Adobe Qualified Timestamp Service Terms and Conditions


This document contains the Adobe Qualified Timestamp Service additional Terms and Conditions from Adobe Systems Software Ireland Limited, a company with registered office in Dublin, 4-6 Riverwalk, Citywest Business Campus, Ireland, VAT Number IE344992, hereinafter referred to as “Adobe”.

1. Definitions and acronyms

**Trust Service (TS):** electronic service which enhances trust and confidence in electronic transactions;

**Trust Service Provider (TSP):** natural or a legal person who provides one or more trust services

**Time-Stamping Authority (TSA):** trust service provider which issues time-stamps using one or more time-stamping units;

**Certification Authority (CA):** authority trusted by one or more users to create and assign public-key certificates;

**Subscriber:** legal or natural person bound by agreement with a Time-Stamping Authority to any subscriber obligations;

**Relying Party:** legal or natural person that relies upon an electronic identification or a Trust Service;

**Time-Stamping Service or Service:** trust service for issuing time-stamps;

**Time-Stamp:** data in electronic form which bind other electronic data to a particular time establishing evidence that these data existed at that time;

**Time-Stamp Token:** the data object that binds a representation of a datum to a time, thus establishing evidence that the datum existed before that time;

**Certificate or Public Key Certificate:** public key of an entity, together with some other information, rendered unforgeable by digital signature with the private key of the Certification Authority which issued it;

**Contract:** set of all the contractual documents in relation to the delivery of the Services by Adobe to the Subscribers;
Public Key Infrastructure (PKI): infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.

Time-Stamp Policy: named set of rules that indicates the applicability of a time-stamp to a particular community and/or class of application with common security requirements. The Time-Stamp Policy may be unilaterally modified by Adobe at any time, and may be consulted at the Adobe web site https://www.adobe.com/misc/pki/cds_cp.html;

Time-Stamp Practice Statement: statement of the practices which a Time-Stamping Authority employs in issuing managing, revoking, and renewing or re-keying certificates. The Time-Stamp Practice Statement may be unilaterally modified by Adobe at any time, and may be consulted at the Adobe web site https://www.adobe.com/misc/pki/cds_cp.html;

Authentication Credentials: the code or the codes, preserved as confidential, for identification of the Subscriber to the Service;

Time-Stamping Unit (TSU): set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time;

Coordinated Universal Time: the time scale based on the second as defined in ITU-R Recommendation TF.460-6 (02/02);

Fees: amounts paid by the Subscriber for the Time-Stamp Service;

Certificate revocation list: signed list indicating a set of certificates that are no longer considered valid (and thus unusable) by Adobe. It is accessible on its web site http://qcrl.adobe.com/ts/adobeqtsa.crl;

Party: singly the Subscriber or Adobe;

Parties: collectively the Subscriber and Adobe.

2. Terms and Conditions

2.1 The Contract between Adobe and the Subscriber is regulated in descending hierarchical order by:

a) the Adobe General Terms of Use available at http://www.adobe.com/ie/legal/terms.html;
b) the Adobe Sign Additional Terms of Use available at http://www.adobe.com/go/signterms;
c) the present Adobe Qualified Timestamp Service Terms and Conditions;
d) the Time-Stamp Policy;
e) the Time-Stamp Practice Statement.

2.2 Adobe Time-Stamping Service is provided in accordance with the eIDAS regulation, the Irish legislation, ETSI EN 319 421 (Policy and Security Requirements for Trust Service Providers issuing Time-Stamps) and ETSI
EN 319 401 (General Policy Requirements for Trust Service Providers), the Time-Stamp Policy and the Time-Stamp Practice Statement.

2.3 The present Terms and Conditions provide the conditions of use of Time-Stamping Service and are binding for the Subscriber, while using Time-Stamping Service and for the Relying Party, while relying on issued Time-Stamps.

3. Subscriber’s Obligations

3.1 The Time-stamp Service subscriber is obliged to:

- use the Time-Stamping Services in compliance with (i) if any, the Adobe commercial offer (ii) the present Terms and Conditions, (iii) Time-Stamp Policy and (iv) Time-Stamp Practice Statement;
- communicate to Adobe all information needed to enable correct provision of the Time-Stamping Services and guarantee the accuracy and regular updating of these information;
- pay the Fees in compliance with the time requirements and procedures requested by Adobe;
- apply utmost diligence in the use, preservation and protection of the Authentication Credentials, as referred to in the Time-Stamp Policy and Practice Statement. In particular, the Subscriber must take all necessary measures to avoid causing damage to others while using the Time-Stamping Services;
- not sell nor lend nor disclose the Authentication Credentials – neither directly nor indirectly, for whatever purpose – to any third party;
- immediately inform Adobe in the event of theft or tentative of theft of the Authentication Credentials in order to permit Adobe to block the Time-Stamping Services. Failing to comply, the Subscriber will be considered solely liable for the consequences for Adobe, the Relying Party and other third parties.
- implement, maintain and develop a technical infrastructure (including hardware and software solutions) such as to permit use of the Time-Stamping Services in accordance with the Contract.
- verify the various fields contained in the Time-Stamp Token and the validity of the digital signature of the Time-Stamp Token;
- verify that what was time-stamped corresponds to what was requested to be time-stamped. The Subscriber shall also verify that the Time-Stamp Token contains the correct certificate identifier of Adobe, the correct data imprint and the correct hash algorithm OID.

3.2 If upon identification or subsequently, also by using fake identification means, the Subscriber:

a) uses Services in an improper way by violating the law or causing damage to third parties;

b) fails to adopt the necessary procedures needed to avoid the illegal use of the Services by third parties;
he or she shall be considered responsible for any ensuing damage caused to Adobe and/or third parties by wrong information included in the Services, with the obligation to guarantee and release Adobe of responsibility in the event of any request of compensation.

4. Adobe’s Obligations

4.1 Adobe is obliged to:

- operate in accordance with the Time-Stamp Policy and Practice Statement;
- ensure that its reference clock is synchronized with Coordinated Universal Time within the declared accuracy of 1 second;
- undergo internal and external reviews to assure compliance with relevant legislation and internal Adobe policies and procedures;
- provide high availability access to Adobe systems except in the case of maintenance or unavailability of Adobe systems, planned technical interruptions and loss of time synchronization.

4.2 The Trust Service Provider logs are retained as required by applicable laws.

Time-stamp protocols, meaning every issued Time-stamp, are kept for the minimum period as required by applicable laws.

Record data integrity is protected and maintained in a secure site for storage.

If the Subscriber or the Relying Party ask Adobe the proof of the existence of issued Time-stamp, they have to cover the costs of such service.

5. Information for Relying Parties

5.1 The Relying Party is obliged to study the risks, liabilities, limitations and uses related to the acceptance of the Time-Stamping Services, which are established in the Time-Stamp Policy and Practice Statement and in the present Terms and Conditions.

5.2 Before placing any reliance on a Time-Stamp, the Relying Party shall verify that the Time-Stamping Unit has been correctly used and that the Certificate associated to the private key used to sign the Time-Stamp Token is not listed on the Adobe Revocation List.


6.1 Updates to these Terms and Conditions will be posted on the Adobe website at https://www.adobe.com/misc/pki/cds_cp.html;
6.2 Updates to the Time-Stamp Policy and Time-Stamp Practice Statement will be posted on the Adobe website at https://www.adobe.com/misc/pki/cds_cp.html.

7. Information on the Version of this Document

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Modifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/06/2017</td>
<td>1.0</td>
<td>Initial Version</td>
</tr>
</tbody>
</table>