ADOBE PDM – Adobe Primetime DRM (2014v2)

Products described in this PDM are governed by the terms of this PDM, the Sales Order, the General Terms, and the Exhibit for On-premise Software. As used in this PDM, On-premise Software means the Adobe Primetime DRM, which provides a scalable, efficient workflow to help Customer deliver and protect premium video across desktop, mobile devices, and platforms.

1. Description. Adobe Primetime DRM (fka – Adobe Access) includes:

1.1 the software development kit and documentation provided to Customer by Adobe under this Agreement that combines Object Code, Sample Source and Certificates for the sole purposes of creating Protected Content, Content Licenses and Content Policies;

1.2 any updates and fix releases thereto that Adobe may provide to Customer under this Agreement; and

1.3 any other documentation or source or object code provided by Adobe under this Agreement that is intended to assist Customer in development of the Licensed Product.

2. Additional Definitions

2.1 "**Account**" means a billing account for Customer's multi-channel and on-demand video delivery service.

2.2 "**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.

2.3 "**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 Agreement.

2.4 "**Authorized Site(s)**" means those Developments Site(s) identified in a Sales Order that may use and store Highly Confidential Information, subject to the terms of this PDM and the General Terms.

2.5 "**Adobe Primetime Offline Packagers**" means Adobe's proprietary software that packages MP4 and TS files for HDS streaming or HLS streaming and supports (i) Content protection using Adobe Primetime DRM (subject to a valid license) and Adobe Primetime Protected Streaming (subject to a valid license), and (ii) Adobe Primetime Ad Insertion in Customer Content. For the avoidance of doubt, Adobe Primetime DRM and Adobe Primetime Protected Streaming are not permitted under this PDM.

2.6 "**Adobe Primetime Live Packagers**" means Adobe's proprietary software that translates MPEG-TS broadcast feeds for HDS streaming or HLS streaming and supports (i) Content protection using Adobe Primetime DRM and Adobe Primetime Protected Streaming (subject to a valid license), and (ii) Adobe Primetime Ad Insertion in Customer Content.

2.7 "**Adobe Primetime Player SDK**" means Adobe's proprietary SDK for creating desktop and mobile application video players.

2.8 "**Certificates**" means electronic documents provided by Adobe pursuant to this Agreement 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.

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

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

2.11 "**Consumer**" means an individual end user that receives Protected Content and obtains a Content License in order to obtain access to and view the Protected Content on a supported Customer Player.

2.12 "**Content**" means any and all audio, video, multimedia, text, images, documents, computer programs, data and any other information or materials. The definition of Content does not include Ads.

2.13 "**Content Encryption Key**" means a cryptographic value for use in encrypting Content for secure distribution and for use by Customer Player to decrypt Protected Content for access and use in accordance with a Content License.

2.14 "**Content License(s)**" means metadata (stored on a computer and/or embedded in an electronic file delivered to an Customer Player) that (i) contains an encrypted Content Encryption Key and (ii) contains or refers to usage rules for Protected Content designed to be enforced directly through the Adobe Primetime DRM technology incorporated into Customer Player.

2.15 "**Content Policy**" means metadata that contains usage rules for Protected Content.

2.16 "**Content Protection Functions**" means those aspects of the On-premise Software that are designed to implement requirements of the 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.

2.17 "**Customer Content**" means HDS and HLS audio, video or data that is (i) made available or provided by Customer and/or other third parties or (ii) is uploaded by or on behalf of Customer in connection with Customer's use of the On-demand Services (as defined in the Exhibit for On-demand Services), in each case to be distributed on or through the Customer Player.

2.18 "**Customer Player**" means the video players that Customer created using the Adobe Primetime Player SDK under a valid license from Adobe.

2.19 "**Deliver**" or "**Delivery**" means to deliver or otherwise make available, directly or indirectly, by any means, Protected Content to one or more Consumers.

2.20 "**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.

2.21 "**Highly Confidential Information**" means Private Keys generated and controlled by the Customer for the purpose of creating Protected Content or issuing Content Licenses.

2.22 "**License Server**" means that portion of a Licensed Product that generates and issues Content Licenses.

2.23 "**Licensed Product**" means the software solution for creating Protected Content, Content Licenses and Content Policies developed by Customer using the On-premise Software.

2.24 "**Packager**" means a software utility that can create Protected Content and DRM Metadata that is derived from, or provided with, the On-premise Software, including the Adobe Online Packager and the Adobe Offline Packager.

2.25 "**Private Key**" means a cryptographic value generated by the Customer and uniquely associated with a Public Key.

2.26 "**Protected Content**" means Customer Content encrypted by a Content Encryption Key using a Packager.

2.27 "**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

2.28 "**Root License(s)**" means metadata (stored on a computer and/or embedded in an electronic file delivered to Customer Player) that grants access to any number of cryptographically linked Content Licenses which in turn grants access to content protected by the Content Encryption Key contained within each Content License. Each Root License is cryptographically linked to each device by an encryption key unique to each device.

3. Additional Licenses and Restrictions. The following additional license restrictions apply to the On-premise Software described in this PDM:

3.1 **Licensed Product**. Customer may use the On-premise Software solely to develop and use the Licensed Product for the purpose of protecting and distributing Protected Content to a Customer Player, Content Policies and Content Licenses for Customer's own account.

3.2 **Evaluation and Testing**. If the On-premise Software includes Evaluation Software, then Customer may use such Evaluation Software solely to develop and use the Licensed Product for the purposes of internal evaluation and testing the development of a Licensed Product. Any such evaluation deployment will use only evaluation Certificates issued by Adobe upon request by Customer. For avoidance of doubt, distribution of Protected Content, Content Policies and Content Licenses using evaluation Certificates, to Consumers, other than employees of Customer, is prohibited without the express written permission of Adobe.

3.3 **Compliance with Compliance and Robustness Rules; Audit Rights**. Customer will ensure that the Licensed Product complies with the Compliance and Robustness Rules at all times. In the event that Adobe posts changes to the Compliance and Robustness Rules, Customer is required to comply with such changes as soon as commercially practicable, but in any event no later than 6 months after the date the changes were posted. Customer is responsible for checking the web site listed in the definition for Compliance and Robustness Rules above periodically so as to be aware of such changes. Adobe may at its option notify Customer via email or other electronic channel, but in no way will the lack of such notification exempt Customer from the obligation to comply with the then-current rules within the required period. Adobe's right of audit under this Agreement extends to inspection of Customer's books, records, procedures and facilities necessary to verify Customer's compliance with the Compliance and Robustness Rules.

3.4 **Content Protection Updates**. In the event that Adobe delivers an update to the Content Protection Functions 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.

3.5 **Prohibited Use**. Except as expressly authorized under this Agreement, Customer is prohibited from:

(A) using the On-premise Software to deploy applications or services other than the Licensed Product;

(B) using the On-premise Software to distribute Content in violation of applicable laws and regulations, including copyright laws; or

(C) using the On-premise Software to protect any other formats or media other than Content.

3.6 **No Circumvention**. No element of the On-premise Software may be used to circumvent or defeat the Content Protection Functions or other requirements of the On-premise Software, Documentation or related technical specifications, provided hereunder. Customer may not:

(A) use Confidential Information or Highly Confidential Information to circumvent the Content Protection Functions of either the On-premise Software or any related Adobe software that is used to encrypt or decrypt digital content for authorized consumption by users of the On-premise Software; or

(B) develop or distribute products that are designed to circumvent the Content Protection Functions of the On-premise Software or the content protection functions of any related Adobe software that is used to encrypt or decrypt digital content for authorized consumption by users of the On-premise Software.

3.7 **No Transfer; Limited Distribution**. Except as may be explicitly provided in this Agreement, Customer may not:

(A) sublicense, assign or transfer the On-premise Software to any third party nor may Customer sublicense, assign or transfer Customer's rights in the On-premise Software, or

(B) distribute or make available the Sample Source to any third party.

3.8 **Open Source Software**. Customer will not directly or indirectly grant, or purport to grant, to any third party any rights or immunities under Adobe's intellectual property or proprietary rights that will subject such intellectual property to an open source license or scheme in which there is or could be interpreted to be a requirement that as a condition of use, modification and/or distribution, the software be:

(A) disclosed or distributed in source code form;

(B) licensed for the purpose of making derivative works; or

(C) 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 this PDM.

3.9 **Confidential Treatment of Content Encryption Keys**. Customer will treat Content Encryption Keys as Confidential Information, except that the marking requirements does not apply and Customer has no further responsibility for Content Encryption Keys that have been distributed to End Users in Content Licenses.

4. Additional Terms for the Handling of Highly Confidential Information. Private Keys are subject to requirements applicable to Highly Confidential Information contained in the Compliance and Robustness Rules and any updates thereto (the "**Security Requirements**"), together with the following provisions:

4.1 All Authorized Employees must sign confidentiality agreements containing terms at least as restrictive as those in this section 5 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 audit permitted under this Agreement. Customer is fully responsible for the conduct of its employees (including Authorized Employees) who may in any way breach this Agreement. 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, including breaches in its security. Customer must cause each Authorized Employee to strictly abide by their obligations under this Section 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.

4.2 Without limitation to any requirement of this Section and the Security Requirements, Customer agrees to 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 such confidential information.

4.3 Customer's obligations with respect to the Highly Confidential Information are in effect in perpetuity. Customer's obligations not to disclose Highly Confidential Information is not subject to any of the exceptions set forth in section 5 of the Agreement, with the exception of section 4.1 regarding disclosure required by law or the order of a court or similar judicial or administrative body.

5. Certificates.

5.1 **Use of Current Certificate**. Each Certificate expires 2 years from the date it is generated by Adobe. Customer will place an order for new Certificates as needed.

5.2 **Certificate Administrator**. 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.

5.3 **Revocation of Certificates**. Adobe has the right to take measures to revoke Certificates issued to Customer in the event that 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 Agreement has expired or been terminated by either party; or

(E) Customer has requested or consented in writing to such expiration.

5.4 **Revocation Process**. In the event that Adobe determines that any of the foregoing 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 On-premise 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 the On-premise Software.