Adobe Qualified Trust Service Provision Policy (CP)

Version 1.2
Date: 20th June 2017

OID: 1.2.840.113583.1.2.5
## 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>QTSSP</td>
<td>First edition</td>
<td>1.0</td>
<td>01/06/2017</td>
<td>Andrea Valle</td>
<td>Mangesh Bhandarkar</td>
</tr>
<tr>
<td>QTSSP</td>
<td>Updated Root CA information</td>
<td>1.1</td>
<td>12/06/2017</td>
<td>Andrea Valle</td>
<td>Mangesh Bhandarkar</td>
</tr>
<tr>
<td>QTSSP</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 .......................................................................................................................... 6

1.1 QTSPP Overview .............................................................................................................. 6

1.1.1 Purpose ......................................................................................................................... 6

1.1.2 Level of specificity ....................................................................................................... 6

1.1.3 References ................................................................................................................... 7

1.2 Document name and identification .................................................................................. 7

1.3 PKI participants ................................................................................................................ 7

1.3.1 Adobe as Time-stamping and Certification Authority .................................................. 8

1.3.2 Subscribers .................................................................................................................. 8

1.4 Certificate usage .............................................................................................................. 8

1.4.1 Appropriate certificate uses ......................................................................................... 8

1.4.2 Prohibited certificate uses .......................................................................................... 8

1.5 Policy administration ........................................................................................................ 9

1.5.1 Organization administering the document .................................................................... 9

1.5.2 Contact person ........................................................................................................... 9

1.6 Definitions and acronyms ............................................................................................... 9

2 Publication and repository responsibilities ......................................................................... 10

2.1 Repositories .................................................................................................................... 10

2.2 Publication of certification information ............................................................................ 10

2.3 Time or frequency of publication ................................................................................... 10

2.4 Access controls on repositories ..................................................................................... 10

3 Identification and authentication ....................................................................................... 11

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

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

3.3 Identification and Authentication for Re-key Requests .................................................... 11

3.4 Identification and Authentication for Revocation Requests .......................................... 11

4 Certificate life-cycle operational requirements .................................................................. 11

4.1 Certificate Application ...................................................................................................... 11

4.2 Certificate Application Processing ............................................................................... 11

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

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

4.5 Key Pair and Certificate Usage ....................................................................................... 12

4.6 Certificate Renewal ........................................................................................................ 12
Certificate and CRL profile ...............................................................................................................................................................17

Facilities, management and operational controls........................................................................................................... 13
  6.1 Physical security ...................................................................................................................................................................13
  6.2 Procedural controls .................................................................................................................................................................14
  6.3 Personnel controls ...................................................................................................................................................................14
  6.4 Event logging ............................................................................................................................................................................14
  6.5 Record Archival .......................................................................................................................................................................14
  6.6 Renewal of CA Key .................................................................................................................................................................15
    6.6.1 Root CA ..............................................................................................................................................................................15
    6.6.2 Sub-CA ..............................................................................................................................................................................15
  6.7 Backup copy .............................................................................................................................................................................15
  6.8 Disaster recovery ...................................................................................................................................................................15
    6.8.1 Incident and compromise handling procedures ..............................................................................................................15
  6.9 Cessation of the CA .................................................................................................................................................................15

Technical Security Controls .............................................................................................................................................................16
  7.1 Key pair generation and installation ...............................................................................................................................................16
    7.1.1 Root CA ..............................................................................................................................................................................16
    7.1.2 Sub-CA ..............................................................................................................................................................................16
    7.1.3 Time-Stamp Unit Certificate ...........................................................................................................................................16
  7.2 Private Key Protection and Cryptographic Module Engineering Controls ................................................................................16
    7.2.1 Root CA ..............................................................................................................................................................................16
    7.2.2 Sub-CA ..............................................................................................................................................................................16
    7.2.3 Time-Stamp Unit Certificate ...........................................................................................................................................16
  7.3 Other Aspects of Key Pair Management .........................................................................................................................................17
  7.4 Activation data ..........................................................................................................................................................................17
  7.5 Computer Security Controls .....................................................................................................................................................17
  7.6 Life cycle technical controls .......................................................................................................................................................17
  7.7 Network security controls ............................................................................................................................................................17
  7.8 Time-stamping ...........................................................................................................................................................................17

Certificate and CRL profile ..............................................................................................................................................................17
  8.1 Certificate profile .......................................................................................................................................................................17
8.2 CRL profile................................................................. 18
9 Compliance audit................................................................................................. 18
  9.1 Frequency or circumstances of assessment .............................................. 18
  9.2 Identity and qualification of assessor.......................................................... 18
  9.3 Assessor’s relationship to assessed entity.................................................... 18
  9.4 Topics covered by assessment.................................................................. 18
  9.5 Actions taken as result of deficiency .......................................................... 19
  9.6 Communication of results......................................................................... 19
10 Other business and legal matters.................................................................... 19
  10.1 Service fees............................................................................................ 19
  10.2 Financial responsibility........................................................................... 19
  10.3 Confidentiality of Business information.................................................. 19
  10.4 Privacy of personal information............................................................... 19
  10.5 Intellectual property rights........................................................................ 19
  10.6 Representation and warranties................................................................. 20
    10.6.1 Certification Authority............................................................... 20
    10.6.2 Registration Authority.............................................................. 20
    10.6.3 Subscribers................................................................................. 20
    10.6.4 Relying parties.......................................................................... 20
  10.7 Disclaimer of warranties.......................................................................... 20
  10.8 Limitations of Liability............................................................................ 20
  10.9 Indemnities............................................................................................ 20
  10.10 Term and Termination.......................................................................... 20
  10.11 Amendments....................................................................................... 20
  10.12 Dispute Resolution Provisions............................................................... 20
  10.13 Governing Law.................................................................................... 21
  10.14 Compliance with Applicable Law........................................................... 21
  10.15 Miscellaneous Provisions...................................................................... 21
1 Introduction

1.1 QTSSPP Overview

This Qualified Trust Service Provision Policy (hereafter referenced also as QTSSPP) covers the technical, security and organizational requirements for Adobe Systems Software Ireland Limited (hereafter referenced also as "Adobe") to provide Qualified Trust Services in compliance with the Regulation (UE) n. 910/2014 (eIDAS Regulation).

In general, the present QTSSPP states "what is to be adhered to", while the specific practices needed to implement the present QTSSPP, "how it is adhered to", are described in the Adobe Qualified Trust Service Provider Practice Statement, published on the Adobe web site, together with the present policy, at the following URI:

https://www.adobe.com/misc/pki/cds_cp.html

Compliance with security and policy requirements specified in ETSI EN 319 401 v2.1.1, ETSI EN 319 411-1 v1.1.1 and ETSI EN 319 421 v1.1.1 guarantees that Adobe adopts international state-of-the-art in trust service provisioning and fulfilment of the eIDAS Regulation requirements. The present document describes the policy to which the Adobe Qualified Trust Services adheres, to confirm to Subjects, Subscribers and Relying Parties of the correct operation and management of the respective services.

1.1.1 Purpose

The present document specifies a Qualified Trust Service Provider Policy to meet general requirements for Adobe Qualified Trust Services.

This Certificate Policy applies to the following certificates and time-stamp tokens issued by Adobe:

- Time-stamp Unit (TSU) certificates;
- Qualified Electronic Time-stamps (Qualified Time-stamp Tokens, QTST).

The TSU certificates and the QTSTs issued by Adobe that specify the OID of this QTSSPP respectively in their Certificate Policies and TSAPolicyId field, can be considered as fully compliant with the relevant requirements of the eIDAS Regulation, specifically as Qualified Electronic Time-stamps.

The present document is publicly available. Distribution is restricted as described in the "Intellectual Property Rights" section.

1.1.2 Level of specificity

The present Qualified Trust Service Provider Policy describes only general rules of issuing and managing time-stamps. Detailed description of the infrastructure and related operational procedures are described in the Security Plan that is available only to authorised Adobe personnel, to auditors and to the Supervisory Body of Ireland.
1.1.3 References


3. ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

4. ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp profiles.


7. ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

8. ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.


1.2 Document name and identification

Policy Name: Adobe Qualified Trust Service Provision Policy v. 1.0

Object Identifier (OID) for TSU certificates: 1.2.840.113583.1.2.5

Object Identifier (OID) for Timestamp Tokens: 0.4.0.2023.1.1

This is the Best Practices Policy for Time-stamp specified in EN 319 421 and is included to claim conformance to it.

1.3 PKI participants

This Certificate Policy applies to:

- The Adobe Time-stamp Authority and dedicated Certification Authority, i.e.:
  - its logistic and technical infrastructure;
  - its personnel.

- End users to whom Time-stamps have been issued in compliance with this Qualified Trust Service Provision Policy.

- Relying parties, relying on Time-stamps issued by Adobe TSA in compliance with this Qualified Trust Service Provision Policy to support assertions of proof that a datum existed before the time indicated in the time-stamp itself.
1.3.1 Adobe as Time-stamping and Certification Authority

Adobe Systems Software Ireland Limited is a company based in Dublin (Ireland).

Adobe as Time-stamping Authority (TSA) issues qualified time-stamp tokens to any subscriber (private or public user) according to the eIDAS Regulation.

Adobe issues TSU certificates to each Time-stamp Unit under its own responsibility.

Adobe Root CA issues certificates to any sub-CAs issuing qualified certificates or certificates for keys used to create qualified trust tokens, for example qualified time-stamp tokens.

1.3.2 Subscribers

Subscribers are natural persons (individual end-users) or legal persons (several end-users) bound by agreement with Adobe as Time-stamping Authority to any subscriber obligations.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

1.4.1.1 Time-stamp Unit certificates appropriate uses

TSU certificates issued by Adobe may be used only to sign Time-stamp Tokens with the authorized technical and physical infrastructure.

1.4.1.2 Time-stamp Tokens appropriate uses

Time-stamps issued by Adobe may be used:

1. to testify that the datum represented by the time-stamped digest existed before the time specified in the time-stamp, with the accuracy provided for in section 7.3.3;
2. to extend a signature validity beyond the signer's certificate expiration date;
3. generally speaking, in all cases unless otherwise stated in the rules of law and the Terms and Conditions agreed upon by Adobe and the subscriber.

1.4.2 Prohibited certificate uses

1.4.2.1 Time-stamp Unit certificates prohibited uses

TSU certificates issued by Adobe must not be used other than for signing Time-stamp Tokens with the authorized technical and physical infrastructure.

1.4.2.2 Time-stamp Tokens prohibited uses

Time-stamps issued under this policy must not be used by applications:

1. requesting for time accuracy outside the limits specified in this policy;
2. providing datum digests computed with has algorithm other than what is provided for time-stamp in this policy;
3. inconsistent with the Terms and Conditions in force and accepted by the subscriber;
4. requiring a time-stamp life span beyond the TSS certificate expiration date. Should such case be required, the time-stamped object shall be re-time-stamped before the time specified in the TSS certificate expiration.

1.5 Policy administration

1.5.1 Organization administering the document

This Policy is issued under the responsibility of:

Adobe Systems Software Ireland Limited
4-6 Riverwalk
Citywest Business Campus
Dublin 24
Ireland
Email: CloudSignatures@adobe.com

1.5.2 Contact person

The person in charge of this Policy is:
Andrea Valle, System Auditor.

1.6 Definitions and acronyms

AES Advanced Electronic Signature
ARL Authority Revocation List
B2B Business to Business
CA Certification Authority
CRL Certificate Revocation List
HSM Hardware Security Module
IETF Internet Engineering Task Force
ISO International Organisation for Standardisation
ITU International Telecommunications Union
LDAP Lightweight Directory Access Protocol
NCP Normalised Certificate Policy
NCP+ Normalised Certificate Policy +
OID Object Identifier
PKCS Public Key Certificates Standard
PKI Public Key Infrastructure
PKIX Public Key Infrastructure (X.509) (IETF Working Group)
QES Qualified Electronic Signature
2 Publication and repository responsibilities

2.1 Repositories
Adobe QTSP board has the responsibility for operation of the repositories listed in clause 2.2.

2.2 Publication of certification information
The following will be available at the URL https://www.adobe.com/misc/pki/cds_cp.html:

- CRL repository
- this QTSP (Certificate Policy)
- the QTSPPS (Certificate Practice Statement) corresponding to this QTSP
- the following Adobe certificates:
  - certificates of the public keys corresponding to the private ones used by Adobe to sign the TSU certificates and the certificate revocation lists (CRL)
  - the Adobe Root CA G2 self-signed certificate.

2.3 Time or frequency of publication
- All certificates shall be published as soon as they are issued.
- CRL will be routinely published every 6 hours.
- Subsequent versions of QTSP and QTSPPS will be published soon after completion of the approval process.

2.4 Access controls on repositories
Read privileges will be granted to end-users without any access control.
Write and modify privileges will be granted solely to Adobe officers in charge of repository maintenance.

3 Identification and authentication

3.1 Naming

All the TSU certificates issued by Adobe Qualified Timestamp Services CA (a Sub-CA of the Root CA) are compliant with the profile specified in ETSI EN 319 412-3.

3.2 Initial Identity Validation

The TSU certificate is requested and issued according to internal Adobe procedures under the supervision of the Security Officer and TSP Operation Officer.

3.3 Identification and Authentication for Re-key Requests

The re-key operation is not available for the TSU certificates. Every certificate change (renew or re-key) is managed issuing a new certificate.

3.4 Identification and Authentication for Revocation Requests

The TSU certificate is revoked according to internal Adobe procedures under the supervision of the Security Officer and TSP Operation Officer.

4 Certificate life-cycle operational requirements

4.1 Certificate Application

The Manager in charge of the TSA acts as the applicant subscriber.

4.2 Certificate Application Processing

Upon TSS key pair generation, the public key certificate request is generated and the Adobe CA dedicated to TSA certificate generation issues the requested certificate. The issued certificate data are checked for correctness.
4.3 Certificate Issuance

The procedure is part of the TSA initiation key ceremony and is authorized by the Security Officer and performed under the supervision of the TSP officers. The content of the certificate must be verified before service activation.

4.4 Certificate Acceptance

The Manager in charge of the TSA shall immediately request a revocation of erroneous certificates.

4.5 Key Pair and Certificate Usage

Each private key is used for a maximum of 15 months.

Certificate usage is reserved to timestamp-token signing according to RFC 3161.

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

The conditions which may lead to a revocation are:

- the certificate is not correct in terms of information contained.
- the TSP ceases the time-stamping service.
- the TSP loses its qualification, upon request by the Supervision Authority.
- there is the evidence of a private key compromise.
- the TSP is made aware of a possible compromise of the private key of the TSS CA or the root CA used for issuing the TSS CA certificate.

Certificate revocation must be duly authorized by the management and must be published within 24 hours after the revocation authorization.

Certificate suspension is not available for TSU and CA certificates.
4.9 Certificate Status Service

The status of the TSU certificates is made available to all interested parties through the publication of the Certificate Revocation List (CRL) that is publicly available from HTTP repositories.

4.10 End of Subscription

Not applicable to TSU certificates.

5 Key Escrow and Recovery

The Key Escrow is not applicable to TSU certificates.

In case of failure the TSU keys can be recovered from backup with the same security level of CA keys.

6 Facilities, management and operational controls

The qualified trust service controls shall comply with EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps and ISO/IEC 27001 certified.

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 personnel, to auditors and to the Supervisory Body of Ireland.

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

6.1 Physical security

Adobe TSP systems and devices (both HW and SW) are managed in and from secure facilities, protected from unauthorized access.

Only Adobe CA authorized staff is authorized to access PKI specific areas under stringent security policies and procedures, audited on a regular basis.

TSP systems are within restricted access and electronically controlled areas.

Active and passive anti intrusion systems are operational at all times.

Alarm facilities react when detecting unauthorized access attempt.

Cryptographic devices (belonging to CA, TSS, RA, LRA) when not in use shall be kept in safe containers.

Security measures are in force to ensure safe and secure air conditioning systems and a suitable power supply.

Fire prevention and protection measures compliant with the current rules of law are in place.

Data media are stored in safe and secure places and handled under specific procedures.

The waste is disposed of in order to prevent from disclosure of confidential data.
Media disposal procedures provide for their sanitization. Confidential paper documents are shredded before being disposed of. Dangerous and toxic waste is disposed of according to the rules of law in force.

6.2 Procedural controls
TSP officers are authenticated when accessing the systems and role separation is strictly enforced.

6.3 Personnel controls
Officers covering the TSP management roles have a minimum of 5 years background in information systems analysis, development, planning or managing. They all have explicitly accepted their duties on which they have received proper training and are timely trained on Adobe's PKI technological, security policies and procedures, and organization changes.

TSP related personnel cannot be assigned to perform incompatible PKI related task.

TSP personnel must have no known records of willful, negligent or reckless wrongdoing in performing security duties. 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.

6.4 Event logging
All TSP systems keep track of all relevant operations. Log files are securely kept and protected against tampering.

Logged events range from normal operations (e.g.: SW installation and update, log-in and log-out by operators) up to abnormal operations (e.g.: operator errors, unauthorized attempts).

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

Log files are preserved for 20 years as per rules of law currently in force.

Log records are digitally signed daily to protect them for integrity. Log files are kept in a safe and tamper proof environment.

6.5 Record Archival
All documentation (either on electronic or paper media) and events are archived, related to:

1. certificate generation,
2. certificate revocation and suspension,
3. time-stamp tokens issuing (including issued time-stamp tokens),
4. logs recorded by access and relevant task activation/deactivation,
5. abnormal events on TSS systems, specifically in relation to time synchronization.
6. Minutes of the CA and TSS key ceremonies.
Archived records include the time they have been recorded

6.6 Renewal of CA Key

6.6.1 Root CA

The Root CA of the Adobe Qualified Timestamp Service (Adobe Root CA G2) is covered in a separate Certificate Policy. Refer to the "CDS Certificate Policy" available from this URL:

https://www.adobe.com/misc/pdfs/Adobe_CDS_CP.pdf

6.6.2 Sub-CA

At least 3 years before the CA key expiration a new key pair and CA certificate are generated and shall be used to sign new TSU certificates and related CRLs.

6.7 Backup copy

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

6.8 Disaster recovery

6.8.1 Incident and compromise handling procedures

In case of disaster the predefined continuity plan is enacted which stipulates that:

1. issued CRLs are seamlessly kept available;
2. issuance of new CRLs, of new certificates and of new Time-stamps may be delayed up to 24 hours if the secondary site must be configured as primary due to exceptional circumstances;

TSP cryptographic devices are similarly protected from unauthorized removal and, consequently, from the consequences of theft.

6.9 Cessation of the CA

If the TSP intends to terminate its services, it will do what is necessary to minimize disruption to relying parties.

At least 30 days before such termination, informs appropriately all the subscribers, the supervision authority, subcontractors and relevant parties.

Before termination Adobe shall transfers to another organization the obligation to keep all the registration and all the relevant logs for the due time and make unusable private keys unless services are taken over by another QTSP.
7 Technical Security Controls

ETSI EN 319 421 controls shall be implemented to protect systems, cryptographic keys, repositories and their management.

7.1 Key pair generation and installation

7.1.1 Root CA

Root CA key pair generation and activation is covered in a separate Certificate Policy. Refer to the “CDS Certificate Policy” available from this URL: https://www.adobe.com/misc/pdfs/Adobe_CDS_CP.pdf

7.1.2 Sub-CA

Sub-CA key pair generation and activation is safely performed within the HSM by authorized personnel, in a physically secured environment, in presence of the appointed Officers.

Minutes of the process are drafted by Adobe internal auditor and kept for 20 years.

7.1.3 Time-Stamp Unit Certificate

TSU key pair generation and activation is safely performed within a properly certified HSM by authorized personnel, in a physically secured environment, then the TSU certificate is issued in presence of the appointed Officers and according to the internal procedures.

Minutes of the process, including certificate issuance, are drafted by Adobe internal auditor and kept for 20 years.

7.2 Private Key Protection and Cryptographic Module Engineering Controls

7.2.1 Root CA

The key pair used by the Root CA is generated and managed by a properly certified HSM, at least according to FIPS PUB 140-2 Level 3 or Common Criteria (ISO 15408) at EAL 4 or higher.

Refer to CDS Certificate Policy downloadable from URL:

https://www.adobe.com/misc/pdfs/Adobe_CDS_CP.pdf

7.2.2 Sub-CA

The key pair used by the Sub-CA for TSU certificates is generated and managed by a properly certified HSM, at least according to FIPS PUB 140-2 Level 3 or Common Criteria (ISO 15408) at EAL 4 or higher.

7.2.3 Time-Stamp Unit Certificate

The key pair used by the TSU is generated and managed by a properly certified HSM, at least according to FIPS PUB 140-2 Level 3 or Common Criteria (ISO 15408) at EAL 4 or higher.
7.3 Other Aspects of Key Pair Management

All the certificates are archived by Adobe.

7.4 Activation data

Adobe authorized officers are provided with activation codes for CA and TSS cryptographic devices stored safely that can be accessed and used only under appropriate security controls.

7.5 Computer Security Controls

Role separation is enforced and all activities performed are traced by the systems and the applications logging features.

7.6 Life cycle technical controls

TSP systems and storage devices are cleared of all sensitive data when retired from operations.

7.7 Network security controls

The Adobe TSS network is protected by firewalls and IDS systems.

Only necessary functions are enabled on Computers hosting Adobe TSS systems.

Communications between the Adobe TSS primary site, the Adobe secondary site and the operation site are cryptographically secured and protected by individual security zones.

7.8 Time-stamping

TSS makes use of secure and accurate time source.

Issued Time-stamps comply with the format specified in EN 319 422 and are archived on tamper resistant media.

TSS activity is securely logged.

8 Certificate and CRL profile

8.1 Certificate profile


As for cryptographic algorithms, minimum length of keys, key parameters and hashing functions, the CA certificates conform to ETSI TS 119 312.
8.2 CRL profile

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

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

9 Compliance audit

Adobe provides for auditing of all procedures as described in this QTSPP and in the related QTSPPS, with the purpose of verifying:

- actual compliance by personnel
- procedures efficaciousness and effectiveness
- actual possibility to comply with the procedures.

The goal is to improve the overall Adobe security by adopting procedures that can be effectively complied with and that present no known security loopholes.

9.1 Frequency or circumstances of assessment

Inspections are held every month or yearly depending on the audited procedures.

Compliance audit are performed every 24 months engaging a Conformity Assessment Body accredited according to the eIDAS Regulation, with yearly confirmation.

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.

9.2 Identity and qualification of assessor

The Internal Auditing is performed by personnel of the Internal Adobe Auditor.

External Auditing is performed by a Conformity Assessment Body accredited for eIDAS audit according to ISO/IEC 17065 and EN 319 403.

9.3 Assessor’s relationship to assessed entity

There are no hierarchical relationships between audited Adobe departments and Internal Auditor.

External Auditing is performed by an independent CAB.

9.4 Topics covered by assessment

The audit covers the procedures and obligations listed in this QTSPP and in the related QTSPPS.
9.5  Actions taken as result of deficiency

Security violation will be prosecuted as per the rules of law currently in force.

Should the violation have possibly exposed at risk the CA and / or the TSS private key, relevant provisions apply.

9.6  Communication of results

Significant deviations from the procedure or severe security breaches are reported to TSS Officers or senior level managers, depending on the violation severity.

When relevant and according to the eIDAS Regulation security incidents with loss of personal data integrity will be notified to the Supervision Body and relevant authorities.

10  Other business and legal matters

The general Terms & Conditions of the TSP services are made available to subscribers and end users as a separate document, published on the CA web site.

The "Terms & Conditions" document takes precedence in case of discrepancies with this document.

10.1  Service fees

Adobe will charge fees for provision of Time-stamps.

In any case no fee will be charged for CRL fetch.

10.2  Financial responsibility

Adobe maintains proper capital and insurance in relation to its performance and obligations as TSP.

10.3  Confidentiality of Business information

No additional stipulation.

10.4  Privacy of personal information

All personal data collected in the operation of the TSP are kept confidential and handled according to Regulation (EU) 2016/679.

10.5  Intellectual property rights

This Policy (QTSPP) is the property of Adobe who reserves all rights associated with the same.
10.6 Representation and warranties

10.6.1 Certification Authority
The CA shall operate in compliance with this QTSPP and relevant stipulations in the related QTSPPS.

10.6.2 Registration Authority
Not applicable for Time-Stamp service.

10.6.3 Subscribers
Refers to "Terms and Conditions" document at chapter 5.

10.6.4 Relying parties
Refers to "Terms and Conditions" document at chapter 7.

10.7 Disclaimer of warranties
Adobe warrants the clients that it will use reasonable skill and care in the provision of its services in accordance with this QTSPP and with the related QTSPPS and shall issue certificates and Time-stamps in compliance with its obligations stated in the policies and procedures therein.

Adobe acting as a Certificate issuer warrants the clients that policies and procedures contained in its QTSPP and QTSPPS shall be audited and, should the audit outcomes require it, the Supervision Body will be informed of the results.

10.8 Limitations of Liability
Refers to "Terms and Conditions" document at chapter 8.

10.9 Indemnities
Refers to "Terms and Conditions" document at chapter 8.

10.10 Term and Termination
This QTSPP 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.

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

10.12 Dispute Resolution Provisions
Complaints received by Adobe will be treated by Adobe internal services according to QTSPPS.
10.13 Governing Law

This QTSPP is subject to the Law of Ireland and as such shall be interpreted and carried out. For that not expressly prescribed in this Policy or the related QTSPPS, the law shall apply.

Other contracts in which this QTSPP is incorporated by means of reference, may contain distinct and separate clauses with respect to applicable law.

10.14 Compliance with Applicable Law

Mandatory applicable laws shall prevail on the provisions of this Policy.

10.15 Miscellaneous Provisions

Adobe acting as TSP when referencing the present Policy incorporates by reference in all Certificates it issues the terms and conditions stated in this Policy and the related QTSPPS.