



## PSLT - Adobe Primetime TVSDK Platform (2017v1)

### 1. Additional License Grants and Restrictions.

- 1.1 License Grant to the Adobe Primetime TVSDK.** Adobe grants Customer a non-exclusive license to copy, install, use and integrate the Adobe Primetime TVSDK in accordance with the Documentation provided with the Adobe Primetime TVSDK solely to develop, use, and distribute a Customer Player to Consumers, and to distribute the Redistributable Code as a fully integrated part of such Customer Player for the respective licensed Platform.
- 1.2 License Grant to the Origin Server.** Adobe grants Customer a non-exclusive license to copy, install and use the Adobe Primetime Origin Server to distribute Customer Content to a Customer Player on behalf, and for the benefit, of Customer.
- 1.3 License Restriction.**
- (A) Customer may not: (i) distribute or make available the On-premise Software on a stand-alone basis; (ii) use the Adobe Primetime TVSDK to deploy applications or services other than a Customer Player; or (iii) deliver Customer Content to a non-Customer Player.
  - (B) Customer must (i) only use Adobe Primetime DRM or Adobe Primetime Protected Streaming to encrypt, decrypt and protect Customer Content; (ii) insert Ads into Customer Content to be delivered by the Customer Player using only Adobe Primetime Ad Insertion; and (iii) only distribute the desktop Customer Player on Customer Sites or via the applicable app store for mobile applications.
  - (C) Customer must have a separate valid license to (i) the applicable On-premise Software to enable and use Adobe Primetime Ad Insertion, Adobe Primetime Ad Serving or Adobe Primetime DRM or (ii) stream a type of Customer Content not designated in a Sales Order (e.g., if the Sales Order states that Customer may only stream VOD Content, then Customer must not stream Live Content or Linear Content).
- 1.4 No Circumvention.** No element of the On-premise Software may be used to circumvent or defeat any Adobe Primetime Protected Streaming, Adobe Primetime DRM or Content Protection Functions or other requirements of the On-premise Software or Documentation provided hereunder related to the protection of Content. Customer will not (A) use any Protected Streaming Certificates Private Key to circumvent the Content Protection Functions of either (i) the On-premise Software; or (ii) any related Adobe Technology that is used to encrypt or decrypt digital content for authorized consumption by users of the Customer Players; or (B) use the On-premise Software in any way that decrypts Content except as expressly permitted in this PSLT.
- 1.5 Viral Open Source.** Except as permitted under this Agreement, Customer must not integrate, combine or include, any software that is licensed under a VOSL with the On-premise Software, or take any other action that could require Adobe to disclose, distribute, or license all or any part of the On-premise Software in source code form, for the purpose of making derivative works, or redistributing at no charge. For the purposes of this section, “VOSL” or “Viral Open Source Licenses” means the GNU General Public License (GPL), GNU Affero General Public License (AGPL), GNU Lesser General Public License (LGPL), or any other license that requires (as a condition of use, modification or distribution) that software be: (A) disclosed or distributed in source code form; (B) licensed for the purpose of making derivative works; or (C) redistributed at no charge.

## 1.6 Protected Streaming Certificates.

**1.6.1 Restrictions.** The Protected Streaming Certificates may only be used with PHDS and PHLs and may not be distributed.

**1.6.2 P-Cert Security Requirements.** The Protected Streaming Certificates Private Key will be subject to the following requirements and any updates thereto (the "**P-Cert Security Requirements**"):

(A) Customer must take commercially reasonable steps to prevent the Protected Streaming Certificates Private Key from being compromised.

(B) All Authorized Employees will sign, or have signed, confidentiality agreements containing terms at least as restrictive as those in these P-Cert Security Requirements, either as a condition of their employment or before they are granted access to the Protected Streaming Certificates Private Key. Customer will ensure that all Authorized Employees are made aware of their obligation to comply with the P-Cert 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. 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 Protected Streaming Certificates Private Key and will bear the cost of such steps. Customer will notify Adobe if there is any breach of the terms of this section 2.6 including breaches in its security. Customer must cause each Authorized Employee to strictly abide by their obligations under the P-Cert 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.

(C) Without limitation to any of the P-Cert Security Requirements, Customer agrees that it will treat the Protected Streaming Certificates Private Key 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.

(D) Customer's obligations with respect to the Protected Streaming Certificates Private Key are in effect in for a period of 5 years from the expiration of all Protected Streaming Certificates associated with a Protected Streaming Certificates Private Key. Customer's obligations not to disclose Protected Streaming Certificates Private Key will not be subject to any of the exceptions stated in any applicable non-disclosure agreement or confidentiality terms between the parties, with the exception regarding disclosure required by law or the order of a court or similar judicial or administrative body.

**1.6.3 Use of Current Protected Streaming Certificates.** Each Protected Streaming Certificate may expire during the License Term. Upon expiration, Customer may be required to place an order for new Protected Streaming Certificates as needed.

**1.6.4 Revocation of Protected Streaming Certificates.** Adobe will have the right to take measures to revoke Protected Streaming 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 Protected Streaming Certificate or the Protected Streaming Certificates 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 Protected Streaming Certificates Private Key corresponding to a Protected Streaming

Certificates Public Key for which Adobe has issued a Protected Streaming 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) this PSLT or the Agreement has expired or been terminated by either Party; or
- (E) Customer has requested or consented in writing to such expiration.

If 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 Streaming Content or of the Content Protection Functions of the On-premise Software, or the content protection capabilities of any other Product and Services as applied to any digital content. Adobe will not initiate such revocation prior to 90 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 Products and Services. Adobe will re-issue a revoked certificate only upon its determination that Customer has resolved the breach and all issues leading to the revocation.

**1.6.5 Certificate Administration and Delivery.** Customer must provide Adobe with the name of one employee to serve as the Protected Streaming Certificate administrator responsible for administering the names of those Authorized Employees of Customer who are permitted to request Protected Streaming Certificates from Adobe ("**Certificate Administrator**"). No Protected Streaming Certificates will be issued until a Certificate Administrator has been designated and Authorized Employees are identified. The Certificate Administrator is prohibited from requesting Protected Streaming Certificates. Protected Streaming Certificates are time limited. The Certificate Administrator may be changed from time to time during the License Term with notice to Adobe, but no more than 3 times in a 12-month period.

**2. Service Metrics Collection.** The On-demand Service collects various metrics regarding delivery of Customer Content via the Customer Player. The On-demand Service contains functionality that allows Adobe to receive such metrics, and Customer acknowledges that Adobe may use that information for billing or support purposes, or to otherwise provide and improve the On-demand Services or On-premise Software.

**3. Effect of Termination.** Upon expiration or termination of the License Term, Customer will also, at its expense, remove and delete all copies of the Customer Players under its control, and remove from distribution on Customer Sites or any online application store.

#### **4. Definitions.**

4.1 "**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.

4.2 "**Adobe Primetime TVSDK**" means Adobe's proprietary SDK for creating video players on specified Platforms.

4.3 "**Adobe Primetime Protected Streaming**" means PHDS and PHLs that require Adobe Primetime TVSDK and do not require Adobe Primetime DRM or the use of a DRM license server.

4.4 "**Authorized Employees**" means only the individuals authorized to place or approve orders for Protected Streaming Certificates through the online process for ordering Protected Streaming Certificates that is 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 Protected Streaming Certificates Private Key in order to perform Customer's obligations or exercise Customer's

rights under the Agreement.

- 4.5 **“Consumer”** means an individual end user that receives Customer Content and Ads to, and view the on, a supported Customer Ad Player.
- 4.6 **“Content”** means audio, video, multimedia, text, images, documents, computer programs, data and any other information or materials. The definition of Content does not include Ads.
- 4.7 **“Content Protection Functions”** means those aspects of the On-premise Software that are designed to implement requirements to prevent unauthorized access to Protected Streaming Certificates Private Key, and Protected Streaming Certificates or unauthorized access to or use of Protected Streaming Content inconsistent with the access and usage rules contained in a content license associated with such Protected Streaming Content.
- 4.8 **“Customer Content”** In addition to the definition in the General Terms, means (A) Linear Content; (B) Live Content; and/or (C) VOD Content.
- 4.9 **“Customer Data”** In addition to the definition in the General Terms, **“Customer Data”** also includes data and information collected from a Customer Player.
- 4.10 **“Customer Player(s)”** means Customer-branded Content players and Ad players, developed using the Adobe Primetime TVSDK, for use on Customer Sites or as part of an application on the Platform(s) specified in the Sales Order.
- 4.11 **“HDS”** means HTTP Dynamic Streaming.
- 4.12 **“HLS”** means HTTP Live Streaming.
- 4.13 **“Linear Content”** means Content that includes (A) Live Content or (B) pre-produced Customer Content that is (1) being packaged and delivered to a Customer Player in real time and (2) uploaded or provided by Customer for distribution on or through a Customer Player.
- 4.14 **“Live Content”** means Content that is (A) being packaged and delivered to a Customer Player in real time; and (B) uploaded or provided by Customer for distribution on or through a Customer Player.
- 4.15 **“Origin Server”** means the software that distributes Customer Content to a Customer Player.
- 4.16 **“PHDS”** means protected HDS, a protection method using Adobe Primetime DRM client (as part of the Customer Player) but does not require an Adobe Primetime DRM license server.
- 4.17 **“PHLS”** means protected HLS, a protection method using Adobe Primetime DRM client (as part of the Customer Player) but does not require an Adobe Primetime DRM license server.
- 4.18 **“Platform(s)”** means those platform(s) supported by the TVSDK or as expressly set forth in the Sales Order.
- 4.19 **“Protected Streaming Content”** means Content encrypted using Adobe Primetime Protected Streaming.
- 4.20 **“Protected Protocols”** means PHDS and PHLS.
- 4.21 **“Protected Streaming Certificates”** means revocable, time-limited, electronic documents (A) provided by Adobe 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; and (B) that are issued by Adobe directly to Customer’s customer solely for converting to the Protected Protocols.
- 4.22 **“Protected Streaming Certificates Private Key”** means a cryptographic value generated by the Customer’s customer

and uniquely associated with a Protected Streaming Certificates Public Key.

4.23 **“Protected Streaming Certificates Public Key”** means a cryptographic value generated by the Customer’s customer and uniquely associated with a Protected Streaming Certificates Private Key that is incorporated into a Protected Streaming Certificate issued by Adobe when Customer’s customer follows the Protected Streaming Certificate generation process described in the Documentation.

4.24 **“Redistributable Code”** means (A) object code libraries in the "frameworks" folder in the applicable SDK for each Platform and (B) such other files that Adobe may designate as Redistributable from time to time during the License Term.

4.25 **“VOD”** means video on demand Content that has been uploaded or provided by Customer for distribution on or through a Customer Player. Linear Content and Live Content are expressly excluded from the definition of VOD.