly, by any means, Protected Content to one or more Consumers.
- 9.24 **“DRM Metadata”** means a data structure that contains the URL of a License Server and may contain the encrypted Content Encryption Key and/or a Content Policy.
- 9.25 **“DRM Technology”** means certain technology which enables the distribution of Managed Content, and which consists of a particular combination of intellectual property, specifications, software, services, implementation requirements, and commercial license agreement rights and obligations.
- 9.26 **“FairPlay Streaming”** means the DRM Technology licensed by Apple.
- 9.27 **“Google”** means Google Inc. and its affiliates.
- 9.28 **“Highly Confidential Information”** means Private Keys generated and controlled by the Customer for the purpose of creating Protected Content or issuing Content Licenses, using the On-premise Software.
- 9.29 **“ICSC”** means Intertrust Cloud Services Corporation.
- 9.30 **“License Server”** means a server that generates and issues Content Licenses.
- 9.31 **“Managed Content”** means content that is distributed, used and/or otherwise governed in accordance with the requirements of a Commercial DRM.

- 9.32 **“Marlin”** means the DRM Technology licensed by the MTMO.
- 9.33 **“Marlin Service Provider Agreement”** means the Marlin Service Provider Agreement Version 2.0 published March 9, 2011 by MTMO, as amended.
- 9.34 **“Microsoft”** means Microsoft Corporation and its affiliates.
- 9.35 **“MTMO”** means the Marlin Trust Management Organization, LLC.
- 9.36 **“On-demand Service”** means the Adobe Primetime Cloud Multi-DRM hosted service that through the use of one or more Commercial DRMs or Adobe Access DRM, as applicable, (A) registers a Marlin device, (B) fulfills Customer Player requests for acquisition of secure instructions, (C) issues a Content License and (D) issues a device a license to use Managed Content and/or an applicable Content Key.
- 9.37 **“On-premise Software”** means the Adobe Access DRM SDK software.
- 9.38 **“PlayReady”** means the DRM Technology licensed by Microsoft.
- 9.39 **“PlayReady Compliance Rules”** means Microsoft’s then-effective compliance rules for users of PlayReady technology. The PlayReady Compliance Rules are available, as of the Effective Date, at <http://www.microsoft.com/PlayReady/Licensing/compliance.mspx>.
- 9.40 **“Private Key”** means a cryptographic value generated by the Customer and uniquely associated with a Public Key.
- 9.41 **“Protected Content”** means Customer Content encrypted by a Content Encryption Key.
- 9.42 **“Public Key”** means a cryptographic value generated by the Customer and uniquely associated with a Private Key that is incorporated into a Certificate issued by Adobe when Customer follows the Certificate generation process described in the Documentation.
- 9.43 **“Register”** means to issue cryptographically secure digital credentials which represents a Consumer.
- 9.44 **“Widevine Modular”** means the DRM Technology licensed by Google.

Appendix A

**Trademarks under which Customer Services
that Utilize PlayReady shall Operate**

Customer Name:

**Trademarks Under Which Customer
Services That Utilize PlayReady Shall
Operate:**

This statement is accurate and complete as of _____, 201_.

CUSTOMER

By:

Name:

Title:
