Adobe Qualified Trust Service Certificate Practice Statement (CPS)

Version 1.2
Date: 20th June 2017
Disclaimer

All the information contained in this document is CONFIDENTIAL and can't be used entirely or in part without a written permission from Adobe Systems Software Ireland Limited.
## History

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Changes</th>
<th>Revision</th>
<th>Date</th>
<th>Author</th>
<th>Approver</th>
</tr>
</thead>
<tbody>
<tr>
<td>QTSCPS</td>
<td>First edition</td>
<td>1.0</td>
<td>12/06/2017</td>
<td>Andrea Valle</td>
<td>Mangesh Bhandarkar</td>
</tr>
<tr>
<td>QTSCPS</td>
<td>Updated business and legal matters</td>
<td>1.1</td>
<td>20/06/2017</td>
<td>Andrea Valle</td>
<td>Mangesh Bhandarkar</td>
</tr>
<tr>
<td>QTSCPS</td>
<td>Editorial review</td>
<td>1.2</td>
<td>20/06/2017</td>
<td>Andrea Valle</td>
<td>Mangesh Bhandarkar</td>
</tr>
</tbody>
</table>
# Summary

1. Introduction ................................................................................................................................................................................. 7

1.1 Overview .................................................................................................................................................................................. 7

1.2 Document Name and Identification ........................................................................................................................................ 7

1.3 PKI participants ......................................................................................................................................................................... 8

1.3.1 Certification authorities ......................................................................................................................................................... 8

1.3.2 Registration authorities ......................................................................................................................................................... 9

1.3.3 Subscribers ............................................................................................................................................................................. 9

1.3.4 Relying parties ................................................................................................................................................................. 9

1.4 Certificate Usage .................................................................................................................................................................... 9

1.5 Policy Administration .......................................................................................................................................................... 9

1.6 Definition and Acronyms .................................................................................................................................................... 10

2. Publication and Repository ..................................................................................................................................................... 10

2.1 Repository management ....................................................................................................................................................... 10

2.2 Published information ........................................................................................................................................................ 11

2.3 Time and frequency of publications ................................................................................................................................... 11

2.4 Access control .................................................................................................................................................................... 11

3. Identification and Authentication ........................................................................................................................................ 11

3.1 Naming ................................................................................................................................................................................. 11

3.2 Initial Identity Validation ...................................................................................................................................................... 11

3.3 Identification and Authentication for Re-keying Requests ............................................................................................ 12

3.4 Identification and Authentication for Revocation Requests ............................................................................................ 12

4. Certificate life-cycle operational requirements .................................................................................................................. 12

4.1 Certificate Application .......................................................................................................................................................... 12

4.2 Certificate Application Processing ..................................................................................................................................... 12

4.3 Certificate Issuance ............................................................................................................................................................... 12

4.4 Certificate Acceptance ........................................................................................................................................................ 12

4.5 Key Pair and Certificate Usage ........................................................................................................................................ 13

4.6 Certificate Renewal ........................................................................................................................................................... 13

4.7 Certificate Re-key and Certificate Modification ............................................................................................................. 13

4.8 Certificate Revocation and suspension .................................................................................................................................. 13

4.9 Certificate Status Service .................................................................................................................................................. 13

4.10 End of Subscription ........................................................................................................................................................ 13

4.11 Key Escrow and Recovery ................................................................................................................................................. 14
5 Facilities, Management, and Operational Controls
  5.1 Physical security
  5.2 Procedural controls
  5.3 Personnel controls
  5.4 Event logging
  5.5 Record Archival
  5.6 Renewal of CA Key
    5.6.1 Root CA
    5.6.2 Sub-CA
  5.7 Backup copy
  5.8 Disaster recovery
    5.8.1 Incident and compromise handling procedures
    5.8.2 Computing resources, software and/or data are corrupted
    5.8.3 Entity private key compromise procedures
    5.8.4 Business continuity capabilities after disaster
  5.9 Cessation of the CA
6 Technical Security Controls
  6.1 Key pair generation and installation
    6.1.1 Root CA
    6.1.2 Sub-CA
    6.1.3 TSU Certificate
  6.2 Private Key Protection and Cryptographic Module Engineering Controls
    6.2.1 Root CA
    6.2.2 Sub-CA
    6.2.3 TSU Certificate
  6.3 Other Aspects of Key Pair Management
  6.4 Activation data
  6.5 Computer Security Controls
  6.6 Life cycle technical controls
  6.7 Network security controls
  6.8 Time-stamping

7 Certificate and CRL profile
  7.1 Certificate profile
    7.1.1 Adobe Root CA G2
    7.1.2 Sub-CA for Time-stamp certificate
8 Compliance audit ................................................................................................................................................................................. 21
  8.1 Frequency or circumstances of assessment .......................................................................................................................... 22
  8.2 Identity and qualification of assessor .................................................................................................................................. 22
  8.3 Assessor’s relationship to assessed entity ........................................................................................................................... 22
  8.4 Topics covered by assessment ........................................................................................................................................ 22
  8.5 Actions taken as result of deficiency ................................................................................................................................ 22
  8.6 Communication of results ................................................................................................................................................ 22
9 Other business and legal matters ................................................................................................................................................ 23
  9.1 Service fees ........................................................................................................................................................................ 23
  9.2 Financial responsibility ............................................................................................................................................... 23
  9.3 Confidentiality of Business information .......................................................................................................................... 23
  9.4 Privacy of personal information ........................................................................................................................................... 23
    9.4.1 Information pursuant to Italy’s Legislative Decree n° 196/2003 ...................................................................................... 23
    9.4.2 Archives containing personal information .................................................................................................................. 24
    9.4.3 Privacy protection measures ........................................................................................................................................ 24
  9.5 Intellectual property rights .................................................................................................................................................. 24
  9.6 Representation and warranties ................................................................................................................................................. 24
    9.6.1 Certification Authority ................................................................................................................................................ 24
    9.6.2 Registration Authority .............................................................................................................................................. 25
    9.6.3 Subscribers ..................................................................................................................................................................... 25
    9.6.4 Relying Parties .............................................................................................................................................................. 25
  9.7 Disclaimer of warranties ......................................................................................................................................................... 25
  9.8 Limitations of Liability ..................................................................................................................................................... 25
  9.9 Indemnities .............................................................................................................................................................................. 26
  9.10 Term and Termination ....................................................................................................................................................... 26
  9.11 Amendments ...................................................................................................................................................................... 26
  9.12 Dispute Resolution Provisions ....................................................................................................................................... 26
  9.13 Governing Law ................................................................................................................................................................. 26
  9.14 Compliance with Applicable Law ..................................................................................................................................... 26
  9.15 Miscellaneous Provisions ................................................................................................................................................ 26
1 Introduction

1.1 Overview

This Qualified Trust Service Certificate Practice Statement (QTSCPS) describes the technical, security and organizational requirements implemented by Adobe System Software Ireland Limited (hereinafter referred to also as "Adobe") applicable to:

- a dedicated sub-CAs (TSS CA) supporting qualified trust services;
- the certificates issued by this sub-CA, associated to the Time-stamping Units issuing qualified Time-stamping tokens;
- issuance and management of the qualified Time-stamping tokens.

The service complies with the eIDAS regulation (Regulation (EU) N°910/2014) for Qualified Trust services, specifically for issuing Qualified electronic Time-stamps.

The Time-stamping Service of Adobe conforms to the following standards:

- "ETSI EN 319 401" Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- "ETSI EN 319 421" Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- "ETSI EN 319 422" Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

The structure of this QTSCPS conforms to the public specification [RFC 3647].

This QTSCPS refers to the Certificate Policy whose OIDs are specified in subsection 7.1.3, hereafter referenced as "related QTSCPS". This QTSCPS applies to the following certificates and time-stamp tokens issued by Adobe:

- Adobe root certificates;
- Adobe TSA CA certificates;
- Time-stamp Server certificates;
- Time-stamp tokens.

1.2 Document Name and Identification

This document is the Qualified Trust Service Practice Statement (QTSCPS) applying to Qualified Time-stamps and Certificates issued to Time-stamping Servers by Adobe Systems Software Ireland Limited.

This document is published and freely downloadable from the Adobe’s web site.
1.3 PKI participants

1.3.1 Certification authorities

The Certification Authority (CA) is the trusted third party who issues the certificates and signs them with its own private key (CA key) and manages the status of the certificates.

For the service described in this document the role of Root CA is played by the Irish company Adobe Systems Software Ireland Limited, identified as follows:

<table>
<thead>
<tr>
<th>Company name:</th>
<th>Adobe Systems Software Ireland Limited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Office:</td>
<td>4-6 Riverwalk, Citywest Business Campus, Dublin 24, Ireland</td>
</tr>
<tr>
<td>Legal representative:</td>
<td>Mr. Mark C. Higgins, Ms. Tracy Hanson (US)</td>
</tr>
<tr>
<td>VAT Reg. No. and Tax Code:</td>
<td>VAT-IE344992</td>
</tr>
<tr>
<td>Telephone:</td>
<td>+353 1 242 6700</td>
</tr>
<tr>
<td>Fax:</td>
<td>+353 1 242 6711</td>
</tr>
<tr>
<td>ISO Object Identifier (OID):</td>
<td>1.2.840.113583.1.2.5</td>
</tr>
<tr>
<td>Company web site:</td>
<td><a href="http://www.adobe.com">www.adobe.com</a></td>
</tr>
<tr>
<td>Company e-mail address:</td>
<td><a href="mailto:CloudSignatures@adobe.com">CloudSignatures@adobe.com</a></td>
</tr>
</tbody>
</table>

The Public Key Infrastructure of Adobe used to issue Time-stamping certificates is based on a two-level hierarchy, as shown in the following diagram:

```
  Root CA
   /   \
  /     \
Sub CA 1   Sub CA 1  ...  Sub CA N
```

The Root CA is used for issuing Sub-CA certificates and related CRLs, whereas end-entity certificates are issued by Sub-CAs.

The Root CA is described as follows:

<table>
<thead>
<tr>
<th>SubjectDistinguishedName</th>
<th>SubjectKeyId</th>
<th>Not Before</th>
<th>Not After</th>
</tr>
</thead>
<tbody>
<tr>
<td>OU=Adobe Trust Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>O=Adobe Systems Incorporated</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C=US</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Subordinate CAs maintained by Adobe is described as follows:
### SubjectDistinguishedName
- **CN=Adobe Qualified Timestamp Service CA**
- **OU=Adobe Trust Services**
- **O=Adobe Systems Software Ireland Ltd.**
- **C=IE**

### SubjectKeyId

### Not Before
- Jun 1, 2017 00:00:00 GMT

### Not After
- May 31, 2037 23:59:59 GMT

### 1.3.2 Registration authorities

The Registration Authority (RA) is a person, structure or organization responsible for:

- collection and validation of certification requests and certificate management requests;
- registration of the applicant and organization to which the same belongs;
- authorization of issuance of the certificate requested;

For certificates of the time-stamping service the RA activities are performed by Adobe only.

### 1.3.3 Subscribers

Certificate Subscribers of the Adobe Qualified Timestamp Service CA are employees of Adobe authorized to request and install time-stamping certificates on the time-stamp server.

### 1.3.4 Relying parties

Relying Parties all the clients of the Time-stamp Service who obtain a time-stamp signed by the time-stamp certificate.

### 1.4 Certificate Usage

The **Time-stamp Certificate** can be used only in Time-stamping Servers and can be used only to sign time-stamp tokens, according to [RFC3161].

The policy of certificates issued under this QTSCPS are identified by this OID

1.2.840.113583.1.2.5

under the Adobe OID arc 1.2.840.113583.

The certificates issued under this policy respects the ETSI requirements for Trust Service Providers (TSP) providing services to the public, including TSPs issuing time-stamps.

### 1.5 Policy Administration

This QTSCPS is developed, reviewed, published and updated by Adobe Systems Software Ireland Limited

For further information or explanations about this QTSCPS, please write e-mail to the following address:

CloudSignatures@adobe.com

This QTSCPS and the certificate policies (QTSPP) herein described are approved by Adobe's top management on recommendation by the QTSCPS maintainer.
Adobe periodically reviews its certification processes including the responsibility for maintaining this QTSCPS.

1.6 Definition and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware Security Module</td>
</tr>
<tr>
<td>QTSA</td>
<td>Qualified Time-stamping Authority</td>
</tr>
<tr>
<td>QTSCPS</td>
<td>Certificate Practice Statement</td>
</tr>
<tr>
<td>QTSP</td>
<td>Certificate Policy</td>
</tr>
<tr>
<td>RFC</td>
<td>Request For Comments</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TSA</td>
<td>Time-stamping Authority</td>
</tr>
<tr>
<td>TSP</td>
<td>Trust Service Provider</td>
</tr>
<tr>
<td>TSU</td>
<td>Time-stamping Unit</td>
</tr>
</tbody>
</table>

2 Publication and Repository

2.1 Repository management

Adobe repositories consist of websites:

- http://www.adobe.com

and CRL published on a website:

- http://qcrl.adobe.com

Adobe manages the repositories and is responsible for their maintenance and to update their content. This website repositories are available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under its control, Adobe shall make best endeavors to ensure that this service is not unavailable for more than 5 days.

The certificate status information (CRL) is designed in high availability architecture to guarantee an uptime operational performance better than 99.9%.
2.2 Published information

In the web repositories, the following documents are published:

- Qualified Trust Service Policy (QTSPol), for each qualified trust service
- Qualified Trust Service Practice Statement (QTSCPS).
- Terms & Conditions of the services.
- Maximum fees charged for the service.
- CRL – Certificate Revocation List.

2.3 Time and frequency of publications

Each new revision of the documents is published on the web sites and replaces the previous release.
An archive for the previous releases is also maintained on the web site.
For the CRL issuance frequency refer to section 4.

2.4 Access control

All documents can be freely downloaded from the repository. The editing and publishing of these documents can be performed only by authorized personnel of Adobe.

3 Identification and Authentication

3.1 Naming

The TSU certificates issued by Adobe TSU CA contain the following fields:

<table>
<thead>
<tr>
<th>Adobe TSU Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country (C)</td>
</tr>
<tr>
<td>Organization (O)</td>
</tr>
<tr>
<td>organizationIdentifier</td>
</tr>
<tr>
<td>dnQualifier</td>
</tr>
<tr>
<td>Common Name (CN)</td>
</tr>
</tbody>
</table>

(*) YYYY and MM are the certificate issuing year and month, used to guarantee the DN uniqueness.
("") "x" is a placeholder for the sequential number of the TSU certificate (1, 2, etc.).

3.2 Initial Identity Validation

The validation of the private key corresponding to the requested certificate is based on the cryptographic verification of the CSR (Certificate Signing Request) signature sent to the CA.
The TSA operator generates public keys on the HSM and transmits the public key in the form of a CSR in PKCS#10 format [RFC2986] to the CA issuing the TSU certificates. The CA software, before issuing the certificates, verifies that the digital signature in the CSR is valid.

Transmission of the CSR to the CA is done only using physical devices like USB flash drives by authorized personnel.

3.3 Identification and Authentication for Re-keying Requests

No stipulation.

3.4 Identification and Authentication for Revocation Requests

The revocation of the certificate shall be requested or authorized by the Security Officer according to the procedure described in 4.8.

4 Certificate life-cycle operational requirements

4.1 Certificate Application

The TSA certificate is issued on TSP Operation Officer request as part of the TSA initiation key ceremony.

4.2 Certificate Application Processing

This is part of the TSA initiation key ceremony documented in the security plan.

4.3 Certificate Issuance

The certificate request is handled manually on a physical support by the TSP Operator who proceeds through the following steps, under the supervision of the TSA Officer:

- checks that the CSR is well-coded and does not contain unexpected data;
- generate the certificate;
- save the certificate to the same physical support where it is saved the certificate request.

4.4 Certificate Acceptance

In case of erroneous certificates the TSA Officer shall request to the security officer to authorize the certificate revocation according to the procedure described in 4.8.
4.5 **Key Pair and Certificate Usage**

Each private key is used for a maximum of 15 months then the private key is securely destroyed in presence of the TSA Officer. The certificate is installed and used only in the TSU that is reserved to timestamp token creation and signing according to [rfc3161].

4.6 **Certificate Renewal**

A new TSA key pair is generated and related certificate is issued every 15 months under the TSP Operation Officer supervision.

Previous certificates, under ordinary operations, shall not be revoked. Previous signing key are securely deleted.

4.7 **Certificate Re-key and Certificate Modification**

In case the TSA certificate needs an update a new certificate is issued on TSP Operation Officer request as part of a new TSA initiation key ceremony.

4.8 **Certificate Revocation and suspension**

In case a revocation of the certificate is decided, according to clause 4.8 of the QTSP policy, it is performed by the System Administrator after request of or approval by the Security Officer and the updated CRL published within 24 hours from the request. After the certificate revocation, the System Administrator proceed with the deletion of the related private keys from the HSM.

The suspension of the TSU certificate is not available.

4.9 **Certificate Status Service**

The status of the TSU certificates is made available through the publication of CRLs, in conformance to RFC 5280, via HTTP protocol [RFC7230] on the server http://qcrl.adobe.com.

The complete HTTP address of the CRL, listed below, is inserted in the CRLDistributionPoints extension of the certificate:

   http://qcrl.adobe.com/ts/adobeqtsa.crl

The CRL is re-generated and re-published:

- at least every 6 hours, even in the absence of new revocation events;
- following each new revocation event.

The ARL, namely the list of revoked Sub-CA certificates, is re-generated and re-published:

- at least every day, even in the absence of revocation events;
- following each new revocation event.

4.10 **End of Subscription**

Not applicable to TSU certificates.
4.11 Key Escrow and Recovery

The Key Escrow is not applicable to time-stamp certificates. The TSU keys can be recovered from the backup, created according to the HSM certification, in case of fault of the HSM or any erroneous operation with the same procedure used for the CA key pair backup (see 5.7).

5 Facilities, Management, and Operational Controls

The management, operational, procedural, personnel and physical (non-technical security) controls that are used by Adobe Systems Software Ireland Limited with regards to its qualified service is compliant with the technical standards ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" and Adobe’s ISO/IEC 27001 certified Information Security Management System.

Adobe's information security policy as well as documentation on security controls and operating procedures are available in the security plan and other reserved documents that are available only to authorised Adobe's personnel, to auditors and to the Supervisory Body of Ireland.

The Adobe information security management system is guided by and compliant with ISO/IEC 27001.

5.1 Physical security

All computer systems used for the provision of the qualified trust services herein described are housed in the Adobe's data centers that guarantee:

- a physical access control system, so that access to the building is only possible to authorized personnel;
- access to the TSP services is only possible for authorized personnel holding a personal badge and the corresponding PIN;
- a video surveillance;
- a fire protection system including smoke detection (VEWASD) and dedicated extinguishing system;
- a power supply system fully redundant at all levels (transformers, power centers, generators, UPS's, distribution panels, etc.);
- an air conditioning system (HVAC) which guarantees optimal working conditions;
- redundant Internet connectivity, with a capacity of at least twice the minimum necessary.

5.2 Procedural controls

Adobe Systems Software Ireland Limited carries out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. This risk analysis performed with the full support and collaboration of all component services providers and is regularly reviewed and revised if necessary. This risk analysis is part of the reserved documentation. Appropriate systems, infrastructures and measures for quality and information security management are
implemented and maintained at all times. Any changes that would impact on the level of security provided must be approved by the Security Officer.

Operational procedures are documented under the company’s Quality Management System, certified in accordance with the ISO 9001 standard.

5.3 Personnel controls

All members of the personnel staff that involved for the provision of the trust services are either employees of Adobe Systems Software Ireland Limited or authorised and qualified personnel. All members are subject to personnel and management practices that Adobe follows to provide reasonable assurance of the trustworthiness and competence of the staff members within the fields of electronic signature-related technologies and time-stamping related technologies.

Personnel involved in the service development and management time-stamp service have been adequately trained on the procedures and tools to be used during the various operational phases.

The roles assigned to personnel are defined in accordance with the ETSI EN 319 401.

5.4 Event logging

The main events relevant to the time-stamping service operations are registered in electronic form.

The following events are logged:

- Physical access to the data center.
- Physical access to the QTSP server area.
- Logical access to all the TSP systems.
- Events related to the certificate life cycle (issuance, revocation, renewal, etc.).
- Events related to clock synchronization.
- Events related to the release and updating of software.

For each event, information about the type, date and time of occurrence are logged.

Log files are preserved for 20 years.

5.5 Record Archival

The TSP keeps the following information related to the time-stamp issuing and management processes:

- Event logging;
- All the logging files of the systems involved in the time-stamp service;
- All the Time-stamp token issued;

The archive system has a daemon that checks the consistency and the immutability of the stored log files. In case of inconsistencies fires an alarm to the monitoring system.

The access to the log files is allowed to Adobe’s personnel with role of “System Administrators” and “System Auditors”.
5.6 Renewal of CA Key

5.6.1 Root CA

No stipulation.

5.6.2 Sub-CA

At least 3 years before the end of the validity of the current certification key (Sub-CA key), a new Sub-CA key pair will be generated. From that moment on, TSU certificates and related CRLs shall be signed with the new Sub-CA key.

5.7 Backup copy

A backup copy of data, applications, and any other file necessary for a complete recovery of the service is performed on a daily basis.

5.8 Disaster recovery

5.8.1 Incident and compromise handling procedures

The applicable and appropriate incident and/or compromise reporting and handling procedures, contingency and Business Continuity Plan have been established and are part of the reserved documentation. All such procedures are compliant against ISO/IEC 27001 standard. All incident and/or compromise events are documented and any associated records are archived as described in section 5.5 of this QTSCPS.

5.8.2 Computing resources, software and/or data are corrupted

Adobe Systems Software Ireland Limited acting as TSP establishes the necessary measures to ensure full and highly automated recovery of the Adobe trust services in case of a disaster, corrupted servers, software or data. Any such measures are compliant against the ISO/IEC 27002 standard. Business continuity resources are established at sufficient distance from the original resources to avoid that a disaster would corrupt resources at both sites. Sufficiently fast communications are established between primary and secondary sites to ensure data integrity.

5.8.3 Entity private key compromise procedures

Compromise of the CA private key(s) or of the associated activation data implies immediate revocation of the certificate of the compromised key(s).

Adobe will additionally take the following measures:

1. suspend the time-stamp service;
2. revoke all certificates that became unreliable because of the event;
3. immediately publish the ARL/CRL with revocation information;
4. generate new key pair and a new CA and a new key pair and a new TSU certificate in substitution of the compromised ones.
5. Install the new TSU certificate and restart the time-stamp service.
5.8.4 Business continuity capabilities after disaster
Adobe Systems Software Ireland Limited establishes the necessary measures to ensure full and highly automated recovery of the time-stamping service in case of a disaster, corrupted servers, software or data. Any such measures are compliant against the ISO/IEC 27002 standard. A Contingency Plan has been implemented to ensure business continuity following a natural or other disaster and is available as a separate internal document.

5.9 Cessation of the CA
In the event that the CA intends to cease the provision of service under this QTSCPS, the CA will do what is necessary to minimize disruption to the certificate holders and relying parties; in particular, the CA shall:

- at least 30 days before such termination, inform all time-stamp service clients;
- with the same notice, publish a prominent notice on its website;
- terminate all contracts with any subcontractor;
- before the effective date of termination, transfers to another organization the obligation to keep the registration information, certificate status information and all the relevant logs for the due time;
- at the date of termination, destroy its private CA keys or render them unusable.

6 Technical Security Controls
The security measures taken by Adobe Systems Software Ireland Limited with regards to its CAs to protect CAs cryptographic key and activation data, the constraints on repositories, subject CAs, and other PKI Participants, to protect their Private Keys, activation data for their Private Keys, and critical security parameters, ensuring secure key management, and other technical security controls used by Adobe Systems Software Ireland Limited to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, auditing, archiving, and other technical security controls on PKI Participants are compliant with the following technical standards:

- ETSI EN 319 421

These controls are further described and ruled by the following sub-sections.

6.1 Key pair generation and installation

6.1.1 Root CA
Generation of the Root CA is covered under a separate CPS available from Adobe.

6.1.2 Sub-CA
Generation of the Sub-CA key pair takes place in a physically secured environment, according to the Sub-CA internal procedures that require the joint intervention of two different people ("dual control"). Execution of the key generation procedure (or "key ceremony") is recorded by Adobe's internal auditor.
The key pair used by the CA to sign the certificates and CRLs is generated inside a high quality HSM (Hardware Security Module), with a security certification in accordance with FIPS PUB 140-2 Level 3 and Common Criteria (ISO 15408) at EAL 4 or higher.

6.1.3 TSU Certificate

Generation of the TSU key pair takes place in a physically secured environment, according to the Time-Stamp internal procedures.

Execution of the key generation procedure is recorded by Adobe’s internal auditor.

The key pair used by the time-stamp to sign the Time-stamp token is generated inside a high quality HSM (Hardware Security Module), with a security certification in accordance with FIPS PUB 140-2 Level 3 and Common Criteria (ISO 15408) at EAL 4 or higher.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Root CA

The private key used by the Root CA is kept inside a high quality HSM (Hardware Security Module), with a security certification in accordance with FIPS PUB 140-2 Level 3 or higher.

6.2.2 Sub-CA

The private key used by the CA is kept inside a high quality HSM (Hardware Security Module), with a security certification in accordance with FIPS PUB 140-2 Level 3 and Common Criteria (ISO 15408) at EAL 4 or higher.

6.2.3 TSU Certificate

The private key used by the time-stamp to sign the Time-stamp token is generated inside a high quality HSM (Hardware Security Module), with a security certification in accordance with FIPS PUB 140-2 Level 3 and Common Criteria (ISO 15408) at EAL 4 or higher.

6.3 Other Aspects of Key Pair Management

Root CA and Sub-CA public key are distributed in the following ways:

- by means of publication on the CA web site (http://www.adobe.com)

The public key contained in the TSU public key certificate can be distributed through the time-stamp token on client request.

6.4 Activation data

Adobe Systems Software Ireland Limited ensures that activation data associated to Adobe Systems Software Ireland Limited private keys and operations are securely generated, managed, stored and archived as described in the relevant sub-section of sections 6.1 and 6.2.
6.5 Computer Security Controls

The operating systems are configured so that the user is always required to identify him/herself by means of personal credentials. The access events are logged as described in section 5.4. The operating systems are also subject to periodic hardening in order to disable non-necessary services and functionalities.

Certificate issuance and management is supported by Web interfaces, protected by TLS/SSL secure channel, also used for performing routine certificate management operations by suitably authorized personnel. Multi-factor authentication is required for all accounts capable of directly causing certificate issuance.

6.6 Life cycle technical controls

Periodic development control, security management and life cycle security controls are implemented in compliance with the standard ETSI EN 319 411-1 and with ETSI EN 319 411-2 when this standard impose higher requirements on certification practices. Detailed descriptions of implemented life cycle technical controls are available as internal document(s).

6.7 Network security controls

Network security controls including but not limited to firewalls, network intrusion detection secure communication between PKI Participants ensuring confidentiality and mutual authentication, anti-virus protection, website security, databases and other resources protection from outside boundaries, etc. are implemented in compliance with the standard ETSI EN 319 411-1 and with ETSI EN 319 411-2 when this standard impose higher requirements on certification practices.

Detailed descriptions of implemented network security controls are available as internal document(s).

6.8 Time-stamping

All the computer systems used by the CA and Time-stamping service are synchronised with a time server which in turn is synchronized with a Network Time Protocol (NTP) synchronized using “Stratum 1” time source.

7 Certificate and CRL profile


As for cryptographic algorithms, minimum length of keys, key parameters and hashing functions, the CA conforms to ETSI TS 119 312.

7.1 Certificate profile

7.1.1 Adobe Root CA G2

### 7.1.2 Sub-CA for Time-stamp certificate

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>V3</td>
</tr>
<tr>
<td>Signature</td>
<td>Sha256WithRSAEncryption (1.2.840.113549.1.1.11)</td>
</tr>
<tr>
<td>Issuer</td>
<td>CN=Adobe Root CA G2, OU=Adobe Trust Services, O=Adobe Systems Incorporated, C=US</td>
</tr>
<tr>
<td>Validity</td>
<td>&lt;20 years&gt;</td>
</tr>
<tr>
<td>Subject</td>
<td>CN=Adobe Qualified Timestamp Service CA, OU=Adobe Trust Services, O=Adobe Systems Software Ireland Ltd., C=IE</td>
</tr>
<tr>
<td>SubjectPublicKeyInfo</td>
<td>&lt;RSA public key of 4096 bits&gt;</td>
</tr>
<tr>
<td>Signature Value</td>
<td>&lt;Root CA signature&gt;</td>
</tr>
<tr>
<td>Extension</td>
<td>Value</td>
</tr>
<tr>
<td>Basic Constraints</td>
<td>critical: CA=true</td>
</tr>
<tr>
<td>KeyUsage</td>
<td>critical: keyCertSign, cRLSign</td>
</tr>
<tr>
<td>CRLDistributionPoints (CDP)</td>
<td><a href="http://crl.adobe.com/adoberootg2.crl">http://crl.adobe.com/adoberootg2.crl</a></td>
</tr>
</tbody>
</table>

### 7.1.3 Time-stamp Unit (TSU) certificate

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>V3</td>
</tr>
<tr>
<td>Signature</td>
<td>Sha256WithRSAEncryption (1.2.840.113549.1.1.11)</td>
</tr>
<tr>
<td>Issuer</td>
<td>CN=Adobe Qualified Timestamp Service CA, OU=Adobe Trust Services, O=Adobe Systems Software Ireland Ltd., C=IE</td>
</tr>
<tr>
<td>Validity</td>
<td>&lt;135 months&gt;</td>
</tr>
<tr>
<td>Subject</td>
<td>CN=Time-Stamping Authority TSU, OU=Adobe Trust Service, O=Adobe Systems Software Ireland Ltd., C=IE</td>
</tr>
</tbody>
</table>
7.2 CRL profile

The CRLs are compliant with the with the ISO/IEC 9594-8:2005 [X.509] International Standard and public specification [RFC 5280].

Besides the mandatory information, the CRLs also contain:

- `nextUpdate` (date for the next issue of CRL)
- `CRLNumber` (sequential number of CRL)

The CRL is digitally signed using the signature algorithm sha256WithRSAEncryption (1.2.840.113549.1.1.11). Moreover, in correspondence with each item of the CRL there is a `reasonCode` extension to indicate the reasons for revocation.

8 Compliance audit

The technological infrastructure, physical and logical security controls, several operating procedures, and the personnel employed in providing the TSA service described in this QTSCPS are the same as those used for issuing qualified certificates according to the EU Regulation n. 910/2014 on electronic signatures (eIDAS).

Adobe Systems Software Ireland Limited is a Qualified Trust Service Provider (QTSP) according to the European legislation; as such, Adobe Systems Software Ireland Limited is under supervision by the Irish Department of Communications Energy and Natural Resources (the Supervisory Body of Ireland) and is required to perform periodic internal audits and periodic conformity assessment by a Conformity Assessment Body accredited according to the eIDAS Regulation.
8.1 Frequency or circumstances of assessment

Adobe commits to do what is necessary so that a compliance audit be done at least every 12 months engaging a Conformity Assessment Body accredited according to the eIDAS Regulation.

The internal audits are carried out in accordance with a schedule which provides different periods (from quarterly to annual) for the various technical-operational aspects of the CA service.

8.2 Identity and qualification of assessor

The internal audits are carried out by Adobe's internal auditor, who is suitably qualified for the task. External audits, are performed by a Conformity Assessment Body accredited according to the eIDAS Regulation.

8.3 Assessor's relationship to assessed entity

No relationship shall exist between the CA and any external auditors that can influence the outcome of the audits in favour to Adobe.

Adobe's internal auditor does not belong to the organizational unit in charge of CA operations.

8.4 Topics covered by assessment

Audits performed by external assessors (other than the Irish Department of Communications Energy and Natural Resources) are aimed at verifying compliance of Adobe and the qualified services it provides according to the applicable requirements of the eIDAS Regulation.

The main objective of the internal audit is to verify the respect of Adobe's internal operating procedures and their compliance with this QTSCPS.

8.5 Actions taken as result of deficiency

In the case of non-compliances, the Irish Department of Communications Energy and Natural Resources will require the CA to adopt the necessary corrective measures within a certain period of time, under penalty of fines and revocation of the accreditation.

Non-compliances found by CABs are brought to the attention of the Irish Department of Communications Energy and Natural Resources and Adobe's top management who decides how to handle them on a case-by-case basis.

8.6 Communication of results

The results of internal audits are presented directly to Adobe's top management, and shared with the other internal stakeholders, via an audit report. When relevant, and according to the eIDAS Regulation, security incidents will be notified to the interested parties.
9 Other business and legal matters

The general Terms & Conditions of the CA service herein described are provided to customers as a separate document, to be accepted at application time, published on the CA web site.

In the case of a discrepancy between this QTSCPS and the separate "Terms & Conditions" document, "Terms & Conditions" will take precedence.

9.1 Service fees

The fees are published on the CA web site www.adobe.com and are subject to change without prior notification.

Different conditions may be negotiated case by case, according to the volumes requested and the use case.

9.2 Financial responsibility

Adobe maintains the following insurance related to its performance and obligations under this QTSCPS:

- Commercial General Liability insurance;
- Professional Liability/Errors and Omissions insurance.

Such insurance is with a company rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide.

9.3 Confidentiality of Business information

Provisions relating to the treatment of confidential information that PKI Participants may communicate to each other, and in particular relating to the scope of what is considered as information within or not within the scope of confidential information, to the responsibility to protect confidential information, and to disclosure conditions are provided within the QTSCPS.

Adobe acting as a TSP guarantees the confidentiality of any data not published in the Certificates, according to the applicable laws on privacy.

9.4 Privacy of personal information

Adobe is the processor of the personal information collected during the registration phase of parties requesting time-stamps under this QTSCPS, and shall process such information ensuring their confidentiality and in compliance with the Regulation (EU) n. 679/2016 and Italy's Legislative Decree n.196/2003 [DLGS196].

9.4.1 Information pursuant to Italy's Legislative Decree n° 196/2003

Adobe, processor of the personal data provided by the subscriber, hereby informs the subscriber that, pursuant to the Italy's Legislative Decree 196/2003 [DLGS196], such personal data shall be processed by means of both paper archives and information systems that guarantee their security and confidentiality.

The information supplied by the subscriber falls into two categories: mandatory and optional. The mandatory information is necessary for delivering the requested service; failure by the subscriber to
provide that information will not allow the contract to be concluded. The optional information is used to assist in the service; failure by the subscriber to provide this information will not prevent the contract to be concluded.

The information provided by the applicant is processed exclusively for the purpose of issuing and managing the certificates, and can be communicated to companies providing consultancy and technical support to the CA in relation to this data processing. The subscriber shall be granted the rights provided for in aforesaid Decree.

9.4.2 Archives containing personal information

The data provided are processed using both electronic and non-electronic instruments. Adobe takes all necessary precautions in order to guarantee their security and confidentiality. Data are handled and protected in environments whose access is constantly under control.

9.4.3 Privacy protection measures

Adobe complies with the provisions of the Regulation (EU) n. 679/2016 and Italy’s Legislative Decree n.196/2003 [DLGS196] and subsequent modifications and amendments, by putting in place suitable security controls. In particular, Adobe:

- adopts suitable measures to control access to the archives;
- adopts suitable procedures for management of authentication credentials;
- keeps a permanent audit log of access to the archives.

9.5 Intellectual property rights

Adobe performs periodic backup of data for recovery purposes.

Within the service regulated by this QTSCPS, the CA does not collect and does not process any sensitive data nor judicial data (with reference to article 4 of the aforesaid Decree [DLGS196]).

This QTSCPS is the property of Adobe which reserves all the rights associated with the same.

The subscriber of the service keeps all the rights on its own commercial marks (brand names) and its own domain names.

With regards to the property rights of other data and information, the applicable law shall be applied.

9.6 Representation and warranties

9.6.1 Certification Authority

The Certification Authority shall:

- operate in compliance with this QTSCPS;
- identify the subscriber as described in this QTSCPS;
- issue and manage the certificates as described in this QTSCPS;
- provide an efficient revocation service for the certificates;
- guarantee that the subscriber, at the time when the certificate is issued, did possess the corresponding private key;
timely inform about any eventual compromise of its own private key;
provide clear information about the procedures and requirements of the service;
provide a copy of this QTSCPS to anyone requesting it;
guarantee processing of personal data in compliance with applicable laws;
provide an efficient and reliable information service about the status of the certificates.

9.6.2 Registration Authority
Not applicable to a Time-Stamp service.

9.6.3 Subscribers
Subscribers are entities that hold a service contract with Adobe and have agreed to the Adobe Time-Stamping Authority Subscriber Agreement.
Organisations that are Subscribers are responsible for the activities of their associated users and are expected to inform them about the correct use of time-stamps and the conditions of this QTSCPS.
Subscribers must use a method, software, toolkit or service approved by Adobe to create time-stamps, unless otherwise specifically authorised in writing by Adobe.

9.6.4 Relying Parties
A Relying Party is an individual or entity that relies on a time-stamp generated by the Adobe Qualified Time-stamping service. A Relying Party may or may not be a Subscriber.

9.7 Disclaimer of warranties
Except as expressly provided elsewhere in this QTSCPS, the applicable QTSPPP and in the applicable legislation, Adobe Systems Software Ireland Limited acting as TSP disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except that it came from an authorised source), and further disclaims any and all liability for negligence and lack of reasonable care on the part of Subscribers and Relying Parties. Adobe Systems Software Ireland Limited does not warrant "non-repudiation" of any Certificate or message. Adobe Systems Software Ireland Limited does not warrant any software as part of its Qualified Time-stamping service.

9.8 Limitations of Liability
Adobe undertakes to operate the Qualified Time-stamping service in accordance with the QTSCPS, the QTSPPP, and the terms of agreements with the Subscriber. Adobe makes no express or implied representations or warranties relating to the availability or accuracy of the time-stamping service. Adobe shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of the QTSCPS or QTSPPP, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term "loss" means a partial loss or reduction in value as well as a complete or total loss. Adobe bears specific liability for damage to Subscribers and Relying Parties in relationship to valid Qualified Time-stamp Certificates relied upon in accordance with specific national laws and regulations.
9.9 Indemnities
Adobe Systems Software Ireland Limited acting as TSP assumes no financial responsibility for improperly used Certificates, CRLs, Time-stamps, etc.

9.10 Term and Termination
This QTSCPS is effective from the time it is published on the CA website (see Chapter 2) and will remain in force until it is replaced with a new version.

9.11 Amendments
Adobe reserves the right to modify this QTSCPS at any time whatsoever without prior notification.

9.12 Dispute Resolution Provisions
Subscribers can submit their claims or complaints to the following email: CloudSignatures@adobe.com
Complaints received by Adobe will be treated by Adobe’s internal services in order to resolve any disputes promptly and efficiently.
Any controversy that cannot be solved by Adobe’s internal services shall be submitted to the exclusive jurisdiction of the Law of Ireland, except for the conditions that apply in case the Subscriber can be qualified as Consumer according to the applicable European or National consumer laws.

9.13 Governing Law
This QTSCPS is subject to the Law of Ireland and as such shall be interpreted and carried out. For that not expressly prescribed in this QTSCPS, the applicable law shall prevail.
Other contracts in which this QTSCPS is incorporated by means of reference, may contain distinct and separate clauses with respect to applicable law.

9.14 Compliance with Applicable Law
Mandatory applicable laws shall prevail on the provisions of this QTSCPS.

9.15 Miscellaneous Provisions
Terms and conditions described in the applicable QTSPPP and in the Adobe’s QTSCPS;
Adobe acting as QTSP incorporates by reference the following information in all Certificates it issues:
- Any other applicable Certificate Policy as may be stated in an issued Certificate;
- The mandatory elements and any non-mandatory but customised elements of applicable standards;
- Content of extensions and enhanced naming not addressed elsewhere;
- Any other information that is indicated to be so in a field of a Certificate.
To incorporate information by reference, Adobe through its CAs uses computer-based and text based pointers that include URLs, OIDs, etc.