



## **Certification Practice Statement for TC TrustCenter Adobe Certified Document Services Certificates**

Version 1.0

October 11<sup>th</sup>, 2007

## Table of Contents

<b>I. INTRODUCTION</b>	<b>4</b>
A. Overview	4
B. Definitions	4
C. Description and Use of CDS Certificates (“CDS Certificates”)	4
<b>II. GENERAL PROVISIONS</b>	<b>5</b>
A. Obligations	5
B. Fees	5
C. Compliance Audit	6
D. Limited Warranty/Disclaimer	6
E. Limitation on Liability	7
F. Force Majeure	8
G. Financial Responsibility	8
H. Interpretation & Enforcement	9
I. Repository, CRL, OCSP	9
J. Confidentiality Policy	10
K. Waiver	10
L. Survival	10
M. Export	10
<b>III. OPERATIONAL REQUIREMENTS</b>	<b>12</b>
A. Application Requirements	12
B. Certificate Information	14
C. Procedure for Processing Certificate Applications	14
D. Application Issues	15
E. Certificate Delivery	15
F. Certificate Acceptance	16
G. Certificate Renewal, Reissuance and Rekey	16
H. Certificate Expiration	16
I. Certificate Revocation	16
J. Certificate Suspension	18
K. Key Management	18
L. Subscriber Key Pair Generation	18
M. Records Archival	19
N. CA Termination	19
<b>IV. PHYSICAL SECURITY CONTROLS</b>	<b>20</b>
A. Site Location and Construction	20

<b>B.</b>	<b>Physical Access Controls</b>	20
<b>C.</b>	<b>Power and Air Conditioning</b>	20
<b>D.</b>	<b>Water Exposures</b>	20
<b>E.</b>	<b>Fire Prevention and Protection</b>	20
<b>F.</b>	<b>Media Storage</b>	20
<b>G.</b>	<b>Waste Disposal</b>	20
<b>H.</b>	<b>Off-Site Backup</b>	21
<b>V.</b>	<b><i>TECHNICAL SECURITY CONTROLS</i></b>	<b>22</b>
<b>A.</b>	<b>CA Key Pairs</b>	22
<b>B.</b>	<b>Subscriber Key Pairs</b>	22
<b>C.</b>	<b>Business Continuity Management Controls</b>	22
<b>D.</b>	<b>Event Logging</b>	23
<b>VI.</b>	<b><i>CERTIFICATE AND CRL PROFILE</i></b>	<b>24</b>
<b>A.</b>	<b>Certificate Profile</b>	24
<b>B.</b>	<b>CRL Profile</b>	24
<b>VII.</b>	<b><i>CPS ADMINISTRATION</i></b>	<b>25</b>
<b>A.</b>	<b>CPS Authority</b>	25
<b>B.</b>	<b>Contact Person</b>	25
<b>C.</b>	<b>CPS Change Procedures</b>	25
<b>VIII.</b>	<b><i>DEFINITIONS</i></b>	<b>26</b>

## **I. INTRODUCTION**

### **A. OVERVIEW**

This Certification Practice Statement (the "CPS") presents the principles and procedures TC TrustCenter employs in the issuance and life cycle management of CDS Certificates. This CPS and any and all amendments thereto are incorporated by reference into all of the above-listed CDS Certificates.

### **B. DEFINITIONS**

For the purposes of this CPS, all capitalized terms used herein shall have the meaning given to them in Section VIII, or elsewhere in this CPS.

### **C. DESCRIPTION AND USE OF CDS CERTIFICATES ("CDS CERTIFICATES")**

#### **1. CDS Certificates**

CDS Certificates are X.509 Certificates that are issued from the TC TrustCenter CA for Adobe which is chained to the Adobe Root CA. These CDS Certificates may be used solely for purposes of digitally signing and verifying documents in Adobe document formats, e.g. documents in pdf format.

#### **2. Operational Period of CDS Certificates**

CDS Certificates generally have an Operational Period of 365 days from the date of issuance, unless another time period or expiration date is specified on such CDS Certificate, or unless the CDS Certificate is revoked prior to the expiration of the CDS Certificate's Operational Period.

#### **3. Installation of Certificates**

The certificate will be stored within the device also storing the private key.

#### **4. Technical Requirements of CDS Certificates**

In order to use a CDS Certificate, the appropriate application for client authentication must be used.

## II. GENERAL PROVISIONS

### A. OBLIGATIONS

#### 1. TC TrustCenter Obligations

TC TrustCenter will: (i) issue CDS Certificates in accordance with this CPS; (ii) perform authentication of Subscribers and if applicable Organizations as described in this CPS; (iii) revoke Certificates as described in this CPS; and (iv) perform any other functions which are described within this CPS.

#### 2. Organization Obligations

Organization will (i) approve CDS Certificates when issued in affiliation with an Organization in accordance with this CPS; (ii) perform authentication of Subscribers as described in this CPS; (iii) revoke Certificates as described in this CPS; and (iv) perform any other functions which are described within this CPS.

#### 3. Subscriber Obligations

Subscribers will submit truthful information about themselves and their Organization, as applicable. Subscribers will not install a CDS Certificate on more than one client token or cryptographic device. Subscribers will at all times abide by this CPS. Subscribers will only use the CDS Certificates according to section I.C. The Subscriber is solely responsible for the protection of its Private Key or in the case of a TC TrustCenter Signature Portal, for the User name and Password or Client Certificate and corresponding private key used to access the Subscriber's private signing key securely stored and operated on the TC TrustCenter Signing Portal and for immediately notifying the Registration Authority in the event that its Private Key has been Compromised.

#### 4. Relying Party Obligations

With regard to CDS Certificates, Relying Parties must verify that the CDS Certificate is valid by examining the Certificate Revocation List before validating a certified document. In addition, Relying Parties may only rely on a CDS-signed document if verified on a Supported Platform. TC TrustCenter does not accept responsibility for reliance on a fraudulently obtained CDS Certificate or a CDS Certificate marked as revoked in the validation service.

### B. FEES

#### 1. Issuance, Management, and Renewal Fees

TC TrustCenter is entitled to charge Subscribers for the issuance, management, and re-issuance of CDS Certificates. The fees charged will be as stated on TC TrustCenter's web site or in any applicable contract at the time the CDS Certificate is issued or renewed, and may change from time to time without prior notice.

#### 2. Certificate Access Fees

TC TrustCenter does not charge a fee as a condition of making a CDS Certificate available in a repository or otherwise making CDS Certificates available to Relying Parties.

#### 3. Revocation or Status Information Fees

TC TrustCenter does not charge a fee as a condition of making the CRL available in a repository or otherwise available to Relying Parties. TC TrustCenter may, however, charge a fee for providing customized CRLs, OCSP services, time stamping services, signing services or other value-added revocation and status information services. With the exception of Adobe, TC TrustCenter does not permit access to revocation information, Certificate status information, or time stamping in its repository by other third parties that provide products or services that utilize such Certificate status information without TC TrustCenter's prior express written consent.

#### 4. Fees for Other Services Such as Policy Information

TC TrustCenter does not charge a fee for access to this CPS.

### **C. COMPLIANCE AUDIT**

An annual WebTrust for Certification Authorities examination or an audit with comparable requirements will be performed for the Certificates issued under this CPS. TC TrustCenter's CA compliance audits are performed by a public third party that (1) demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function, and (2) is accredited by some CPA equivalent organization or governmental authority in Germany, which requires the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education. Compliance audits of TC TrustCenter's operations will be performed by a public third party that is independent of TC TrustCenter. The scope of TC TrustCenter's annual WebTrust (or equivalent) audit for Certification Authorities examination will include certificate life cycle management and CA business practices disclosure.

TC TrustCenter is accredited by the German Federal Net Agency (Bundesnetzagentur) as a CA for qualified electronic certificates and thus compliant with the requirements of the European and especially the German Digital Signature Act.

With respect to WebTrust (or equivalent) audits of TC TrustCenter's operations, significant exceptions or deficiencies identified during the WebTrust (or equivalent) audit will result in a determination of actions to be taken. This determination is made by TC TrustCenter's management with input from the auditor. TC TrustCenter's management is responsible for developing and implementing a corrective action plan. If TC TrustCenter determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the Certificates issued under this CPS, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, TC TrustCenter's management will evaluate the significance of such issues and determine the appropriate course of action. Results of the WebTrust (or equivalent) audit of TC TrustCenter's operations may be released at the discretion of TC TrustCenter's management. TC TrustCenter also performs periodic internal security audits by trained and qualified security personnel according to TC TrustCenter's security policies and procedures. Results of the periodic audits are presented to TC TrustCenter's PKI Policy Authority with a description of any deficiencies noted and corrective actions taken.

### **D. LIMITED WARRANTY/DISCLAIMER**

TC TrustCenter provides the following limited warranty at the time of Certificate issuance: (i) it has complied in all material respects with the CDS CP and this CPS; (ii) the information contained within the Certificate accurately reflects the information provided to TC TrustCenter by the Applicant, or the Registration Authority (if applicable), in all material respects; (iii) it has taken reasonable steps to verify that the information within the Certificate is accurate; and (iv) it has required the Subscriber to accept the Subscriber Agreement. The nature of the steps TC TrustCenter takes to verify the information contained in a CDS Certificate is set forth in section III of this CPS.

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, TC TRUSTCENTER EXPRESSLY DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, WITH RESPECT TO THIS CPS OR ANY CERTIFICATE ISSUED HEREUNDER, INCLUDING WITHOUT LIMITATION, ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR USE OF A CERTIFICATE OR ANY SERVICE (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) PROVIDED BY TC TRUSTCENTER AS DESCRIBED HEREIN, AND ALL WARRANTIES, REPRESENTATIONS, CONDITIONS, UNDERTAKINGS, TERMS AND OBLIGATIONS IMPLIED BY STATUTE OR COMMON LAW, TRADE USAGE, COURSE OF DEALING OR OTHERWISE ARE HEREBY EXCLUDED TO THE FULLEST EXTENT PERMITTED BY LAW. EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, TC TRUSTCENTER FURTHER DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, TO ANY APPLICANT, SUBSCRIBER OR ANY RELYING PARTY THAT (A) THE SUBSCRIBER TO WHICH IT HAS ISSUED A CDS CERTIFICATE IS IN THE FACT THE PERSON, ENTITY OR ORGANIZATION IT CLAIMS TO HAVE BEEN (B) A

SUBSCRIBER IS IN FACT THE PERSON, ENTITY OR ORGANIZATION LISTED IN THE CDS CERTIFICATE, OR (C) THAT THE INFORMATION CONTAINED IN THE CDS CERTIFICATES OR IN ANY CDS CERTIFICATE STATUS MECHANISM COMPILED, PUBLISHED OR OTHERWISE DISSEMINATED BY TC TRUSTCENTER, OR THE RESULTS OF ANY CRYPTOGRAPHIC METHOD IMPLEMENTED IN CONNECTION WITH THE CDS CERTIFICATES IS ACCURATE, AUTHENTIC, COMPLETE OR RELIABLE.

IT IS AGREED AND ACKNOWLEDGED THAT APPLICANTS ARE LIABLE FOR ANY MISREPRESENTATIONS MADE TO TC TRUSTCENTER AND RELIED UPON BY A RELYING PARTY. TC TRUSTCENTER DOES NOT WARRANT OR GUARANTEE UNDER ANY CIRCUMSTANCES THE "NON-REPUDIATION" BY A SUBSCRIBER AND/OR RELYING PARTY OF ANY TRANSACTION ENTERED INTO BY THE SUBSCRIBER AND/OR RELYING PARTY INVOLVING THE USE OF OR RELIANCE UPON A CDS CERTIFICATE.

IT IS UNDERSTOOD AND AGREED UPON BY SUBSCRIBERS AND RELYING PARTIES THAT IN USING AND/OR RELYING UPON A CDS CERTIFICATE THEY ARE SOLELY RESPONSIBLE FOR THEIR RELIANCE UPON THAT CDS CERTIFICATE AND THAT SUCH PARTIES MUST CONSIDER THE FACTS, CIRCUMSTANCES AND CONTEXT SURROUNDING THE TRANSACTION IN WHICH THE CDS CERTIFICATE IS USED IN DETERMINING SUCH RELIANCE.

THE SUBSCRIBERS AND RELYING PARTIES AGREE AND ACKNOWLEDGE THAT CDS CERTIFICATES HAVE A LIMITED OPERATIONAL PERIOD AND MAY BE REVOKED AT ANY TIME. SUBSCRIBERS AND RELYING PARTIES ARE UNDER AN OBLIGATION TO VERIFY WHETHER A CERTIFICATE IS EXPIRED OR HAS BEEN REVOKED. TC TRUSTCENTER HEREBY DISCLAIMS ANY AND ALL LIABILITY TO SUBSCRIBERS AND RELYING PARTIES WHO DO NOT FOLLOW SUCH PROCEDURES. MORE INFORMATION ABOUT THE SITUATIONS IN WHICH A CERTIFICATE MAY BE REVOKED CAN BE FOUND IN SECTION III(I) OF THIS CPS.

TC TrustCenter provides no warranties with respect to another party's software, hardware or telecommunications or networking equipment utilized in connection with the use, issuance, revocation or management of CDS Certificates or providing other services (including, without limitation, any support services) with respect to this CPS. Applicants, Subscribers and Relying Parties agree and acknowledge that TC TrustCenter is not responsible or liable for any misrepresentations or incomplete representations of CDS Certificates or any information contained therein caused by another party's application software or graphical user interfaces. The cryptographic key-generation technology used by Applicants, Subscribers and Relying Parties in conjunction with the CDS Certificates may or may not be subject to the intellectual property rights of third-parties. It is the responsibility of Applicants, Subscribers and Relying Parties to ensure that they are using technology which is properly licensed or to otherwise obtain the right to use such technology

## **E. LIMITATION ON LIABILITY**

EXCEPT TO THE EXTENT CAUSED BY TC TRUSTCENTER'S WILLFUL MISCONDUCT, IN NO EVENT SHALL THE CUMULATIVE LIABILITY OF TC TRUSTCENTER TO APPLICANTS, SUBSCRIBER AND/OR ANY RELYING PARTY FOR ALL CLAIMS RELATED TO THE INSTALLATION OF, USE OF OR RELIANCE UPON A CDS CERTIFICATE OR FOR THE SERVICES PROVIDED HEREUNDER INCLUDING WITHOUT LIMITATION ANY CAUSE OF ACTION SOUNDING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY EXCEED FIVE THOUSAND U.S. DOLLARS (\$5,000.00).

TC TRUSTCENTER SHALL NOT BE LIABLE IN CONTRACT, TORT (INCLUDING NEGLIGENCE), AND STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY (EVEN IF TC TRUSTCENTER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) FOR:

- (i) ANY ECONOMIC LOSS (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUES, PROFITS, CONTRACTS, BUSINESS OR ANTICIPATED SAVINGS);
- (ii) TO THE EXTENT ALLOWED BY APPLICABLE LAW, ANY LOSS OR DAMAGE RESULTING FROM DEATH OR INJURY OF SUBSCRIBER AND/OR ANY RELYING PARTY OR ANYONE ELSE;
- (iii) ANY LOSS OF GOODWILL OR REPUTATION; OR
- (iv) ANY OTHER INDIRECT, CONSEQUENTIAL, INCIDENTAL, MULTIPLE, SPECIAL, PUNITIVE, EXEMPLARY DAMAGES

IN ANY CASE WHETHER OR NOT SUCH LOSSES OR DAMAGES WERE WITHIN THE CONTEMPLATION OF THE PARTIES AT THE TIME OF THE APPLICATION FOR, INSTALLATION OF, USE OF OR RELIANCE ON THE CDS

CERTIFICATE, OR AROSE OUT OF ANY OTHER MATTER OR SERVICES (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) UNDER THIS CPS OR WITH REGARD TO THE USE OF OR RELIANCE ON THE CDS CERTIFICATE.

BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, THE ABOVE EXCLUSIONS OF INCIDENTAL AND CONSEQUENTIAL DAMAGES MAY NOT APPLY TO AN APPLICANT, SUBSCRIBER AND/OR A RELYING PARTY BUT SHALL BE GIVEN EFFECT TO THE FULLEST EXTENT PERMITTED BY LAW.

EXCEPT AS OTHERWISE SPECIFIED IN WRITING BETWEEN THE PARTIES, THE FOREGOING LIMITATIONS OF LIABILITY SHALL APPLY ON A CERTIFICATE-BY-CERTIFICATE BASIS, REGARDLESS OF THE NUMBER OF TRANSACTIONS OR CLAIMS RELATED TO EACH CDS CERTIFICATE, AND SHALL BE APPORTIONED FIRST TO THE EARLIER CLAIMS TO ACHIEVE FINAL RESOLUTION.

In no event will TC TrustCenter be liable for any damages to Applicants, Subscribers, Relying Parties or any other party arising out of or related to the use or misuse of, or reliance on any CDS Certificate issued under this CPS that: (i) has expired or been revoked; (ii) has been used for any purpose other than as set forth in the CPS (See Section I.C for more detail); (iii) has been tampered with; (iv) with respect to which the Key Pair underlying such CDS Certificate or the cryptography algorithm used to generate such CDS Certificate's Key Pair, has been Compromised by the action of any party other than TC TrustCenter (including without limitation the Subscriber or Relying Party); (v) is the subject of misrepresentations or other misleading acts or omissions of any other party, including but not limited to Applicants, Subscribers and Relying Parties; or (vi) not verified on a Supported Platform.

In no event shall TC TrustCenter be liable to the Applicant, Subscriber, Relying Party or other party for damages arising out of any claim that a CDS Certificate infringes any patent, trademark, copyright, trade secret or other intellectual property right of any party.

## **F. FORCE MAJEURE**

TC TrustCenter shall not be liable for any default or delay in the performance of its obligations hereunder to the extent and while such default or delay is caused, directly or indirectly, by fire, flood, earthquake, elements of nature or acts of God, acts of war, terrorism, riots, civil disorders, rebellions or revolutions, strikes, lockouts, or labor difficulties or any other similar cause beyond the reasonable control of TC TrustCenter.

## **G. FINANCIAL RESPONSIBILITY**

### **1. Fiduciary Relationships**

TC TrustCenter is not an agent, fiduciary, trustee, or other representative of the Applicant or Subscriber and the relationship between TC TrustCenter and the Applicant and the Subscriber is not that of an agent and a principal. TC TrustCenter makes no representation to the contrary, either explicitly, implicitly, by appearance or otherwise. Neither the Applicant nor the Subscriber has any authority to bind TC TrustCenter by contract or otherwise, to any obligation.

### **2. Indemnification by Applicant and Subscriber**

Unless otherwise set forth in this CPS and/or Subscriber Agreement, Applicant and Subscriber, as applicable, hereby agree to indemnify and hold TC TrustCenter and its suppliers (including, but not limited to, their officers, directors, employees, agents, successors and assigns) harmless from any claims, actions, or demands that are caused by the use or publication of a CDS Certificate and that arises from (a) any false or misleading statement of fact by the Applicant (or any person acting on the behalf of the Applicant); (b) any failure by the Applicant or the Subscriber to disclose a material fact, if such omission was made negligibly or with the intent to deceive; (c) any failure on the part of the Subscriber to protect its Private Key and CDS Certificate or to take the precautions necessary to prevent the Compromise, disclosure, loss, modification or unauthorized use of the Private Key or CDS Certificate; (d) any failure on the part of the Subscriber to immediately notify TC TrustCenter or the RA, as the case may be, of the Compromise, disclosure, loss, modification or unauthorized use of the Private Key or CDS Certificate once the Subscriber has constructive or

actual notice of such event; or (e) caused by any breach of the Subscriber Agreement, including without limitation, as a result of reliance on any misrepresentation of a material fact by Subscriber.

### 3. Indemnification by Relying Parties

The Relying Party hereby agrees to indemnify and hold TC TrustCenter and Adobe (including, but not limited to, their officers, directors, employees, agents, successors and assigns) harmless from any claims, actions, or demands that are caused by the breach of any Relying Party agreements, Adobe end user license agreement, including, without limitation any failure to check the CDS Certificate status prior to any reliance on a digital signature from a Subscriber.

## H. INTERPRETATION & ENFORCEMENT

### 1. Governing Law

The enforceability, construction, interpretation, and validity of this CPS and any CDS Certificates issued by TC TrustCenter shall be governed by the substantive laws of the Federal Republic of Germany, excluding the United Nations Convention on Contracts for the International Sale of Goods.

### 2. Dispute Resolution Procedures

It is in the interest of TC TrustCenter as a Certification Authority and trusted third party to resolve any dispute promptly and efficiently. Therefore, any party intending to make claims should contact TC TrustCenter first, regardless of the nature of the claim.

### 3. Conflict of Provisions

This CPS represents the entire agreement between any Subscriber (including the Subscriber Agreement, if any) or Relying Party and TC TrustCenter and supersedes any and all prior understandings and representations pertaining to its subject matter. In the event, however, of a conflict between this CPS and any other express agreement a Subscriber has with TC TrustCenter with respect to a CDS Certificate, including but not limited to a Subscriber Agreement, such other agreement shall take precedence.

### 4. Severability

If any provision of this CPS shall be held to be invalid, illegal, or unenforceable, the validity, legality, or enforceability of the remainder of this CPS shall not in any way be affected or impaired hereby.

## I. REPOSITORY, CRL, OCSP

TC TrustCenter shall publish a CRL that will be available to both Subscribers and Relying Parties. TC TrustCenter shall post the updates to the CRL online no later than twenty-four (24) hours after revocation by TC TrustCenter. Information relating to the status of a CDS Certificate will be published no later than twelve (12) hours after revocation by TC TrustCenter. Each CRL is signed by the issuing TC TrustCenter CA or by a special CRL signing key.

It is the responsibility of the relying party to either obtain the latest CRL and check the revocation status, or to check the revocation status on-line. In order to check a CRL's signature, a relying party must be in possession of, or obtain, the appropriate CRL certificate. This certificate may differ from the certificate of the issuer(s) of any certificate on the CRL, and if so, it is available from TC TrustCenter's Web Site or upon request by e-mail.

The procedures for revocation are stated elsewhere in this CPS.

TC TrustCenter retains copies of all Certificates online for two years, but is not obliged to archive or retain expired or superseded CRLs.

TC TrustCenter may provide other online status mechanisms such as Online Certificate Status Protocol (OCSP) for checking certificate status requests. OCSP provides a method to obtain timely information about a CDS Certificate's revocation status when on-line signing and / or validation is performed via certain Adobe products. OCSP requests contain the following data:

- Protocol version

- Service request
- Target certificate identifier

If a CDS Certificate contains an OCSP-URL as extension (AuthorityInfoAccess), then certain Adobe Products may make an OCSP request using the URL as specified in that extension.

The definitive OCSP response message includes the following:

- Version of the response syntax
- Name of the responder
- Responses for each of the certificates in a request
- Signature computed across hash of the response

The Certificate used to sign the OCSP response is issued by TC TrustCenter CA for Adobe. When the CA returns an error message in response to a certificate status request, the error message is not digitally signed.

## **J. CONFIDENTIALITY POLICY**

### **1. Individual Subscriber Information**

Information regarding Subscribers that is submitted on enrollment forms for CDS Certificates (whether submitted by the Subscriber, the Registration Authority or Organization Representative) will be kept confidential by TC TrustCenter and TC TrustCenter shall not release such information without the prior consent of the Subscriber. Notwithstanding the foregoing, TC TrustCenter may make such information available to (a) courts, law enforcement agencies or other third parties (including release in response to civil discovery) upon receipt of a court order or subpoena or upon the advice of TC TrustCenter's legal counsel, (b) law enforcement officials and others as may be necessary for the purpose of investigating suspected fraud, misrepresentation, unauthorized access, or potential illegal activity by the Subscriber (as determined by TC TrustCenter), (c) independent third party auditors as may be necessary for audit purposes, and (d) other third parties as may be necessary for TC TrustCenter to fulfill its obligations under this Agreement. The foregoing confidentiality obligation shall not apply, however, to information appearing on CDS Certificates, information relating to CDS Certificate revocation, or to information regarding Subscribers that is already in the possession of or separately acquired by TC TrustCenter. In addition, TC TrustCenter will release information regarding a Subscriber upon request submitted by the Subscriber in form satisfactory to TC TrustCenter. TC TrustCenter is not responsible ensuring the confidentiality of the information collected and reviewed by a Organization Representative or Registration Authority.

### **2. Aggregate Subscriber Information**

Notwithstanding the previous section, TC TrustCenter may disclose Subscriber information on an aggregate basis, and the Subscriber hereby grants to TC TrustCenter a license to do so, including the right to modify the aggregated Subscriber information and to permit third parties to perform such functions on its behalf.

## **K. WAIVER**

A failure or delay in exercising any right or remedy hereunder shall not operate as a waiver of that right or remedy, nor shall any single or partial exercise of any right or remedy preclude any other or further exercise thereof or the exercise of any other right or remedy.

## **L. SURVIVAL**

The following sections shall survive, along with all definitions required thereby: Sections I, II, and VIII.

## **M. EXPORT**

Subscribers and Relying Parties acknowledge and agree to use CDS Certificates in compliance with all applicable laws and regulations, including without limitation U.S., European, and German

export laws and regulations. TC TrustCenter may refuse to issue or may revoke CDS Certificates if in the reasonable opinion of TC TrustCenter such issuance or the continued use of such CDS Certificates would violate applicable laws and regulations.

### III. OPERATIONAL REQUIREMENTS

#### A. APPLICATION REQUIREMENTS

##### 1. Organizations

The following process is applicable to Applicants requesting CDS Certificates for use in his/her role on behalf of the Organization either on an individual basis or in connection with a Function.

##### 1.1 Enrollment of Organization

Before any Applicant in affiliation with an Organization can request a CDS Certificate, the Organization must enroll in the service.

The Organization Representative, on behalf of the Organization, shall complete a TC TrustCenter CDS Certificate enrollment form in a form prescribed by TC TrustCenter. All enrollment forms are subject to review, approval and acceptance by TC TrustCenter.

The Organization Representative, must, at a minimum, provide the following Organization data on the enrollment form: Organization Name, Address, City/Locality, State/Province, Country, and, Organization Representative Name, Organization Representative Phone Number, and Organization Representative E-mail Address. The following data may also be required either on the enrollment form or in the letter of authorization ("LOA"): Organization Unit and Dun & Bradstreet number (or similar third party verification). TC TrustCenter will require the Organization Representative to submit a LOA that is signed by the Organization Representative and includes the following: Organization Representative's name and title. The Organization Representative shall also identify one or more persons as being designated by the Organization as the Registration Authority ("RA") and include a statement that such RA has the authority to approve requests for CDS Certificates. The Organization Representative must also include the following information regarding the RA in the LOA: name, title, telephone number, mobile phone number, and email address of the RA as well as the RA's signature.

Each Applicant shall agree in the Subscriber Agreement to use the CDS Certificate in compliance with all applicable laws and regulations, including without limitation U.S. export laws and regulations.

TC TrustCenter performs the authentication steps listed below (and checks generally for errors and omissions relevant to the authentication steps taken), but does not otherwise verify the authority of the Applicant to request a CDS Certificate or verify accuracy of the information contained in the Applicant's CDS Certificate request or otherwise check for errors and omissions.

TC TrustCenter will take reasonable steps to establish that the CDS Certificate request made on behalf of the Organization is legitimate and properly authorized. For that purpose an Organization Representative must confirm that the Applicant is authorized to apply for a CDS Certificate. Before issuing a CDS Administrator Certificate to the RA, TC TrustCenter shall verify that the RA's email address matches the domain name of the Organization identified on the LOA. In addition, the correctness of an email address may be verified by an access test.

TC TrustCenter will not include an Organization Name in a CDS Certificate without first ensuring the following:

- (a) the Organization Name appears in conjunction with a country and possibly a state or province of other locality to sufficiently identify its place of registration or a place where it is currently doing business; and
- (b) in the case of an organization or individual that could reasonable be expected to be registered with a local, state or national authority, TC TrustCenter will obtain, view, and verify copies of the registration documents.

For instance, TC TrustCenter will

- (w) verify the validity of the registration through the authority that issued it, or
- (x) verify the validity of the registration through a reputable third party database or other resource, or

- (y) verify the validity of the organization through a trusted third party, or
- (z) confirm that the organization exists if such organization is not the type that is typically registered or is capable of being verified under clause (y).

## 1.2 Registration of Applicants

Applicants shall complete a TC TrustCenter enrollment form in addition to performing the steps below.

The Organization must designate an RA. The RA will be responsible for approving authorized Applicants for CDS Certificates. RAs shall approve CDS Certificate requests either via a LOA or via a secure web-based or API session. If the RA is not using the web-based or API session then TC TrustCenter will require the Organization to submit an LOA that is signed by the Organization Representative and includes the following: RA's name and title, list of Applicants' names that will apply for CDS Certificates, each Applicant's email address, work telephone number, and mobile telephone number (if existing), and a statement that the Applicant(s) listed are member(s) of the Organization and are authorized to request a CDS Certificate.

## 2. Individuals

The following process is applicable to Applicants requesting CDS Certificates for use in representing him or her self and not in connection with an Organization.

The Applicant shall complete a TC TrustCenter CDS Certificate enrollment form as prescribed by TC TrustCenter. The enrollment form requires the Applicant to complete information regarding him or herself. All enrollment forms are subject to review, approval and acceptance by TC TrustCenter.

The Applicant must, at a minimum, provide the following personal data on the enrollment form: Name, Address, City/Locality, State/Province, Country, and, if applicable, Phone Number, and E-mail Address.

Each Applicant shall agree in the Subscriber Agreement to use the CDS Certificate in compliance with all applicable laws and regulations, including without limitation U.S., European, and German export laws and regulations.

TC TrustCenter performs the authentication steps listed below (and checks generally for errors and omissions relevant to the authentication steps taken), but does not otherwise verify the authority of the Applicant to request a CDS Certificate or verify accuracy of the information contained in the Applicant's CDS Certificate request or otherwise check for errors and omissions.

TC TrustCenter will take reasonable steps to establish that the CDS Certificate request made on behalf of the individual is legitimate. To prove that a CDS Certificate is requested by the individual, TC TrustCenter will require the Applicant to submit a (fax) copy of an official government-issued photo identification document (e.g. ID card or passport).

TC TrustCenter will not include an individual name in a CDS Certificate for an individual without first ensuring the individual's name, country and possibly a state or province or other locality provided on the enrollment form match that which is shown on the document used for identification.

TC TrustCenter may also (a) verify the validity of the identification document through the authority that issued it, or (b) verify the identity of the individual through a reputable third party database or other resource, or (c) verify the identity of the individual through a trusted third party.

## B. CERTIFICATE INFORMATION

### Minimum CDS Certificate Profile

X.509 v3 Certificate Attributes/ Extensions	Critical / Non Critical	Value / Notes
<b>Attributes</b>		
Version		v3
SerialNumber		integer; unique to each certificate issued in the TC TrustCenter CA for Adobe PKI domain
Signature		sha-1 w/ RSAEncryption – {1.2.840.113549.1.1.5}
Issuer		cn=TC TrustCenter CA for Adobe I, o=TC TrustCenter GmbH, c=DE
Validity		<ul style="list-style-type: none"> <li>Minimum = 1 day</li> <li>Maximum = 10 years</li> </ul>
Subject		Based application information
SubjectPublicKeyInfo		<ul style="list-style-type: none"> <li>rsaEncryption – {1.2.840.113549.1.1.1}</li> </ul> RSA public key is 2048 bit public key
<b>Extensions</b>		
AuthorityKeyIdentifier	Non-critical	contains a 20 byte SHA-1 hash of the SUB-Root CA public key
KeyUsage	Critical	Minimum Key Usages <ul style="list-style-type: none"> <li>Digital Signature</li> <li>Non-Repudiation</li> </ul>
CertificatePolicies	Critical	1.2.840.113583.1.2.1 This certificate has been issued in accordance with the Adobe Acrobat Credentials CPS located at <a href="http://www.trustcenter.de/cps">http://www.trustcenter.de/cps</a>
ExtendedKeyUsage	Non-critical	1.2.840.113583.1.1.5
CRLDistributionPoints	Non-critical	<a href="http://crl1.adobe-cds.trustcenter.de/crl/v2/tc_adobe_cds_L1_CA_1.crl">http://crl1.adobe-cds.trustcenter.de/crl/v2/tc_adobe_cds_L1_CA_1.crl</a>

More secure Hash algorithms may be used, e.g. SHA-256 in the Signature.

## C. PROCEDURE FOR PROCESSING CERTIFICATE APPLICATIONS

CDS Certificate Subscribers will generate both the public and private keys on a cryptographic device. Subscribers will submit their Public Key to TC TrustCenter for certification electronically through the use of a web browser or other electronic means.

CDS Signature Services subscriber's keys and certificates shall be generated by TC TrustCenter on their behalf.

TC TrustCenter will process the Certificate enrollment forms to confirm the information on the CDS Certificates as discussed in III.A. above. In addition, TC TrustCenter may use subcontractors or other third parties to assist in the performance of its operational requirements or any other obligation under this CPS. TC TrustCenter may delegate specific registration activities to a Registration Authority ("RA") provided that TC TrustCenter shall remain responsible for the services of its RA.

Exception handling: if an applicant is unable to adhere to the defined identification and authentication procedures, e.g. because in some countries commercial registers don't exist, TC TrustCenter will report this exception to the Adobe Policy Authority.

TC TrustCenter will in addition report an alternative method of verification of the applicant's data to the Adobe Policy Authority provided that the general principles for verifying the application information are maintained by this alternative.

The Adobe Policy Authority will then decide whether a certificate may be issued based upon the alternative identification and authentication process.

TC TrustCenter may waive its standard authentication procedures and the requirement that an Applicant utilize an Approved Hardware Device and issue CDS Certificates to Applicants, (including TC TrustCenter and authorized Adobe representatives) for testing purposes. A test CDS Certificate ("Test CDS Certificate") may be issued if (i) TC TrustCenter approves a request; and (ii) the CDS Certificate has the word "test" in the CDS Certificate's CN field. The Test CDS Certificate shall comply with the minimum test CDS Certificate Profile as shown below.

#### Minimum Test CDS Certificate Profile

X.509 v3 Certificate Attributes/ Extensions	Critical / Non Critical	Value / Notes
<b>Attributes</b>		
Version		v3
SerialNumber		integer; unique to each certificate issued in the TC TrustCenter CA for Adobe PKI domain
Signature		sha-1 w/ RSAEncryption – {1.2.840.113549.1.1.5}
Issuer		cn=TC TrustCenter CA for Adobe I, o=TC TrustCenter GmbH, c=DE
Validity		<ul style="list-style-type: none"> <li>Minimum = 1 day</li> <li>Maximum = 10 years</li> </ul>
Subject		Based application information
SubjectPublicKeyInfo		<ul style="list-style-type: none"> <li>rsaEncryption – {1.2.840.113549.1.1.1}</li> </ul> RSA public key is 2048 bit public key
<b>Extensions</b>		
AuthorityKeyIdentifier	Non-critical	contains a 20 byte SHA-1 hash of the SUB-Root CA public key
KeyUsage	Critical	Minimum Key Usages <ul style="list-style-type: none"> <li>Digital Signature</li> <li>Non-Repudiation</li> </ul>
CertificatePolicies	Critical	1.2.840.113583.1.2.2 This test certificate has been issued for the sole purpose of conducting quality assurance testing and should not be trusted or relied upon.
ExtendedKeyUsage	Non-critical	1.2.840.113583.1.1.5
CRLDistributionPoints	Non-critical	http://crl1.adobe-cds.trustcenter.de/crl/v2/tc_adobe_cds_L1_CA_1.crl

More secure Hash algorithms may be used, e.g. SHA-256 in the Signature.

#### D. APPLICATION ISSUES

At certain times during the application process in which TC TrustCenter or the Registration Authority is not able to verify information in a CDS Certificate enrollment form, a customer service representative may be assigned to the Applicant to facilitate the completion of the application process. Otherwise, the Applicant may be required to correct its associated information with third parties and re-submit its application for a CDS Certificate.

#### E. CERTIFICATE DELIVERY

The Public Key material will be sent to TC TrustCenter for signing and the Applicant's CDS Certificate will be signed by TC TrustCenter and delivered back to the Applicant. The Applicant may utilize his/her own Approved Hardware Device or, if the Applicant does not already have one, the Applicant may purchase one from TC TrustCenter. If the Applicant, or Organization on behalf of the Applicant, purchases an Approved Hardware Device from TC TrustCenter then the Applicant shall have the option of requesting TC TrustCenter to generate a Public and Private Key Pair onto the Approved Hardware Device at TC TrustCenter's facilities and deliver the Approved Hardware Device containing the Certificate to Subscriber. In such case, the Approved Hardware Device shall be delivered to the Subscriber by some appropriate delivery service or by courier or

other in-person delivery and may require signature for delivery. TC TrustCenter shall obtain and keep all receipts for delivery. In certain circumstances the delivery may include a TC TrustCenter customer service representative telephone number and email address for any technical or customer service problems. TC TrustCenter, in its sole discretion, may provide such technical or customer support to the Applicants/Subscribers. In case the Applicant generates the Key Pair the use of an Approved Hardware Device shall be enforced by limiting the available Cryptographic Service Provider ("CSP") presented for key pair generation.

In the case of CDS Signature Service, if TC TrustCenter finds that the Applicant's CDS Certificate enrollment form was verified as described in section III.A. Application Requirements, then a unique key pair and corresponding CDS certificate shall be generated and stored by TC TrustCenter on an approved Hardware device. Private Key will be made available to Subscriber for signing through the CDS Signature Service Portal. Access to Signature Portal shall be made available through either User Name and Password or Client Authentication using a TC TrustCenter issued and approved identity certificate.

#### **F. CERTIFICATE ACCEPTANCE**

The Applicant expressly indicates acceptance of a CDS Certificate by using such CDS Certificate.

#### **G. CERTIFICATE RENEWAL, REISSUANCE AND REKEY**

Prior to the expiration of an existing Subscriber's CDS Certificate, it is necessary for the Subscriber to obtain a new CDS Certificate to maintain continuity of CDS Certificate usage. Subscribers must generate a new Key Pair to replace the expiring Key Pair (technically defined as "rekey"). Rekeying will count as a new CDS Certificate request. The Subscriber must pay the fees and comply with the other terms and conditions for renewal as presented on TC TrustCenter's web site.

In order to prevent the Subscriber from renewing or rekeying the certificate without verification of at least some of the certificate data TC TrustCenter will send an e-mail to the Subscriber's specified e-mail address. The Subscriber must reply to that e-mail thus proving that he/she can still be contacted using this address.

Expiring CDS Certificates are not revoked by TC TrustCenter upon issuance of the rekeyed CDS Certificate.

TC TrustCenter does not provide renewal services for CDS Certificates.

#### **H. CERTIFICATE EXPIRATION**

TC TrustCenter will attempt to notify all Subscribers or their Organization Representative or Registration Authority of the expiration date of their CDS Certificate. Notification will generally be made by e-mail message to the Subscriber. If Subscriber's enrollment form was submitted by another party on Subscriber's behalf, TC TrustCenter likely will not send expiration notices to that party due to contractual limitations.

#### **I. CERTIFICATE REVOCATION**

##### **1. Circumstances For Revocation**

Certificate revocation is the process by which TC TrustCenter prematurely ends the Operational Period of a CDS Certificate.

TC TrustCenter shall revoke a CDS Certificate:

- Upon receipt of a request for revocation from the Adobe Policy Authority.
- Upon TC TrustCenter's, Organization Representative's, or Registration Authority's determination that Subscriber has violated the Subscriber Agreement, failed to meet its material obligations under the Subscriber Agreement, any applicable CP or CPS, or any other agreement, regulation, or law applicable to the CDS Certificate that may be in force.

- Upon TC TrustCenter's, Organization Representative's, Registration Authority's, or Subscriber's knowledge or reasonable suspicion of Compromise of Subscriber's Private Key.
- If TC TrustCenter determines that any material fact contained in the CDS Certificate is no longer true including, without limitation, the fact that Subscriber is no longer authorized to represent the Organization.
- If TC TrustCenter, Organization Representative, or Registration Authority determines that the CDS Certificate was not properly issued in accordance with any applicable agreement and/or the Adobe CP or this CPS.
- If cryptographic algorithms or parameters become insecure because of technological progress or new developments in cryptography.
- In the event that TC TrustCenter ceases operations and there is no plan for transition of TC TrustCenter's services to a successor or no plan to otherwise address such event, any Certificate issued to and all Certificates issued by the TC TrustCenter shall be revoked prior to the date that the TC TrustCenter ceases operations.

TC TrustCenter may notify or confirm with the Organization Representative or Registration Authority (if Subscriber applied for the CDS Certificate in affiliation with an Organization) by e-mail message of any request for revocation and the reason(s) for the request for revocation, regardless of which party requested the revocation.

In the event that TC TrustCenter ceases operations, all CDS Certificates issued by TC TrustCenter shall be revoked prior to the date that TC TrustCenter ceases operations, and TC TrustCenter shall notify Organization Representative or Registration Authority by e-mail message of the revocation and the reasons why. CDS certificates revoked by an Organization Representative or Registration Authority will be marked as revoked and displayed as revoked in a Web-based accessible report and an event log shall be generated and distributed to key personnel.

## 2. Who Can Request Revocation

The only parties permitted to request revocation of or revoke a CDS Certificate issued by TC TrustCenter are the Subscriber, Organization Representative, Registration Authority, TC TrustCenter and the Adobe Policy Authority.

## 3. Procedures For Revocation Request

### 3.1 Revocation via Phone or E-Mail

If the Subscriber initiates the revocation request, Subscriber must contact TC TrustCenter or the Registration Authority (if applicable), either by e-mail message, a national/regional postal service, facsimile, or courier, to request revocation of a CDS Certificate and must identify the reason for the request (as set forth in III.I) above). Upon receipt of a revocation request, TC TrustCenter will attempt to notify the Organization Representative or Registration Authority of the request by e-mail. TC TrustCenter may also seek confirmation of the request by e-mail to the Subscriber. The message will state that TC TrustCenter will revoke the CDS Certificate and that posting the revocation to the appropriate CRL will constitute notice to the Subscriber and Relying Parties that the CDS Certificate has been revoked. Notification will not be sent to others than the Subscriber and the Organization Representative and/or Registration Authority. There is no grace period available to the Subscriber prior to revocation, and TC TrustCenter shall revoke such CDS Certificate within the next business day and post the revocation to the next published CRL.

### 3.2 Revocation using the Administrators Web Front End

A Subscriber shall inform the Registration Authority and promptly request revocation of a CDS Certificate for any reason set forth in III.I above. If the Registration Authority wishes to revoke a Subscriber's CDS Certificate, the Registration Authority may do so through the web-based application provided to the Registration Authority by the Organization. The Registration Authority

shall have sole responsibility for notifying a Subscriber that the CDS Certificate has been revoked. Upon revocation by the Registration Authority, TC TrustCenter will confirm the revocation request to the Registration Authority through the web-based application, the CDS Certificate will be revoked, and the revocation will be posted to the appropriate CRL. Posting the revocation to the appropriate CRL will constitute notice to the Subscriber and Relying Parties that the CDS Certificate has been revoked. No further notification will be sent by TC TrustCenter to the Registration Authority, Subscriber, or others. There is no grace period available to the Subscriber prior to revocation, and TC TrustCenter shall revoke such CDS Certificate within the next business day and post the revocation to the next published CRL.

For revocation of the Certificate provided by TC TrustCenter to the Registration Authority for access to the CDS service, the Registration Authority must contact TC TrustCenter, either by e-mail message, a national/regional postal service, facsimile, or courier, to request revocation of the Certificate. Upon receipt of a revocation request, TC TrustCenter will seek confirmation of the request by e-mail to the Registration Authority. The message will state that upon confirmation of the revocation request TC TrustCenter will revoke the Certificate and that posting the revocation to the appropriate CRL will constitute notice to the Registration Authority and Relying Parties that the Certificate has been revoked. TC TrustCenter will require a confirming e-mail back from the Registration Authority authorizing revocation (or by other means acceptable to TC TrustCenter). Upon receipt of the confirming e-mail, the Certificate will be revoked and the revocation will be posted to the appropriate CRL. Notification will not be sent to others than the Subscriber and the Organization Representative and Registration Authority. There is no grace period available to the Registration Authority prior to revocation, and TC TrustCenter shall revoke such Certificate within the next business day and post the revocation to the next published CRL.

### **3.3 TC TrustCenter Private Key**

In the event of Compromise of TC TrustCenter's Private Key used to sign CDS Certificates, TC TrustCenter will send an e-mail message as soon as practicable to all Subscribers with CDS Certificates issued off the Private Key stating that the CDS Certificates will be revoked by the next business day and that posting the revocation to the appropriate CRL will constitute notice to the Subscriber that the CDS Certificate has been revoked.

## **J. CERTIFICATE SUSPENSION**

TC TrustCenter does not support Certificate suspension for CDS Certificates.

## **K. KEY MANAGEMENT**

TC TrustCenter does not provide Private Key management for certain services that allow TC TrustCenter to sign and or deliver both Private and Public Keys on behalf of the Subscriber.

## **L. SUBSCRIBER KEY PAIR GENERATION**

TC TrustCenter may provide Subscriber Key Pair generation for the CDS Certificates. Both individual Subscribers and Subscribers applying for a CDS certificate issued to a Function must use cryptographic hardware modules that (a) meet or exceed FIPS 140-2 Level 2 standards, or (b) for which the cryptographic hardware module manufacturer has applied for FIPS 140-2 Level 2 status within the previous year without receiving a notice of noncompliance or other communication indicating that such device fails to meet such standard ("Approved Hardware Device").

TC TrustCenter recommends that Subscribers applying for a CDS certificate issued to a Function that will perform a high volume of signings (more than 2,000 annually) use cryptographic hardware modules that (a) meet or exceed FIPS 140-2 Level 3 standards, or (b) for which the cryptographic hardware module manufacturer has applied for FIPS 140-2 Level 3 status within the previous year without receiving a notice of noncompliance or other communication indicating that such device fails to meet such standard ("Recommended Hardware Device for Functions").

**M. RECORDS ARCHIVAL**

TC TrustCenter shall maintain and archive records relating to the issuance of the CDS Certificates for three (3) years following the issuance of the applicable CDS Certificate.

**N. CA TERMINATION**

In the event that it is necessary for TC TrustCenter or its CAs to cease operation, TC TrustCenter makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, TC TrustCenter will develop a termination plan to minimize disruption to Subscribers and Relying Parties. Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers and Relying Parties, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by TC TrustCenter,
- The preservation of the CA's archives and records for the time periods required in this CPS,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs,
- The revocation of unexpired, unrevoked CDS Certificates of Subscribers and subordinate CAs, if necessary,
- The payment of compensation (if necessary) to Subscribers whose unexpired, unrevoked CDS Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement CDS Certificates by a successor CA,
- Destruction of the CA's private key and secure erasing or physical destruction of the hardware tokens containing such private key,
- Provisions needed for the transition of the CA's services to a successor CA, and
- The identity of the custodian of TC TrustCenter's CA and RA archival records. Unless a different custodian is indicated through notice to Subscribers and Relying Parties, the Registered Agent for TC TrustCenter GmbH, a German corporation, shall be the custodian.

## **IV. PHYSICAL SECURITY CONTROLS**

### **A. SITE LOCATION AND CONSTRUCTION**

TC TrustCenter's CA operations are conducted within TC TrustCenter's facilities in Hamburg, Germany which meet WebTrust for CAs (or equivalent) audit requirements. All TC TrustCenter CA operations are conducted within a physically protected environment designed to deter, prevent, and detect covert or overt penetration. TC TrustCenter's CAs are physically located in a highly secure facility which includes the following:

- Slab to slab barriers
- Electronic control access systems
- Alarmed doors and video monitoring
- Security logging and audits
- Smartcard access for specially approved employees with defined levels of management approval required

### **B. PHYSICAL ACCESS CONTROLS**

Access to the TC TrustCenter CA facility requires the two authentication factors of "know and have", incorporating smartcards and PINs. Access to the CA facility requires a minimum of two authorized TC TrustCenter employees and is checked at three independent physical locations.

### **C. POWER AND AIR CONDITIONING**

TC TrustCenter's CA facility is equipped with primary and backup:

- Power systems to ensure continuous, uninterrupted access to electric power and
- Heating/ventilation/air conditioning systems to control temperature and relative humidity.

### **D. WATER EXPOSURES**

The TC TrustCenter CA facility is located above ground and is not susceptible to flooding or other forms of water damage. TC TrustCenter has taken reasonable precautions to minimize the impact of water exposure to TC TrustCenter systems.

### **E. FIRE PREVENTION AND PROTECTION**

The fire detection system in TC TrustCenter CA facility tests air health and looks for certain signatures of possible fire conditions in the air. In addition, the TC TrustCenter CA facility has a fire extinguishing system which floods entire rooms with fire extinguishing gas. Each cabinet is equipped with a temperature sensor. These sensors trigger an alarm if the temperature inside the cabinet exceeds a defined value.

### **F. MEDIA STORAGE**

All media containing production software and data, audit, archive, or backup information is stored within multiple TC TrustCenter facilities in TL-30 rated safes (or equivalent) with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage.

### **G. WASTE DISPOSAL**

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance with the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with TC TrustCenter's normal waste disposal requirements.

## **H. OFF-SITE BACKUP**

TC TrustCenter performs routine backups of critical system data, audit log data, and other sensitive information. Critical CA facility backup media are stored in a physically secure manner at an offsite facility.

## V. TECHNICAL SECURITY CONTROLS

### A. CA KEY PAIRS

CA Key Pair generation is performed by multiple trained and trusted individuals using secure systems and processes that provide for the security and required cryptographic strength for the keys that are generated. All CA Key Pairs are generated in pre-planned key generation ceremonies in accordance with the requirements of TC TrustCenter security and audit requirements guidelines. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by TC TrustCenter management.

CDS Certificates are issued off the TC TrustCenter CA for Adobe which is chained to the Adobe Root CA. The cryptographic modules used for key generation and storage meet or exceed the requirements of FIPS 140-1 level 3. The TC TrustCenter CA for Adobe Private Keys are generated and stored in hardware. Private Keys are backed up but not escrowed. The TC TrustCenter CA for Adobe is maintained under m out of n multiperson control.

The TC TrustCenter CA for Adobe and its Private Keys may be used for Certificate Signing, Off-line CRL Signing, and CRL Signing.

The usage period or active lifetime for the TC TrustCenter CA for Adobe Public and Private Keys is through January 15, 2015. TC TrustCenter CA for Adobe CA Key Pairs are maintained in a trusted and highly secured environment with backup and key recovery procedures. In the event of the Compromise of one or more of the TC TrustCenter CA Key(s), TC TrustCenter shall promptly notify all Subscribers via e-mail and notify Relying Parties and others via the CRL and additional notice posted at <http://www.trustcenter.de>, and shall revoke all Certificates issued with such TC TrustCenter CA Key(s). When TC TrustCenter's CA Key Pairs reach the end of their validity period, such CA Key Pairs will be archived for a period of at least 5 years. Archived CA Key Pairs will be securely stored using hardware cryptographic modules. Procedural controls will prevent archived CA Key Pairs from being returned to production use. Upon the end of the archive period, archived CA Private Keys will be securely destroyed. TC TrustCenter CA Key Pairs are retired from service at the end of their respective maximum lifetimes as defined above, and so there is no key changeover. Certificates may be renewed as long as the cumulative certified lifetime of the Certificate Key Pair does not exceed the maximum CA Key Pair lifetime. New CA Key Pairs will be generated as necessary, for example to replace CA Key Pairs that are being retired, to supplement existing, active Key Pairs and to support new services in accordance with this CPS.

### B. SUBSCRIBER KEY PAIRS

Generation of Subscriber Key Pairs will be performed in accordance with Section III.E of this CPS.

For X.509 Version 3 Certificates, TC TrustCenter generally populates the KeyUsage extension of Certificates in accordance with RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999.

### C. BUSINESS CONTINUITY MANAGEMENT CONTROLS

TC TrustCenter has business continuity plans (BCP) to maintain or restore the TC TrustCenter CAs business operations in a reasonably timely manner following interruption to or failure of critical business processes. The BCP define the following time periods for acceptable system outage and recovery time:

1. Vet a Subscriber - 10 days
2. Issue a Certificate - 10 days
3. Publish a CRL - 48 hours
4. Audit Vetting Procedures - 2 months

Backup copies of essential business and CA information are made routinely. In general, back-ups are performed daily on-site, weekly to an off-site location, but may be performed less frequently in TC TrustCenter's discretion according to production schedule requirements.

**D. EVENT LOGGING**

TC TrustCenter CA event journal data is archived both daily and monthly. Daily event journals are reviewed several times each week. Monthly event journals are reviewed monthly.

## **VI. CERTIFICATE AND CRL PROFILE**

### **A. CERTIFICATE PROFILE**

TC TrustCenter Certificates conform to (a) ITU-T Recommendation X.509 Version 3 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997, and (b) RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 3280"). Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC 3280 standards and recommendations. The name forms for Subscribers are enforced through TC TrustCenter's internal policies and the authentication steps described elsewhere in this CPS. Name constraint enforcement is not through the name constraint extension, but through the authentication steps followed and contractual limitations with each Subscriber. TC TrustCenter does not apply any specific Certificate Policy Object Identifier(s), but instead refers to the applicable CPS version and URL address. The policy constraints extensions and policy qualifiers syntax and semantics, when used, conform to the RFC 3280 standards.

### **B. CRL PROFILE**

TC TrustCenter issued CRLs conform to all RFC 3280 standards and recommendations.

## **VII. CPS ADMINISTRATION**

### **A. CPS AUTHORITY**

The authority administering this CPS is the TC TrustCenter Policy Authority. Inquiries to TC TrustCenter's Policy Authority should be addressed as follows:

TC TrustCenter GmbH  
Sonninstr. 24 - 28  
20097 Hamburg  
Germany  
+49 40 80 80 26 - 0(voice)  
+49 40 80 80 26 - 126 (fax)  
[kipolicy@trustcenter.de](mailto:kipolicy@trustcenter.de)

TC TrustCenter does not support a Certificate Policy (CP) for Adobe CDS Certificates.

### **B. CONTACT PERSON**

Address inquiries about the CPS to [kipolicy@trustcenter.de](mailto:kipolicy@trustcenter.de) or to the following address:

PKI Policy Administrator  
TC TrustCenter GmbH  
Sonninstr. 24 - 28  
20097 Hamburg, Germany  
+49 40 80 80 26 - 0(voice)  
+49 40 80 80 26 - 126 (fax)

### **C. CPS CHANGE PROCEDURES**

This CPS (and all amendments to this CPS) is subject to approval by the PKI Policy Authority. TC TrustCenter may change this CPS at any time without prior notice. The past and current CPS and any amendments thereto are available through <http://www.trustcenter.de>. Amendments to this CPS will be evidenced by a new version number and date, except where the amendments are purely clerical.

## VIII. DEFINITIONS

**Adobe.** Adobe Systems Incorporated.

**Adobe Policy Authority.** Selected members of Adobe's management that define, review and approve policies related to the Adobe PKI.

**Adobe Root CA.** Adobe's root Certification Authority.

**Applicant.** A person or authorized agent that requests the issuance of a Certificate on behalf of the Subscriber.

**Approved Hardware Device.** Cryptographic hardware modules that (a) meet or exceed FIPS 140-2 Level 2 standards, or (b) for which the cryptographic hardware module manufacturer has applied for FIPS 140-2 Level 2 status within the previous year without receiving a notice of noncompliance or other communication indicating that such device fails to meet such standard.

**CA.** Certification Authority.

**CDS.** Certified Document Services.

**CDS Certificate.** A signing certificate issued by TC TrustCenter for the purposes of digitally signing Adobe documents.

**Certificate.** A record that, at a minimum: (a) identifies the CA issuing it; (b) names or otherwise identifies its Subscriber; (c) contains a Public Key that corresponds to a Private Key under the control of the Subscriber; (d) identifies its Operational Period; and (e) contains a Certificate serial number and is digitally signed by the CA. The term Certificate, as referred to in this CPS, means a Certificate issued by TC TrustCenter pursuant to this CPS.

**Certified Document Services Certificate Policy ("CDS CP").** The policy published and managed by Adobe Systems Incorporated that governs all third parties providing CA services for CDS.

**Certificate Revocation List.** A time-stamped list of revoked Certificates that has been digitally signed by the CA.

**Certification Authority.** An entity which issues Certificates and performs all of the functions associated with issuing such Certificates.

**Certified Transcripts Services (CTS)** is a CDS digital certificate issued to an accredited Educational Institution.

**Compromise.** Suspected or actual unauthorized disclosure, loss, loss of control over, or use of a Private Key associated with a Certificate.

**CRL.** See Certificate Revocation List.

**Extension.** To place additional information about a Certificate within a Certificate. The X.509 standard defines a set of Extensions that may be used in Certificates.

**Function.** An organizational unit or department within an Organization

**Key Pair.** Two mathematically related keys, having the following properties: (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally impractical to discover the other key.

**OCSP or On-line Certificate Status Protocol** – A protocol for providing Relying Parties with real-time Certificate Status information

**Operational Period.** A Certificate's period of validity. It typically begins on the date the Certificate is issued (or such later date as specified in the Certificate), and ends on the date and time it expires as noted in the Certificate or is earlier revoked unless it is suspended.

**Organization.** A legally recognized company, enterprise or governmental agency that has applied for or has been issued CDS Certificates.

**Organization Representative.** A representative of the Organization with the authority to contractually bind the Organization. The Organization Representative may also serve as the Registration Authority.

**Private Key.** The key of a Key Pair used to create a digital signature. This key must be kept a secret.

**Public Key.** The key of a Key Pair used to verify a digital signature. The Public Key is made freely available to anyone who will receive digitally signed messages from the holder of the Key Pair. The Public Key is usually provided via a Certificate issued by TC TrustCenter. A Public Key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding Private Key.

**Registration Authority or RA.** A representative designated by the Organization to submit approved requests for CDS Certificates. For Subscribers not associated with Organization and are enrolling in My CDS Certificate, TC TrustCenter shall serve as the RA.

**Relying Party.** A recipient of a digitally signed message who relies on a Certificate to verify the digital signature on the message. Also, a recipient of a Certificate who relies on the information contained in the Certificate.

**SSL.** An industry standard protocol that uses public key cryptography for Internet security.

**Subscriber.** An individual or organization that has been issued a certificate in the CDS PKI. For the purpose of this CPS, a person or entity who applies for a Certificate by the submission of an application is also referred to as a Subscriber.

**Supported Platform.** Those applications specified on the CDS information webpage, currently located on [http://adobe.com/security/partners\\_cds.html](http://adobe.com/security/partners_cds.html).

**TC TrustCenter.** TC TrustCenter GmbH.

Copyright 2007, TC TrustCenter GmbH