GlobalSign
Certification Practice Statement
DocumentSign™ Digital ID for Adobe Certified Document Services (CDS)

Date: May 20th, 2008

Version: v.1.2

Table of Contents

Document History

Document Change Control

Version	Release Date	Author	Status + Description
V.1.0	10/10/07	Steve Roylance	Final
V 1.1	19/10/07	Steve Roylance	Modified Certificate Policy OID in section 7.1 Digital ID Profile table and minor text changes
V 1.2	20/05/08	Steve Roylance	Modified sections relating to subscriber agreement acceptance

History

- Initial issuance of final DocumentSign™ for Adobe Certified Document Services Certificate Practice Statement as governed by Adobe Systems Incorporated – CDS Certificate Policy revision #14 October 2005.
- First revision of DocumentSign for Adobe Certified Document Services Certificate practice statement as governed by Adobe Systems Incorporated – CDS Certificate Policy Revision #14 October 2005.

Acknowledgments

This GlobalSign CA for Adobe CPS endorses in whole or in part the following industry standards:

- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework (obsoletes RFC 2527)
- RFC 2459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.
- RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile
- RFC 3161: Internet X.509 Public Key Infrastructure – Compliant Time Stamping Authority
- The ISO 1-7799 standard on security and infrastructure
- Adobe Systems Incorporated CDS Certificate Policy Revision #15 dated February 2007

1.0 Introduction

This Certification Practice Statement (CPS) of the GlobalSign Certification Authority for Adobe (hereinafter, GlobalSign CA for Adobe) applies only to the services of the GlobalSign CA for Adobe that are associated with the issuance of and management of digital IDs under the Adobe Root certificate hierarchy as part of the Certified Document Services (hereinafter, CDS) agreement between GlobalSign and Adobe Systems Incorporated. Digital IDs can be used to create or rely upon electronic signatures. It does not apply to services and certificates issued under the GlobalSign Root CA which are covered under a separate CPS. This CPS can be found on the GlobalSign CA for Adobe repository at: https://www.globalsign.com/repository. This CPS may be updated from time to time.

A certificate policy is a "named set of rules that indicates the applicability of a digital ID (also referred to as digital certificate) to a particular community and/or class of application with common security requirements". This CPS meets the formal requirements of Internet Engineering Task Force (IETF) RFC 3647, dated November 2003 with regard to content, layout and format. An RFC issued by IETF is an authoritative source of guidance with regard to standard practices in the area of electronic signatures and certificate management. While certain section titles are included in this policy according to the structure of RFC 3647, the topic may not necessarily apply in the implementation of the certificate management services of the GlobalSign CA for Adobe. These sections have been removed from this document. Where necessary, additional information is presented as subsections added to the standard structure. Meeting the format requirements of RFC 3647 enhances and facilitates the mapping and interoperability of the GlobalSign CA for Adobe with other third party CAs and provides relying parties with advance notice on the practices and procedures of the GlobalSign CA for Adobe. Additional assertions on standards used in this CPS can be found under section “Acknowledgements”.

This CPS addresses the technical, procedural personnel policies and practices of the CA in all services and during the complete life cycle of digital IDs as issued by the GlobalSign CA for Adobe.

Request for information on the compliance of the GlobalSign CA for Adobe with accreditation schemes as well as any other inquiry associated with this CPS can be addressed to:

GlobalSign NV
attn. Legal Practices,
Ubicenter,
Philipssite 5
B-3001 Leuven,
Belgium.
Tel:+ 32 (0)16 891900
Fax: + 32 (0) 16 891909
Email: legal@globalsign.com
URL: www.globalsign.com

The GlobalSign CA for Adobe operates within the scope of activities of GlobalSign NV. This CPS addresses the requirements of the CA that issues certificates of various certificate types. More information can be obtained from https://www.globalsign.com/repository.

This CPS is final and binding between GlobalSign NV/SA, a company under public law, with registered office at Ubicenter, Philipssite 5, B-3001 Leuven, VAT Registration Number BE 459.134.256 and registered in the commercial register under number BE 0.459.134.256 RPR Leuven, (Hereinafter referred to as "GlobalSign")

and

the subscriber and/or relying parties, who use rely or attempt to rely upon certification services made available by the GlobalSign CA for Adobe.

For subscribers, this CPS becomes effective and binding by accepting a subscriber agreement. For relying parties, this CPS becomes binding by merely addressing a digital ID related request on a GlobalSign digital ID to a GlobalSign directory. The subscriber agreement forfeits the consent of the relying party with regard to accepting the conditions laid out in this CPS.

1.1 Overview

This CPS applies to the specific domain of the GlobalSign CA for Adobe. The purpose of this CPS is to present the GlobalSign practices and procedures in managing digital IDs and to demonstrate compliance with requirements pertaining to the issuance of digital IDs according to GlobalSign's own and industry requirements pursuant to the standards set out above. This CPS aims at facilitating the GlobalSign CA for Adobe in delivering certification services through discreet CA issuing Client end entity digital IDs. The digital ID types addressed in this CPS are the following:

PersonalSign Digital ID for Adobe	A personal digital ID issued to natural persons (individuals) without a professional context in affiliation with an organization for the purpose of signing Adobe PDF documents.
PersonalSign Pro Digital ID for Adobe	A personal digital ID issued with reference to professional context for the purpose of signing Adobe PDF documents
DepartmentSign Digital ID for Adobe	A role-based digital ID with reference to professional context for the purpose of signing Adobe PDF documents
TrustedRoot for Adobe	A level 2 intermediate CA that enters the GlobalSign CA for Adobe hierarchy

This CPS identifies the roles, responsibilities and practices of all entities involved in the life cycle, use, reliance upon and management of GlobalSign digital IDs for Adobe CDS. The provisions of this CPS with regard to practices, level of services, responsibilities and liability bind GlobalSign CA for Adobe, GlobalSign RA, subscribers and relying parties. Certain provisions might also apply to other entities such as the certification service provider, application providers etc.

This CPS describes the requirements to issue, manage and use digital IDs issued by GlobalSign CA for Adobe under an Adobe Root.

An Adobe CDS Certificate Policy (CP) defines the requirements to be met by this CPS. The purpose of the Adobe CDS CP is to state the "what is to be adhered to" and, therefore, set out an operational rule framework for the broad range of CDS products and services. Such level is generally defined by the entity wishing to ensure a level of trust by managing the life cycle of digital IDs. The Adobe CDS CP addresses the requirements of the entire application domain of Adobe digital IDs focusing on top root and intermediate CA digital IDs and not just the end-entity digital ID area. The Adobe CDS CP is located on the Adobe web-site at
http://www.adobe.com/misc/pdfs/Adobe_CDS_CPv011604clean.pdf

This CPS states, "How the Certification Authority adheres to the Certificate Policy". In doing so this CPS features a greater amount of detail and provides third parties with an overview of the prevailing processes, procedures and overall prevailing conditions that the Certification Authority uses in creating and maintaining the digital IDs that it manages.
Additionally, other pertinent documents include:

- The GlobalSign Privacy Policy regarding data privacy

A subscriber or relying party of a GlobalSign CA for Adobe digital ID must refer to the GlobalSign Adobe CDS CPS in order to establish Trust on a digital ID issued by the GlobalSign CA for Adobe or a level 2 CA issued from the GlobalSign CA for Adobe as well as for notices with regard to the prevailing practices thereof. It is also essential to establish the trustworthiness of the entire digital ID chain of the GlobalSign CA for Adobe certificate hierarchy which can be established on the basis of the assertions of this CPS.

A full list of accreditations and recognition of service is available upon request.

The exact name of the GlobalSign CA for Adobe digital IDs that makes use of this CPS is:

- GlobalSign CA for Adobe

Digital IDs allow entities that participate in an electronic transaction to prove their identity towards other participants or sign data electronically. By means of a digital ID, GlobalSign provides confirmation of the relationship between a named entity (Subscriber) and its Public Key. The process to obtain a digital ID includes the identification, naming, authentication and registration of the client as well as aspects of digital ID management such as the issuance, revocation and expiration of the digital ID. By means of this procedure to issue digital IDs, GlobalSign provides adequate confirmation about the identity of the user of a digital ID and a link to the Public Key that such entity uses. An entity in this instance might be an end user or another Certification Authority, as it might be required under certain circumstances.

This CPS is maintained by the GlobalSign CA for Adobe, which is the issuing authority of digital IDs in the GlobalSign Adobe CDS Public Key Infrastructure. In a certificate management environment based on Public Key Infrastructure (PKI), the Issuing Authority is the entity that manages a trust hierarchy from which all end user digital IDs inherit trust.

This CPS governs the issuance of digital IDs during the application period of the GlobalSign CA for Adobe CA. An application period is for example, the time during which a certain CA may issue GlobalSign CDS digital IDs. The application period is indicated in the digital ID issued to the appropriate Root by a hierarchically superior CA within the Adobe hierarchy.

The GlobalSign CA for Adobe accepts comments regarding this CPS addressed to the address mentioned above in the Introduction of this document.

1.2 GlobalSign CA for Adobe Digital ID types

GlobalSign Adobe CDS offers several types of digital IDs for individuals and organizations that can be used for digital signing and certifying Adobe PDF documents as well as issuing level 2 CA intermediate CAs to organizations wishing to issue digital IDs from the GlobalSign CA for Adobe certificate hierarchy:

1.2.1 PersonalSign™ Digital ID for Adobe

PersonalSign Digital ID for Adobe provides a high level of identity assurance by requiring a mailed or faxed signed copy of an official form of a government issued photo identity element to the Registration Authority to prove its identity. These Digital IDs can be used for commercial transactions such as the application of a digital signature or certification of a PDF document. They are valid for one, two or three years.

1.2.2 PersonalSign™ Pro Digital ID for Adobe

PersonalSign Pro Digital ID for Adobe provides a high level of identity assurance by requiring a mailed or faxed signed copy of an official form of a government issued photo identity element or verification by the Registration Authority (RA) of the applicant’s identity against a previously established trustworthy source. Additionally, an Organization Representative, on behalf of the Organization must provide a Dun & Bradstreet number (or similar third party verification) as well as a Letter of Authorization (LOA) authorizing and accepting or appointing RA responsibilities in a method prescribed by GlobalSign. These digital IDs can be used for commercial transactions such as the application of a digital signature or certification of a PDF document for the purposes of attestation of authorship. They are valid for one, two, three, four or five years.

1.2.3 DepartmentSign Digital ID for Adobe

DepartmentSign Digital ID for Adobe provides a high level of identity assurance by requiring a mailed or faxed signed copy of an official form of a government issued photo identity element or verification by the Registration Authority (RA) of the applicant's identity against a previous established trustworthy source of the subscriber enrolling for a digital ID in the name of a department, organizational unit, or function/role. Additionally, an Organization Representative, on behalf of the Organization must provide a Dun & Bradstreet number (or similar third party verification) as well as a Letter of Authorization (LOA) authorizing and accepting or appointing an RA in a method prescribed by GlobalSign. These digital IDs can be used for commercial transactions such as the application of a digital signature or certification of a PDF document for the purposes of attestation of authorship. They are valid for one, two, three, four, or five years.

1.2.4 TrustedRoot™ for Adobe

TrustedRoot for Adobe provides a high level of identity assurance by requiring Level 2 CAs to accept and abide by the terms of the GlobalSign DocumentSign Digital ID for Adobe CDS Certificate Practice Statement and Adobe CDS Certificate Policy. GlobalSign shall audit Level 2 CAs to ensure compliance with the Adobe CDS Certificate Policy and the GlobalSign Document Digital ID for Adobe CDS Certificate Practice Statement.

1.2.5 Acceptable Subscriber Names

For publication in its digital ID GlobalSign accepts Subscriber names that are meaningful and can be authenticated as required for each product type or class.

1.2.5.1 Pseudonyms

For certain types of products GlobalSign may allow the use of pseudonyms, reserving its right to disclose the identity of the Subscriber as may be required by law or a following a reasoned and legitimate request.

1.2.6 Registration procedures

For all types of digital IDs GlobalSign reserves the right to update registration procedures and Subscriber submitted data to improve the identification and registration process.

1.3 PersonalSign™ Digital ID for Adobe PDF

1.3.1 General

PersonalSign Digital ID for Adobe is intended for commercial transactions such as the application of a digital signature or certification of a PDF document e.g. contract execution.

PersonalSign Digital ID for Adobe offer a high level of identity assurance requiring a mailed or faxed signed copy of an official form of a government issued photo identity element to the Registration Authority.

PersonalSign Digital ID for Adobe is issued to a natural person (individual) without a professional context.

PersonalSign Digital ID for Adobe validity period is between one and three years.

PersonalSign Digital ID for Adobe is issued primarily for personal communications and usages.

1.3.2 Certificate Request:

A digital ID request can be done according to the following means:

The digital ID applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the digital ID and sends a notice to the applicant. The applicant downloads and installs the digital ID onto an approved cryptographic hardware module that a) meet or exceed FIPS 140-1 Level 2 standards or (b) for which the cryptographic hardware module manufacturer has applied for FIPS 140-1 Level 2 status within the previous year without receiving a notice of non-compliance or other communication indicating that such device fails to meet such standard (an “Approved Hardware Device”). GlobalSign shall restrict applicant's Cryptographic Service Provider to a 2048 key generation and FIPS 140-1 level 2 cryptographic device. Applicant may have the option of requesting GlobalSign or approved Registration Authority to generate a Public and Private Key Pair onto the Approved Hardware Device at GlobalSign’s facilities and deliver the Approved Hardware Device containing the digital ID to the applicant. The applicant must notify GlobalSign of any inaccuracy or defect in a digital ID promptly after receipt of the digital ID or earlier notice of the information to be included in the digital ID.

1.3.3 Content

Typical content of information published on a PersonalSign Digital ID for Adobe includes the following elements:

- Subscriber’s e-mail address
- Subscriber’s name
- Applicant’s Public Key
- Code of applicant’s country
- Issuing Certification Authority (GlobalSign CA for Adobe)
- GlobalSign electronic signature
- Type of algorithm
- Validity period of the digital ID
- Serial number of the digital ID

1.3.4 Documents Submitted to Identify the Applicant

The applicant must submit to a GlobalSign Registration Authority a signed copy of a photo identification document such as an identity card, driver’s licence or passport. The applicant’s signature must be preceded by the date of signing and the phrase ‘I have read and I approved the Subscriber Agreement.

.

1.3.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm digital ID application information and issues a digital ID within reasonable time frames. For PersonalSign Digital ID for Adobe verification, 5 to 7 working days might be required.

1.3.6 Issuing Procedure

The issuance procedure for a PersonalSign Digital ID for Adobe is as follows:

1. The applicant fills out the online registration form: e-mail address, common name, country code, verification method, billing information.
2. The applicant accepts online Subscriber Agreement.
3. An RSA Key Pair with at least 2048 bits is generated on an applicant’s Approved Hardware Device.
4. The Public Key and online request are sent to GlobalSign.
5. GlobalSign authenticates the identity of the applicant and issues an e-mail to the applicant with a URL that permits the applicant to retrieve the digital ID.

6. Alternatively a pre-approved RA may positively verify the applicant.
7. GlobalSign may issue the digital ID to the applicant.
8. GlobalSign may publish the issued digital ID in an online database.
9. Renewal: allowed.
10. Revocation: allowed.

GlobalSign might apply minor variations of this procedure in order to meet service, standards or legal requirements without compromise to identity verification or private key protection.

1.3.7 Relevant GlobalSign Documents

The applicant must take notice and is bound by the following documents available on https://www.globalsign.com/repository:

1. CPS
2. Subscriber Agreement
3. Privacy Policy

1.4 PersonalSign Pro Digital ID for Adobe

1.4.1 General

PersonalSign Pro Digital IDs for Adobe are intended for commercial transactions such as the application of a digital signature or certification of a PDF document for the purposes of attestation of authorship, e.g. contract execution.

- PersonalSign Pro Digital IDs for Adobe validity period is between one and five years.

- PersonalSign Pro Digital IDs for Adobe are issued to natural persons (individuals) within their professional context only.

- PersonalSign Pro Digital IDs for Adobe applicant identification is done by a Registration Authority by using a copy of an identity proof.

- PersonalSign Pro Digital IDs for Adobe are issued primarily for professional usages.

1.4.2 Certificate Request:

The digital ID applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the digital ID and sends a notice to the applicant. The applicant downloads and installs the digital ID onto an Approved Hardware Device. Applicant may have the option of requesting GlobalSign or approved Registration Authority to generate a Public and Private Key Pair onto the Approved Hardware Device at GlobalSign's facilities and deliver the Approved Hardware Device containing the digital ID to the applicant. In the event of a centralized server-based signing implementation, Subscriber may agree to have their Private Key held on their behalf by the Registration Authority. Subscriber shall access central signing service with a minimum of two-factor authentication. The applicant must notify GlobalSign of any inaccuracy or defect in a digital ID promptly after receipt of the digital ID or earlier notice of the information to be included in the digital ID.

1.4.3 Content

Minimal content of information published on a PersonalSign Pro Digital ID for Adobe includes the following elements:

- Subscriber's e-mail address
- Subscriber's name

- Organization Name
- Country Code
- Applicant's Public Key
- Code of applicant's country
- Issuing Certification Authority (GlobalSign CA for Adobe)
- GlobalSign electronic signature
- Type of algorithm
- Validity period of the digital ID
- Serial number of the digital ID

1.4.4 Documents Submitted to Identify the Applicant and Organization

In all cases, the applicant must submit to GlobalSign or Organizational appointed Registration Authority a signed or electronically submitted registration form, a signed or electronically submitted and accepted Subscriber Agreement and the articles of association/incorporation or proof of professional context and a copy of organization identity proof (e.g. Dun & Bradstreet number or similar third party verification).

Employees are required to submit the articles of association of their employer and obtain confirmation of their employment relationship via a Letter of Authorization signed by an Organizational Representative of the organization acting as the Registration Authority.

For self-employed applicants who work independently of an association or professional group, a copy of the register of business license is required in addition to the above-mentioned documents.

For a self-employed applicant belonging to an association or professional group, an official document from the professional group and a membership card is required in addition to the above-mentioned documents. GlobalSign may require additional proof of identity in support of the verification of the applicant.

1.4.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm digital ID application information and issue a digital ID within reasonable time frames. For PersonalSign Pro Digital ID for Adobe verification, 5 to 7 working days might be required.

1.4.6 Issuing Procedure

The issuance procedure for a PersonalSign Pro Digital ID for Adobe is as follows:

1. The applicant submits online the required information: e-mail address, common name, organizational information, country code, a pin, billing information.
2. The applicant accepts the online or paper-based Subscriber Agreement.
3. A RSA key pair with at least 2048 bits is generated on an applicant's Approved Hardware Device.
4. The Public Key and the online request are sent to GlobalSign automatically
5. Applicant must mail or fax to the GlobalSign copies of identity, articles of association/incorporation, professional context and payment information.
6. RA may positively verify the applicant and verifies Subscriber has accepted the Subscriber Agreement.
7. GlobalSign may issue the digital ID to the applicant.
8. GlobalSign may publish the issued digital ID in on line database.
9. Renewal: allowed.
10. Revocation: allowed.

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.4.7 Relevant GlobalSign Documents

The applicant must take notice and is bound by the following documents available on https://www.globalsign.com/repository:

1. CPS
2. Subscriber Agreement
3. Privacy Policy

1.5 DepartmentSign Digital ID for Adobe PDF

1.5.1 General

DepartmentSign Digital IDs for Adobe are intended for commercial transactions such as the application of a digital signature or certification of a PDF document for the purposes of attestation of authorship e.g. contract execution.

DepartmentSign Digital IDs for Adobe applicant identification is done by the organization appointed Registration Authority.

When the applicant is an organization acquiring and managing a certificate on behalf of the organization, the organization shall be required to:

- i) Maintain process, including, without limitations, changing of activation data, that assure that each private key can be used only with the knowledge and explicit action of only one human being within the organization (the certificate custodian);
- ii) Maintain information that permits a determination of who signed a particular document;
- iii) Assure that the certificate custodian has received security training appropriate for the purposes for which the certificate is issued;
- iv) Prevent sharing of organizational certificates amongst members of the organization;
- v) Acknowledge that the information identifying the organization in the certificate is true and accurate, or notify GlobalSign immediately upon any inaccuracies in that information;
- vi) Ensure that the certificate custodian accepts a binding Subscriber Agreement which obligates the certificate custodian to:
  - a) Generate a public key pair using a trustworthy system, or use a key pair generated in a secure hardware token by GlobalSign or its RA and take all reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key;
  - b) Use the certificate exclusively for CDS purposes, consistent with this CPS and the Adobe CDS CP.
  - c) Not share any activation data related to the private key corresponding to the public key in the organizational certificate.
  - d) Request certificate revocation immediately upon any actual or suspected loss, disclosure, or other compromise of the Subscriber’s private key.
- vii) Notify RA or GlobalSign immediately upon any actual or suspected loss, disclosure, or other compromise of the private key corresponding to the public key in the organizational certificate and
- viii) Request revocation of an organizational certificate upon any actual or suspected loss, disclosure or other compromise of the private key of the organizational certificate.

DepartmentSign Digital IDs for Adobe are issued to Subscribers enrolling for a Department, organizational unit, or role-based digital ID with a professional context.

DepartmentSign Digital IDs for Adobe validity period is between one and five years.

DepartmentSign Digital IDs for Adobe are issued primarily for professional usages.

1.5.2 Certificate Request:

A digital ID request can be made as follows:
The digital ID applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Alternatively, a paper-based application in a form prescribed by GlobalSign is submitted by the applicant. Additional documentation in support of the application may be required so that GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. Upon verification of identity, GlobalSign issues the digital ID and sends a notice to the applicant. The applicant downloads and installs the digital ID onto an Approved Hardware Device. If the applicant on behalf of the organization, purchases an Approved Hardware Device from GlobalSign then the applicant shall have the option of requesting GlobalSign to generate a Public and Private Key Pair onto the Approved Hardware Device at GlobalSign's facilities and deliver the Approved Hardware Device containing the digital ID to Subscriber. In such case, the Approved Hardware Device shall be delivered to the applicant by U.S. mail or other delivery service or by courier or other in-person delivery and may require signature for delivery. GlobalSign shall obtain and keep all receipts for delivery. In certain circumstances the delivery may include a GlobalSign customer service representative telephone number and e-mail address for any technical or customer service problems. GlobalSign, in its sole discretion, may provide such technical or customer support to the applicant. The applicant must notify GlobalSign of any inaccuracy or defect in a digital ID promptly after receipt of the digital ID or earlier notice of the information to be included in the digital ID.

1.5.3 Content

Minimum content of information published on a DepartmentSign Digital ID for Adobe PDF digital ID includes the following elements:

- Department e-mail address
- Department (or Role) name
- Country Code
- Organization Name
- Applicant's Public Key
- Code of applicant's country
- Issuing Certification Authority (GlobalSign)
- GlobalSign electronic signature
- Type of algorithm
- Validity period of the digital ID
- Serial number of the digital ID

1.5.4 Documents Submitted to Identify the Applicant and Organization

In all cases, the applicant must submit to a GlobalSign a signed registration form, accept the Subscriber Agreement and provide the articles of association/incorporation or proof of professional context and a copy of identity proof (e.g. Dun & Bradstreet number or similar third party verification).

Employees are required to submit the articles of association/incorporation of their employer and obtain confirmation of their employment relationship via a Letter of Authorization signed by an Organizational Representative of the organization acting as the Registration Authority.

For self-employed applicant who works independently of an association or professional group an extract of the register of commerce is required in addition to the above-mentioned documents.

For a self-employed applicant belonging to an association or professional group an official document from the professional group and a membership card is required in addition to the above-mentioned documents. GlobalSign may require additional proof of identity in support of the verification of the applicant.

1.5.5 Time to Confirm Submitted Data

GlobalSign makes reasonable efforts to confirm digital ID application information and issue a digital ID within reasonable time frames. For DepartmentSign Digital ID for Adobe verification, 7 to 10 working days might be required.

1.5.6 Issuing Procedure

The issuance procedure for a DepartmentSign Digital ID for Adobe is as follows:

1) The applicant submits online or on a paper-based form the required information: e-mail address, common name, organizational information, country code, verification method, billing information.
2) The applicant accept the Subscriber Agreement.
3) A RSA key pair with at least 2048 bits is generated on an applicant's Approved Hardware Device.
4) The Public Key and the online or paper-based request are sent to GlobalSign
5) Applicant must mail to the RA copies of identity, articles of association/incorporation, professional context and payment information.
6) RA shall positively verify the applicant.
7) GlobalSign may issue the digital ID to the applicant.
8) GlobalSign may publish the issued digital ID in online database.
9) Renewal: allowed.
10) Revocation: allowed.

GlobalSign might apply variations of this procedure in order to meet service, standards or legal requirements.

1.5.7 Relevant GlobalSign Documents

The applicant must take notice and is bound by the following documents available on https://www.globalsign.com/repository:

1) CPS
2) Subscriber Agreement
3) Privacy Policy

1.6 Digital ID usages

Certain limitations apply to the use of GlobalSign CA for Adobe digital IDs. A GlobalSign digital ID can only be used for purposes explicitly permitted as they are listed below:

Adobe PDF Electronic signature: Electronic signature can only be used for specific electronic transactions that support electronic signing of electronic forms, electronic documents, etc. The signature digital ID is only warranted to produce electronic signatures in the context of the Adobe applications that support digital IDs. It is not recommended that the digital ID be used for encryption due to the singularity of the digital ID and inability to provide key escrow services under the Adobe Certificate Policy.

1.7 Document Name and Identification

GlobalSign ensures compliance of its digital ID with the requirements and assertions of this CPS.

1.8 PKI participants

The GlobalSign CA for Adobe makes its services available to GlobalSign Subscribers. These Subscribers include without limitation entities that use digital IDs for the purposes of:

- Authentication (digital signature)
- Electronic signature (non-repudiation)

An applicant is a natural person that successfully applies for a digital ID. Any other uses of digital IDs are prohibited. Digital IDs can be used for any public purposes. As “public” this CPS considers any use that takes place among Subscribers who are not restricted to uses governed by voluntary agreements under private law among participants.

1.8.1 GlobalSign Certification Authority for Adobe

A Certification Authority for Adobe, such as GlobalSign, is an organization that issues digital IDs to be used in public or private domains, within a business framework, a transactions context, etc. A Certification Authority is also referred to as the Issuing Authority to denote the purpose of issuing digital IDs at the request of an RA.

The GlobalSign CA for Adobe is governed by the Adobe Policy Authority with regard to issuing GlobalSign CA for Adobe digital IDs.

The GlobalSign CA for Adobe ensures the availability of all services pertaining to the management of digital IDs under the GlobalSign CA for Adobe Intermediate CA, including without limitation the issuance, revocation, and status verification of a digital ID, as they may become available or required in specific applications. The GlobalSign CA for Adobe also manages a core online registration system for all digital ID types, issued under the GlobalSign CA for Adobe.

Appropriate publication is necessary to ensure that Relying Parties obtain notice or knowledge of functions associated with the revoked and/or suspended digital IDs. Publication is manifested by including a revoked or suspended digital ID in a digital ID revocation list that is published in an online directory. Issued digital IDs also appear on directories of issued digital IDs. The GlobalSign CA for Adobe operates such directories.

The domain of responsibility of the GlobalSign CA for Adobe comprises the overall management of the digital ID lifecycle including the following actions:

- Issuance
- Revocation
- Renewal
- Status validation
- Directory service

Some of the tasks attributed to the digital ID lifecycle can be delegated to selected GlobalSign RAs that operate on the basis of a service agreement with GlobalSign or customer appointed RAs for managing the digital ID life-cycle of Subscribers within their organizations. Customer appointed RAs shall operate on the basis of a service description.

1.8.1.1 GlobalSign outsource agent

Through an outsource agent or agents, GlobalSign operates a secure facility in order to deliver CA services including the issuance, revocation, renewal and status validation of GlobalSign CA for Adobe digital IDs. The GlobalSign outsource agent operates a service to GlobalSign on the basis of a service agreement. The scope of the service is the support in digital ID management. The GlobalSign outsource agent warrants designated services and service levels that meet those required by GlobalSign. The GlobalSign outsource agent carries out tasks associated with the administration of services and digital IDs on behalf of GlobalSign.

1.8.1.2 GlobalSign CA for Adobe hierarchy

The Adobe Root CA root has been used to issue the Private Keys of the GlobalSign CA for Adobe CA.

All GlobalSign certificates to be used for Adobe document signing services shall be issued from the GlobalSign CA for Adobe CA including.

- PersonalSign Digital ID for Adobe
- PersonalSign Pro Digital ID for Adobe
- DepartmentSign Digital ID for Adobe

1.8.2 GlobalSign Registration Authorities

The GlobalSign CA for Adobe interacts with its Subscribers through designated Registration Authorities ('RA'). An RA requests the issuance, suspension and revocation of a digital ID under this CPS. An RA submits the necessary data for the generation and revocation of the digital IDs to the CA.

1.8.2.1 RA role description

A GlobalSign RA interacts with the Subscriber to deliver public digital ID management services. GlobalSign RA:

- Accepts, evaluates, approves or rejects the registration of digital ID applications including verifying subscriber's identity and delivering certificate securely including exchanging shared secrets such as PINs or passphrases.
- Registers Subscribers to GlobalSign CA for Adobe certification services.
- Attends all stages of the identification of Subscribers as assigned by the GlobalSign CA for Adobe according to the type of digital IDs they issue.
- Uses official, notarised or organizational verified authorised documents to evaluate a Subscriber application.
- Following approval of an application, notify the GlobalSign CA for Adobe to issue a digital ID.
- Initiates the process to revoke a digital ID and request a digital ID revocation from the GlobalSign CA for Adobe.

The GlobalSign RA acts locally on approval and authorisation by the GlobalSign CA for Adobe. The GlobalSign RA acts in accordance with the approved practices and procedures of the GlobalSign CA for Adobe including this CPS and documented GlobalSign RA procedures.

If successful, the evaluation is followed by the issuance of the digital ID to the applicant organization.

Some RA functions are sometimes carried out by Local Registration Authorities (LRAs). LRAs act under the supervision and control of RAs.

1.8.3 Subscribers

Subscribers of GlobalSign services are natural or legal persons that successfully apply for a digital ID. Subscribers use electronic signature services within the domain of the GlobalSign. Subscribers are parties that:

- Have ultimate authority over the Private Key corresponding to the Public Key that is listed in a subject digital ID.

Natural persons that are Subscribers hold a valid identification document, such as an identity card, passport or equivalent, which is used as a credential in order to issue electronic digital IDs.

Legal persons are identified on the basis of the published by-laws and appointment of Director as well as the subsequent government gazette or other third party databases. Self-employed persons are identified on the basis of proof of professional registration supplied by the competent authority in the country in which they reside.

For all categories of subscribers, additional credentials are required as explained on the online process for the application for a digital ID.

Subscribers of end entity digital IDs issued under the GlobalSign CA for Adobe include employees and agents involved in day-to-day activities within GlobalSign that require accessing GlobalSign network resources.

Subscribers are also sometimes operational or legal owners of signature creation devices that are issued with for the purpose of generating a Key Pair and storing a digital ID.

It is expected that a Subscriber organization has an employment or service agreement or otherwise a pre-existing contract relationship with GlobalSign authorising it to carry out a specific function within the scope of an application that uses GlobalSign digital ID services. Granting a digital ID to a Subscriber organization is only permitted pursuant to such an agreement between GlobalSign and the subscribing end organization.

1.8.4 Subjects

Subjects of GlobalSign CA for Adobe digital ID services are natural persons only that are themselves subscribers or are associated with a Subscriber. Subjects use electronic signature services under authorisation of and within the domain that is designated by the Subscriber (if applicable). Subjects are parties that:

- Apply for a digital ID.
- Are identified in a digital ID or is custodian of a digital ID with a subject DN containing a department, role-based or organizational unit common name.
- Hold the Private Key corresponding to the Public Key that is listed in a Subscriber digital ID

A Subject enrolls with the GlobalSign RA that requires it to use a digital ID within the designated service. A Subject nominates a named digital ID applicant to apply for a digital ID. A digital ID applicant can be any natural person acting on behalf of the Subject.

Natural persons can be listed as subjects of the following digital IDs:

- PersonalSign digital ID for Adobe
- PersonalSign Pro digital ID for Adobe

Department or role-based entities can be listed as Subjects of the following digital IDs:

- DepartmentSign digital ID for Adobe

1.8.5 Digital ID Applicants

A digital ID applicant is a party wishing to become a Subscriber of a digital ID. A digital ID applicant is a party designated by the Subject to act on the Subject’s behalf in:

- Applying for a digital ID.
- Agreeing with and accepting the CA’s Subscriber Agreement.

The applicant may be:

- The same as the Subject itself, where this is a named individual.
- A custodian of a department or role-based Subject name.
- An individual employed by the Subject.
- An individual employed by a contractor, or sub-contractor acting upon explicit authorisation of the organizational Registration Authority

1.8.6 Relying Parties

Relying Parties are natural or legal persons that rely on a digital ID and/or a digital signature verifiable with reference to a Public Key listed in a Subscriber's digital ID. For example, the GlobalSign operators that receive signed requests from GlobalSign CA for Adobe subjects are Relying Parties of the GlobalSign digital IDs.

To verify the validity of a digital ID, Relying Parties must always refer to GlobalSign CA for Adobe revocation information, currently a Certificate Revocation List (CRL). Digital ID validation takes place prior to relying on information featured in a digital ID. Alternatively, Relying Parties may refer to an automated response by using the OCSP protocol where available. Relying Parties must meet specific obligations as described in this CPS.

1.9 Digital ID use

Certain limitations apply to the use of GlobalSign CA for Adobe digital IDs.

1.9.1 Appropriate digital ID usage

Digital ID issued under the GlobalSign CA for Adobe can only for digitally signing PDF documents and used in conjunction with Adobe supported platforms"

Unauthorised use of GlobalSign digital IDs may result in an annulment of warranties offered by the GlobalSign CA for Adobe to Subscribers and Relying Parties of GlobalSign digital IDs.

1.9.2 Prohibited digital ID usage

End entity digital ID use is restricted by using digital ID extensions on key usage and extended key usage. Any usage of the digital ID inconsistent with these extensions is not authorised.

1.9.3 Digital ID extensions

GlobalSign issues digital IDs that contain extensions defined by the X.509 v.3 standard as well as any other formats including those used by Adobe.

GlobalSign uses certain constraints and extensions for its public PKI services as per the definition of the International Standards Organization (ISO). Such constraints and extensions may limit the role and position of a CA or Subscriber digital ID so that such subscribers can be identified under varying roles.

A key usage extension limits the technical purposes for which a public key listed in a digital ID may be used. GlobalSign's own digital IDs may contain a key usage extension that limits the functionality of a key to only signing digital ID revocation lists, and other data.

A digital ID policy extension limits the usage of a digital ID to the requirements of a business or a legal context. GlobalSign pro-actively supports and participates in the proliferation of industry, government or other digital ID policies for its public digital IDs as it sees appropriate.

1.9.4 Critical Extensions

GlobalSign uses certain critical extensions in the digital IDs it issues such as:

- A basic constraint in the key usage to show whether a digital ID is meant for a CA or not.
- To show the intended usage of the key.
- To show the number of levels in the hierarchy under a CA digital ID

1.10 Policy Administration

The GlobalSign CA for Adobe is an intermediate CA authority (also known as a Subordinate CA) that manages digital IDs services within its own domain. The GlobalSign CA for Adobe might also interact with or seek recognition by third party Certification Authorities.

The GlobalSign Policy Management Authority manages this GlobalSign CPS. The GlobalSign CA for Adobe registers, observes the maintenance, and interprets this CPS. The GlobalSign CA for Adobe makes available the operational conditions prevailing in the life-cycle management of digital IDs issued under the GlobalSign CA for Adobe intermediate CA. The operational conditions for each CA are publicised in this CPS.

1.10.1 Scope

In an effort to invoke credibility and trust in this publicised GlobalSign CPS and to better correspond to accreditation and legal requirements, GlobalSign may make revisions and updates to its policies as it sees fit or required by the circumstances. Such updates become binding for all digital IDs that have been issued or are to be issued 30 days after the date of the publication of the updated version of the Adobe CP and/or GlobalSign CA for Adobe CPS.

1.10.2 GlobalSign Policy Management Authority

New versions and publicized updates of GlobalSign policies are approved by the GlobalSign Policy Management Authority. The GlobalSign Policy Management Authority in its present organizational structure comprises members as indicated below:

- At least one member of the management of GlobalSign.
- At least two authorised agents directly involved in the drafting and development of GlobalSign practices and policies.

The management member chairs the GlobalSign Policy Management Authority ex officio.

All members of the GlobalSign Policy Management Authority have one vote. There are no other voting rights reserved for any other party. In case of lock vote the vote of the Chair of the GlobalSign Policy Management Authority counts double.

1.10.3 Acceptance of Updated Versions of the CPS

Upon approval of a CPS update by the GlobalSign Policy Management Authority that CPS is published in the GlobalSign online Repository at https://www.globalsign.com/repository.

GlobalSign publishes a notice of such updates on its public web site at https://www.globalsign.com. The updated version is binding against all existing and future Subscribers unless notice is received within 30 days after communication of the notice. After such period the updated version of the CPS is binding against all parties including the Subscribers and parties relying on digital IDs that have been issued under a previous version of the GlobalSign CPS.

Subscribers that are materially affected by changes may file comments with the policy administration organization within 15 days from notice. Only Subscribers and the supervisory authority may submit objections to policy changes. Relying Parties that are not Subscribers do not have the right to submit objections and any such submissions will be regarded as never received.

Individuals communications made to the GlobalSign CA for Adobe must be addressed to
legal@globalSign.com or by post to the GlobalSign in the address mentioned in the introduction
of this document

GlobalSign publishes on its web site at least the two latest versions of its CPS.

1.10.3.1 Changes with notification

Updated versions of this CPS are notified to parties that have a legal duty to receive such updates, e.g. auditors with a specific mandate to do so.

1.10.4 Version management and denoting changes

Changes are denoted through new version numbers for the CPS. New versions are indicated with an integer number followed by one decimal that is zero. Minor changes are indicated through one decimal number that is larger than zero. Minor changes include:

- Minor editorial corrections
- Changes to contact details

1.11 Definitions and acronyms

A list of definitions can be found at the end of this CPS.

2.0 Publication and Repository Responsibilities

GlobalSign may publish information about the digital IDs that it issues in an online publicly accessible repository. GlobalSign reserves its right to publish digital ID status information on third party repositories.

GlobalSign retains an online repository of documents where it makes certain disclosures about its practices, procedures and the content of certain policies including this CPS. GlobalSign reserves its right to make available and publish information on its policies by any appropriate means within the GlobalSign repository.

All parties who are associated with the issuance, use or management of GlobalSign digital IDs are hereby notified that GlobalSign may publish submitted information on publicly accessible directories in association with the provision of electronic digital ID status information.

GlobalSign refrains from making publicly available certain elements of documents including security controls, procedures, internal security policies, etc. However these elements are disclosed in audits associated with formal accreditation schemes that GlobalSign adheres to, such as WebTrust for CAs.

2.1 Access control on repositories

While GlobalSign strives to keep access to its public repository and access to its policy (e.g. CP, CPS etc.) free of charge, it might charge for services such as the publication of status information on third party databases, private directories, etc.

3.0 Identification and Authentication

GlobalSign employs RAs that verify and authenticate the identity and/or other attributes of an end-user digital ID applicant for a digital ID. RA responsibilities may be delegated to the customer.

Prior to requesting the CA to issue a digital ID, GlobalSign RAs verify the identity of applicants of a digital ID.

GlobalSign RAs maintain appropriate procedures to address naming practices, including the recognition of trademark rights in certain names.

GlobalSign RAs authenticate the requests of parties wishing to revoke digital IDs under this policy.

3.1 Naming

To identify a Subscriber, the GlobalSign CA for Adobe follows and the GlobalSign RAs apply certain naming and identification rules that include types of names assigned to the Subject, such as X.500 distinguished names, RFC-822 names or X.400 names. The GlobalSign CA for Adobe issues digital IDs to applicants that submit a documented application containing a verifiable name.

3.2 Initial Identity Validation

The identification of the applicant for a digital ID is carried out according to a documented procedure to be implemented by the GlobalSign RAs.

A GlobalSign RA shall refuse issuing a digital ID to an applicant unless sufficient evidence is produced with regard to the applicant's identity. If an application is rejected, applicants may subsequently reapply.

To issue digital IDs, a GlobalSign RA endeavours to provide the applicant with sufficient credentials (enrolment URL, password) such that the enrolment process can then proceed online.

At GlobalSign's discretion any such credentials may be two-factor, communicated by independent channels using agreed and proven contact methods.

The identification of an applicant for a digital ID is carried out according to a documented procedure to be implemented by the GlobalSign RAs.

3.2.1 Verification of statements about natural persons

For the identification and authentication procedures of the initial Subscriber registration GlobalSign takes the following steps:

- The natural person identified in the subject field must demonstrate possession of the Private Key corresponding to the Public Key presented to the GlobalSign CA for Adobe. The subject itself or its designated representative must demonstrate this.
- To prove that a CDS Certificate is requested by the individual, GlobalSign will require the Applicant to submit a fax copy of an official form of government issued photo identification ("Identification").
- Only official ID documents that contain a photo and a handwritten signature of the ID holder are accepted for verification purposes.

- GlobalSign RAs might rely on such resources as third party databases to identify and authenticate natural persons applying for a digital ID.-

3.2.2 Verification of statements about Subscribers affiliated with an Organization

Applicants affiliated with an organization shall complete a GlobalSign enrollment form in addition to performing the steps below.

- The organization must designate an RA via the Letter of Authorization. The RA will be responsible for approving requests by Subscribers for digital IDs. Approvals may be made via a form, web-based application or API.

3.2.3 Verification of statements regarding Third Party Agent

For the identification and authentication of appropriately authorised third party agents applying for a GlobalSign digital ID controls include the following:

- Any third party must obtain full authorization by the Subscriber that they are an authorized agent for Subscriber and has exclusive rights to act on their behalf.
- Controlling physical identification documents such as an identity card or passport issued by a designated authority in the country of origin of the applicant.
- Authenticating the identity of the applicant based on other documentation or credentials provided.
- Requesting an applicant to physically appear before a GlobalSign RA prior to issuing a digital ID.
- Requesting a third party agent or his/her principal (e.g. a GlobalSign contractor) to produce evidence with regard to the relationship between GlobalSign and the third party agent (e.g. an outsource contract, etc.).

3.3 Subscriber registration process

The following rules apply as to the Subscriber registration process.

GlobalSign ensures that:

- Subscribers of digital IDs are properly identified and authenticated
- Subscriber digital ID requests are complete, accurate and duly authorized.

In particular:

- GlobalSign provides notice to the applicant through its web site at www.globalsign.com and the dedicated policy framework published on its repository at www.globalsign.com/repository.
- Before entering any contractual relationship with the Subscriber, GlobalSign makes available a Subscriber Agreement, which the applicant must review, sign and agree to prior to placing a request with GlobalSign. This agreement can also be consulted in advance on GlobalSign's repository at www.globalsign.com/repository.
- GlobalSign's policy framework is limited under privacy protection laws and warranty, as explained in this GlobalSign CA for Adobe CPS .
- GlobalSign maintains documented contractual relationships with all third party Registration Authorities or outsourced agents it uses to deliver digital IDs.

3.3.1 Documents used for subscriber registration

GlobalSign or an authorized GlobalSign RA or customer appointed GlobalSign CA for Adobe RA verifies by appropriate means and on the basis of a documented procedure, the identity and, if applicable, all specific attributes thereof of applicants of digital IDs.

Evidence of identity is checked against a natural person either directly or indirectly in the case of an organization that has previously verified subscriber either at employment or other registration stages using means which provide equivalent assurance to physical presence. Submitted evidence may be in the form of either paper or electronic documentation. Examples of evidence checked indirectly against a natural person is documentation presented for registration that was acquired as the result of an application requiring physical presence.

Evidence of identity of organizations is checked by comparing Subscriber submitted organization name, address and Dun & Bradstreet number (or similar 3rd party) documents against the existence of organizations or through Dun & Bradstreet or similar independent third-party databases. Submitted evidence may be in the form of either paper or electronic documentation.

Self-employed professionals that are eligible to be issued with digital IDs typically have to prove their identity as individuals as well as their professional registration.

Specific documents required include the following:

3.3.1.1 PersonalSign Digital ID for Adobe

The applicant must submit to a GlobalSign CA for Adobe Registration Authority a signed copy of an identification document such as an identity card, driver's licence or passport.

3.3.1.2 PersonalSign Pro Digital ID for Adobe

In all cases, the applicant must submit to a GlobalSign CA for Adobe Registration Authority a signed registration form and a signed subscriber agreement.

Applicant must also submit to GlobalSign a letter of authorization signed by an organizational representative accepting RA responsibilities.

Letter of authorization shall include articles of association/incorporation or proof of professional context and a copy of identity proof and confirmation of applicant's organizational affiliation and authorization to receive a CDS certificate in the name of organization.

For self-employed applicant who works independently of an association or professional group an extract of the register of commerce is required in addition to the above-mentioned documents.

For a self-employed applicant belonging to an association or professional group an official document from the professional group and a membership card is required in addition to the above-mentioned documents.

GlobalSign may require additional proof of identity in support of the verification of the applicant.

3.3.1.3 DepartmentSign Digital ID for Adobe

In all cases, the applicant must submit to a GlobalSign CA for Adobe Registration Authority a signed registration form and a signed subscriber agreement.

Applicant must also submit to GlobalSign a letter of authorization signed by an organizational representative accepting RA responsibilities.

Letter of authorization shall include articles of association/incorporation or proof of professional context and a copy of identity proof and confirmation of applicant's organizational affiliation and authorization to receive a CDS certificate in the name of organization.

For self-employed applicant who works independently of an association or professional group an extract of the register of commerce is required in addition to the above-mentioned documents.

For a self-employed applicant belonging to an association or professional group an official document from the professional group and a membership card is required in addition to the above-mentioned documents.

GlobalSign may require additional proof of identity in support of the verification of the applicant.

3.3.1.3.1 Registration of Organizations enrolling for a Certified Transcript Service CDS Digital ID

Organizations wishing to enroll for a Certified Transcript Service (CTS) CDS digital ID shall have the additional obligation of submitting a request for accreditation verification on an enrolment form prescribed by GlobalSign. GlobalSign shall verify the Organization's accreditation with the Council of Higher Education Accreditation (CHEA) via its on-line web-site http://www.chea.org.

3.3.1.4 Test Certificates

In addition, GlobalSign may waive its standard authentication procedures and the requirement that an applicant utilize an Approved Hardware Device and issue CDS digital IDs to applicants, (including GlobalSign and authorized Adobe representatives) for testing purposes. A test CDS digital ID may be issued if (i) GlobalSign approves a request; and (ii) the CDS digital ID has the words " **Test CDS Certificate – Not to be relied upon**" in the CDS DN field.

3.3.2 Data needed for subscriber registration

Where an applicant is natural person evidence shall be provided of the following data prior to accepting an application for a digital ID:

- Full name (including surname and given names).
- A nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

Where the Subscriber is a person who is identified in association with an organizational entity, proof will be produced in terms of:

- Full name (including surname and given names) of the subscriber.
- Date of birth, a nationally recognized identity number, or other attributes of the subscriber which may be used to, as far as possible, distinguish the person from others with the same name.
- Any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.
- Evidence that the Subscriber is associated with that organizational entity.

Where the Subscriber is an organization, proof will be produced in terms of:

- Full name and legal status of the associated legal person of the organizational entity.
- Company registration number, federal tax identification number, VAT number or other attributes of the Subscriber which may be used to, as far as possible, distinguish it from others with a similar same name.
- Any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.
- Evidence that any natural person involved in the application process is associated with that organizational entity.

GlobalSign neither recommends nor encourages any specific choice of an end user product. Applicants and subscribers are entirely responsible to make the appropriate requests for the issuance of their digital IDs. Should support in identifying the features of each option be deemed necessary in order to make an informed selection, applicants are prompted to contact GlobalSign at: legal@globalsign.com.

3.3.3 Records for subscriber registration

GlobalSign records all information used to verify the Subscriber identity, including any reference number on the documentation used for verification, and any limitations on the validity thereof.

GlobalSign maintains records of the executed Subscriber Agreement and any material or documents that support the application which also include but are not limited to:

- Subscriber provided consent to the keeping of a record by GlobalSign of information used in registration and any subsequent digital ID status change and passing of this information to third parties under the same conditions as required by this CPS in the case of the CA terminating its services.
- That information held in the digital ID is correct and accurate.
- Events that tie RA approval to certificate request will be recorded. RA is responsible for verifying information populated in the certificate is correct and accurate.
- Full name of the Subscriber.
- Date and place of birth, a nationally recognized identity number, or other attributes of the Subscriber which may be used to, as far as possible, distinguish the person from others with the same name.
- A specifically designed attribute that uniquely identifies the applicant within the context of the GlobalSign CA for Adobe.
- Proof of organization context where necessary.
- Full name and legal status of the associated legal person or other organizational entity.
- Any relevant registration information (e.g. company registration) of the associated legal person or other organizational entity.
- Evidence that the Subscriber is associated with that organizational entity.
- Any evidence produced in support of an application with a pseudonym.

The records identified above shall be kept for a period of no less than 5 years following the expiration of a digital ID. A GlobalSign RA maintains such records. For organizational purposes a GlobalSign LRA may also maintain duplicates of these records for a shorter period of time.

3.4 Identification and Authentication for Revocation Requests

For the identification and authentication procedures of revocation requests of its subject types (CA, RA, Subscriber, and other participants) GlobalSign requires using an online authentication mechanism or a request addressed to the GlobalSign CA for Adobe or an RA. When the certificate request is originally submitted, the applicant is asked to enter a password. That password serves as digital authentication when the applicant online wants to revoke the certificate. An offline request can be submitted to the RA. The RA will only revoke the certificate if the applicants identity is established through a signature verification.

4.0 Digital ID Life-Cycle Operational Requirements

The following operational requirements apply to Digital ID life-cycle.

All entities within the GlobalSign domain including the RAs and Subscribers or other participants have a continuous duty to inform the GlobalSign CA for Adobe of all changes in the information featured in a digital ID during the operational period of such digital ID and until it expires or gets revoked.

The GlobalSign CA for Adobe issues, revokes, or suspends digital IDs following an authenticated and duly signed request issued by a GlobalSign RA.

To carry out its tasks GlobalSign may use third party agents. GlobalSign assumes full responsibility and accountability for all acts or omissions of all third party agents it may use to deliver services associated with CA operations within the GlobalSign CA for Adobe.

4.1 Digital ID Application

A GlobalSign RA has the duty to provide the GlobalSign CA for Adobe with accurate information on digital ID requests it lodges on behalf of the end user applicants.

The GlobalSign CA for Adobe acts upon request of an RA that has the authority to make a request to issue a digital ID.

Subscribers undergo an enrolment process that requires:
a. Filling out an application.
b. Generating a Key Pair, directly or through an agent.
c. Delivering the generated Public Key corresponding to a Private Key to GlobalSign CA for Adobe.
d. Accepting the Subscriber Agreement.

In case of a subject that can be distinguished from a Subscriber, then the above listed requirements (a) through to (d), are met by the subject; else, the subject’s designated applicant meets them. The Subscriber is required to accept the issuance terms by a Subscriber Agreement that will be executed with the GlobalSign CA for Adobe. The Subscriber Agreement incorporates by reference this CPS.

In general, an online enrolment process will be sufficient, only as explicitly permitted by GlobalSign.

In all other cases credentials are requested, as appropriate, in a way that the identity of the applicant can reasonably be established. This includes a manually signed copy of the Subscriber Agreement, and a copy of identity card, or physical appearance before the RA.

4.2 Digital ID Application Processing

A GlobalSign RA acts upon a digital ID application to validate an applicant’s identity. Subsequently, an RA either approves or rejects a digital ID application. Such approval or rejection does not necessarily have to be justified to the applicant or any other party.

The RA acts upon a digital ID application to validate an applicant’s identity as foreseen in a documented procedure.

Pursuant to a digital ID application the RA either approves or rejects a digital ID application. If the application is approved the RA transmits the registration data to GlobalSign.

For rejected applications of digital ID requests, the RA notes the reason for rejecting the application.

4.3 Digital ID Issuance

The GlobalSign RA subsequently sends a digital ID issuance request to the GlobalSign CA for Adobe.

Requests from the RA are granted approval provided that they are validly made and they contain valid Subscriber data, formatted according the GlobalSign CA for Adobe specifications.

The GlobalSign CA for Adobe verifies the identity of the GlobalSign RA on the basis of credentials presented (a special RA administrator digital ID). The GlobalSign CA for Adobe retains its right to reject the application, or any applicant for RA digital IDs.

Following issuance of the digital ID, the GlobalSign CA for Adobe delivers the issued digital ID to the Subscriber directly or through an agent.

4.4 Digital ID generation

With reference to the issuance and renewal of digital IDs GlobalSign represents towards all parties that digital IDs are issued according to the conditions set below:
The procedure to issue a digital ID is securely linked to the associated registration, including the provision of any Subscriber generated Public Key. GlobalSign shall maintain registration records associated with issued digital IDs.

- The confidentiality and integrity of registration data is ensured at all times through appropriate SSL (Secure Socket Layer) links, especially when the applicant carries out CA/RA communications.
- The authentication of Registration Authorities is ensured through appropriate credentials issued to them.
- Digital ID requests and generation are also supported by robust and tested procedures that have been scrutinized for compliance with the prevailing standards.
- GlobalSign verifies that registration data is exchanged with recognized registration service providers, whose identity is authenticated, in the event that external registration service providers are ever used.
- GlobalSign accepts independent audits of its services and practices.

4.5 Digital ID Acceptance

An issued GlobalSign CA for Adobe digital ID is deemed accepted by the Subscriber when it has been downloaded from the service it was issued from.

Any objection to accepting an issued digital ID must explicitly be notified to the GlobalSign CA for Adobe. The reasoning for rejection, including any fields in the digital ID that contain erroneous information, must also be submitted.

The GlobalSign CA for Adobe might post the issued digital ID on a repository (X.500 or LDAP). The GlobalSign CA for Adobe also reserves its right to notify the digital ID issuance by the GlobalSign CA for Adobe to other entities.

4.6 Key Pair and Digital ID Usage

The responsibilities relating to the use of keys and digital IDs include the ones addressed below:

4.6.1 Subscriber

The obligations of the Subscriber include the following ones:

4.6.1.1 Subscriber duties

Unless otherwise stated in this CPS, the duties of Subscribers include the following:

1. Accepting all applicable terms and conditions in the GlobalSign CA for Adobe CPS of GlobalSign published in the GlobalSign Repository.
2. Accepting all applicable terms and conditions in the end user Subscriber Agreement.
3. Notifying the GlobalSign CA for Adobe or a GlobalSign RA of any and all changes in the information submitted that might materially affect the trustworthiness of that digital ID.
4. Ceasing to use a GlobalSign digital ID when it becomes invalid.
5. When using a GlobalSign digital ID, as it may be reasonable under the circumstances.
6. Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private key.
7. Using secure devices and products that provide appropriate protection to their keys.
8. Responsibility for any acts and omissions of partners and agents subscribers use to generate, retain, escrow, or destroy any Private Keys.
9. Refraining from submitting to GlobalSign or any GlobalSign directory any material that contains statements that violate any law or the rights of any party.
10. Request the suspension or revocation of a digital ID in case of an occurrence that materially affects the integrity of a GlobalSign CA for Adobe digital ID.
11. Refraining from modifying with a digital ID.
12. Only using digital IDs for legal and authorised purposes in accordance with the CPS.
13. Refrain from using a digital ID outside possible license restrictions imposed by GlobalSign.

The Subscriber has all above stated duties towards the CA at all times. When the Subscriber applies on behalf of a different named Subject certain duties can be mitigated to the Subject, which in return shall have to inform the Subscriber of any eventualities affecting the life cycle of a digital ID. In such case of mitigation, duties 2, 3, 4, 5, 6, 8, 9 10, 11 above apply to the Subject and not to the Subscriber. In all cases subject shall be the contracting party by accepting the terms of the GlobalSign CA for Adobe CPS, Adobe CDS CP, and any other applicable terms via a Subscriber Agreement.

4.6.1.1.1 Digital ID Life-Cycle Operational Requirements

Subscribers are hereby notified of their continuous duty to inform directly a GlobalSign RA of any and all changes in the information featured in a digital ID during the validity period of such digital ID or of any other fact that materially affects the validity of a digital ID. This duty can be exercised either directly by the Subscriber or through an agent.

GlobalSign issues, revokes or suspends digital IDs only at the request of the RA following a successful application of a digital ID applicant.

4.6.1.2 Subscriber Duty Towards Relying Parties

Without limiting other Subscriber obligations stated elsewhere in this CP, Subscribers have a duty to refrain from any misrepresentations they make in digital IDs to third parties that reasonably rely on the representations contained therein.

4.6.1.3 Reliance at Own Risk

It is the sole responsibility of the parties accessing information featured in the GlobalSign CA for Adobe repositories and web site to assess and rely on information featured therein. Parties acknowledge that they have received adequate information to decide whether to rely upon any information provided in a digital ID. The GlobalSign CA for Adobe takes steps necessary to update its records and directories concerning the status of the digital IDs. Failure to comply with the conditions of usage of the GlobalSign CA for Adobe Repositories and web site may result in terminating the relationship between the GlobalSign CA for Adobe and the party.

4.6.2 Relying party

The duties of a Relying Party are as follows:

4.6.2.1 Relying party duties

A party relying on a GlobalSign digital ID will:

- Acknowledge notice of the GlobalSign CA for Adobe and associated conditions for relying parties.
- Validate a GlobalSign digital ID by using digital ID status information (e.g. a CRL or OCSP) published by GlobalSign, in accordance with the digital ID path validation procedure and validate at least those digital ID attributes that materially affect the Relying Party's own signature policy if available.
- Trust a GlobalSign CA for Adobe digital ID only if all information featured on such a digital ID can be verified via such a validation procedure as being correct and up to date.
- Rely on a GlobalSign digital ID, only as it may be reasonable under the circumstances.
- Trust a digital ID only if it has not been suspended or revoked.
- Validate at least those digital ID attributes that materially affect the Relying Party's own signature policy or practices.

4.6.2.2 GlobalSign CA for Adobe Repository and Web site Conditions

Parties, including Subscribers and Relying Parties, accessing the GlobalSign CA for Adobe Repository and web site agree with the provisions of this CPS and any other conditions of use that the GlobalSign CA for Adobe may make available. Parties demonstrate acceptance of the conditions of usage of the CPS by submitting a query with regard to the status of a digital ID or by anyway using or relying upon any such information or services provided including:

- Obtaining information as a result of the search for a digital ID.
- Verifying the status of digital signatures created with a Private Key corresponding to a Public Key included in a digital ID.
- Obtaining information published on the GlobalSign CA for Adobe web site.

4.7 Digital ID Renewal

Subscribers may request the renewal of GlobalSign digital IDs. To request the renewal of a GlobalSign digital ID, a Subscriber lodges an online request.

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 GlobalSign's web site.

4.8 Digital ID Revocation

GlobalSign shall use reasonable efforts to publish clear guidelines for revoking digital IDs, and maintain a 24/7 ability to accept and respond to revocation requests.

The identification of the Subscriber who applies for a revocation of a digital ID is carried out according to an internal documented procedure. This procedure is subject to auditing by authorised parties in compliance with the requirements set by accreditation schemes.

Subject to prior agreement with GlobalSign, any GlobalSign RA may carry out the identification and authentication of holders seeking to revoke a digital ID. To this effect an authenticated request is needed to initiate the procedure. The requesting party will have to be authenticated as the subscriber of that digital ID or at least as an authorised agent of the Subscriber of the digital ID.

An RA might further challenge the requesting party until its identity is sufficiently established and distinguished from others.

Revocation requests can also be placed directly to the GlobalSign CA for Adobe RA at:
GlobalSign nv/sa, Philipssite 5, 3001, Leuven, Belgium or ra@globalsign.com or to a customer appointed GlobalSign CA for Adobe RA.

Upon request from a subscriber RA or Adobe Policy Authority, the GlobalSign CA for Adobe suspends or revokes a digital ID:

- Upon receipt of a request for revocation from the Adobe Policy Authority.
- If there has been loss, theft, modification, unauthorised disclosure, or other compromise of the private key of the digital ID's subject.
- If the digital ID's subject or their appointed subscriber has breached a material obligation under this CPS.
- If the performance of a person's obligations under this CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, another person's information is materially threatened or compromised.
- If there has been a modification of the information contained in the digital ID of the digital ID's subject.
- For testing purposes.

The GlobalSign RA requests the revocation of a digital ID promptly upon verifying the identity of the requesting party. Verification of the identity can be done through information elements featured in the identification data that the Subscriber has submitted to the GlobalSign RA. Upon request by a GlobalSign RA, the GlobalSign CA for Adobe takes prompt action to revoke the digital ID.

The GlobalSign CA for Adobe does not currently support suspension.

4.8.1 Term and Termination of Revocation

The GlobalSign CA for Adobe publishes notices of revoked digital IDs in the GlobalSign CA for Adobe repository. The GlobalSign CA for Adobe may publish its revoked digital IDs in its CRL and additionally, by any other means as it sees fit.

4.9 Digital ID Status Services

The GlobalSign CA for Adobe makes available digital ID status checking services including CRLs, , and appropriate Web interfaces.

CRL
A CRL lists all revoked and suspended digital IDs during the application period. CRLs for the different products are available from http://crl.globalsign.com.

A CRL is issued each 3 hours.

4.10 End of Subscription

Subscriber subscription ends when a digital ID is revoked, expired or the service is terminated.

4.11 Digital IDs Problem Reporting and Response Capability

In addition to digital ID revocation, GlobalSign provides Subscribers, Relying Parties, Application Software Vendors, and other third parties with clear instructions for reporting complaints or suspected Private Key compromise, digital ID misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to digital IDs. GlobalSign shall use reasonable efforts to provide a 24x7 capability to accept and acknowledge and respond to such reports.

5.0 Management, Operational, And Physical Controls

This section describes non-technical security controls used by GlobalSign CA for Adobe to perform the functions of key generation, subject authentication, digital ID issuance, digital ID revocation, audit, and archival.

5.1 Physical Security Controls

The GlobalSign CA for Adobe implements physical controls on its owned, leased or rented premises.

The GlobalSign CA for Adobe infrastructure is logically separated from any other digital ID management infrastructure, used for other purposes.

The GlobalSign CA for Adobe secure premises is located in an area appropriate for high-security operations.

Physical access is restricted by implementing dual access mechanisms to control access from one area of the facility to another or access into high-security zones. All CA operations takes place in a secure computer room physically monitored and supported by security alarms and requiring movement from zone to zone to be accomplished using a token and access control lists. Next to this, dual control is implemented to access the cryptographic module and computer systems.

The GlobalSign CA for Adobe implements prevention and protection as well as measures against fire exposures.

Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.

The GlobalSign CA for Adobe implements a partial off-site backup.

The sites of the GlobalSign CA for Adobe host the infrastructure to provide the GlobalSign CA for Adobe services. The GlobalSign CA for Adobe sites implement proper security controls, including access control, intrusion detection and monitoring. Access to the sites is limited to authorized personnel listed on an access list, which is subject to audit.

5.2 Procedural Controls

The GlobalSign CA for Adobe follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of the electronic signature-related technologies.

The GlobalSign CA for Adobe obtains a signed statement from each member of the staff on not having conflicting interests, maintaining confidentiality and protecting personal data.

All members of the staff operating the key management operations administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a Trusted Position.

The GlobalSign CA for Adobe conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to make a reasonable attempt to determine their trustworthiness and competence.

Where dual control is required at least two trusted members of the GlobalSign CA for Adobe staff need to bring their respective and split knowledge in order to be able to proceed with an ongoing operation.

The GlobalSign CA for Adobe ensures that all actions with respect to the GlobalSign CA for Adobe can be attributed to the system and the person of the CA that has performed the action.

The GlobalSign CA for Adobe implements dual control for critical CA functions.

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience, Clearances

The GlobalSign CA for Adobe performs checks to establish the background, qualifications, and experience needed to perform within the competence context of the specific job. Such background checks are specifically directed towards:

- Search of criminal record
- Check of professional references
- Confirmation of previous employment
- Confirmation of the most relevant educational degree obtained
- Misrepresentations by the candidate
- Any other as it might be deemed necessary.

5.3.2 Background Checks and Clearance Procedures

The GlobalSign CA for Adobe makes the relevant checks to prospective employees by means of status reports issued by a competent authority, third-party statements or self-declarations.

5.3.3 Training Requirements and Procedures

The GlobalSign CA for Adobe provides training for their personnel to carry out CA and RA functions.

5.3.4 Retraining Period and Retraining Procedures

Periodic training updates might also be performed to establish continuity and updates in the knowledge of the personnel and procedures.

5.3.5 Job Rotation

Not applicable.

5.3.6 Sanctions against Personnel

GlobalSign CA for Adobe sanctions personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems for the purpose of imposing accountability on a participant's personnel, as it might be appropriate under the circumstances.

5.3.7 Controls of independent contractors

Independent contractors and their personnel are subject to the same privacy protection and confidentiality conditions as GlobalSign CA for Adobe personnel.

5.3.8 Documentation for initial training and retraining

The GlobalSign CA for Adobe, and RAs make available documentation to personnel, during initial training, retraining, or otherwise.

5.4 Audit Logging Procedures

Audit logging procedures include event logging and audit systems, implemented for the purpose of maintaining a secure environment.

GlobalSign CA for Adobe implements the following controls:

GlobalSign CA for Adobe audit records events in an automatic method that include but are not limited to

- Issuance of a digital ID
- Revocation of a digital ID
- Suspension of a digital ID
- Publishing of a CRL

Audit trail records contain:

- The identification of the operation
- The data and time of the operation
- The identification of the digital ID, involved in the operation
- The identification of the person that performed the operation
- A reference to the request of the operation.

Documents that are required for audits include:

- Infrastructure plans and descriptions
- Physical site plans and descriptions
- Configuration of hardware and software
- Personnel access lists.

GlobalSign CA for Adobe ensures that designated personnel reviews log files at regular intervals and detects and reports anomalous events.

Log files and audit trails are automatically archived for inspection by the authorized personnel of GlobalSign CA for Adobe, the RA and designated auditors. The log files are properly protected by an access control mechanism. Log files and audit trails are backed up and are available to independent auditors upon request.

Auditing events are not given log notice: audits on the log files are separately recorded in an access log book.

5.5 Records Archival

GlobalSign CA for Adobe keeps archives in a retrievable format.

GlobalSign CA for Adobe ensures the integrity of the physical storage media and implements proper copying mechanisms to prevent data loss.

Archives are accessible to authorized personnel of GlobalSign CA for Adobe and the RA as appropriate.

The GlobalSign CA for Adobe keeps internal records of the following items:

- All digital IDs for a period of a minimum of 3 year after the expiration of the digital ID.
- Audit trails on the issuance of digital IDs for a period of a minimum of 3 year after issuance of a digital ID.
- Audit trail of the revocation of a digital ID for a period of a minimum of 3 year following the revocation of a digital ID.
- CRLs for a minimum of 1 year after expiration or revocation of a digital ID.

- Supporting documentation used for vetting purposes prior to the issuance of digital ID will be held for a period of 2 years after expiration of a digital ID. Support documents may be electronically stored.

GlobalSign maintains records for a period of up to 7 years for the following products including Certified Transcript Service (CTS) option:

- PersonalSign Digital ID for Adobe
- PersonalSign Pro Digital ID for Adobe
- DepartmentSign Digital ID for Adobe

5.5.1 Types of records

GlobalSign CA for Adobe retains in a trustworthy manner records of GlobalSign CA for Adobe digital IDs, audit data, digital ID application information, log files and documentation supporting digital ID applications.

5.5.2 Retention period

GlobalSign CA for Adobe retains in a trustworthy manner records of digital IDs for at least 7 years.

5.5.3 Protection of archive

Conditions for the protection of archives include:

- Only the records administrator (member of staff assigned with the records retention duty) may view the archive.
- Protection against modification of archive, such as storing the data on a write once medium.
- Protection against deletion of archive.
- Protection against deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to fresh media.

5.5.4 Archive Collection

The GlobalSign CA for Adobe archive collection system is internal.

5.5.5 Procedures to obtain and verify archive information

To obtain and verify archive information GlobalSign CA for Adobe maintains records under clear hierarchical control.

The GlobalSign CA for Adobe retains records in electronic or in paper-based format. The GlobalSign CA for Adobe may require RAs, Subscribers, or their agents to submit documents appropriately in support of this requirement.

Filing terms begin on the date of expiration or revocation. Such records may be retained in electronic or in paper-based format or any other format that the GlobalSign CA for Adobe may see fit.

The GlobalSign CA for Adobe may revise record retention terms as it might be required in order to comply with accreditation schemes including WebTrust Program for CAs.

5.6 Compromise and Disaster Recovery

In a separate internal document, the GlobalSign CA for Adobe documents applicable incident, compromise reporting and handling procedures. The GlobalSign CA for Adobe documents the recovery procedures used if computing resources, software, and/or data are corrupted or suspected of being corrupted.

The GlobalSign CA for Adobe establishes the necessary measures to ensure full recovery of the service, in an appropriate time frame depending on the type of disruption, in case of a disaster, corrupted servers, software or data.

Before terminating its CA activities, the GlobalSign CA for Adobe will take steps to transfer to a designated third-party the following information at the GlobalSign CA for Adobe's own costs:

- All information, data, documents, repositories, archives and audit trails pertaining to the GlobalSign CA for Adobe.

CA keys and log files associated with offline management are stored on write-once media which is stored securely in a separate vault. Media during transport is encased in tamper-proof material and is always witnessed by at least two people.
If disposal is required, GlobalSign zeroizes the cryptographic devices in accordance with FIPS 140-3 standards. Electronic media and paper documents are destroyed through a secure and dedicated shredder.

Backups of the GlobalSign CA database for Adobe are made to an offsite secure location continuously.

6.0 Technical Security Controls

This section sets out the security measures taken by the GlobalSign CA for Adobe to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares).

6.1 Key Pair Generation and Installation

The GlobalSign CA for Adobe protects its Private Key(s) in accordance with this CPS. The GlobalSign CA for Adobe uses Private Keys only for signing Level 2 CAs, CRLs, end entity CDS digital IDs, time-stamping and OCSP responses in accordance with the intended use of each of these keys.

The GlobalSign CA for Adobe will refrain from using its Private Keys used within the GlobalSign CA for Adobe in any way outside the scope of GlobalSign CA for Adobe.

6.1.1 GlobalSign CA for Adobe Private Key Generation Process

The GlobalSign CA for Adobe uses a trustworthy process for the generation of its subordinate CA Private Key according to a documented procedure. The GlobalSign CA for Adobe distributes the secret shares of its Private Key(s).

6.1.1.1 GlobalSign CA for Adobe Private Key Usage

The Private Keys of the GlobalSign CA for Adobe are used to sign GlobalSign CA for Adobe issued CDS digital IDs, Level 2 CAs, GlobalSign CA for Adobe certification revocation lists, time-stamping and OCSP responses. Other usages are prohibited.

6.1.1.2 GlobalSign CA for Adobe Private Key Type

For the CA key it uses, the GlobalSign CA for Adobe makes use of the RSA algorithm with a key length of 2048 bits and a validity period of at least 11 years.

6.1.2 GlobalSign CA for Adobe Key Generation

The GlobalSign CA for Adobe securely generates and protects its own Private Keys, using a Trustworthy System, and takes necessary precautions to prevent the compromise or unauthorised usage of them. The GlobalSign CA for Adobe implements and documents key generation procedures, in line with this CPS.

The GlobalSign key generation is carried out using an algorithm recognized as being fit for the purposes of digital IDs. GlobalSign uses RSA SHA-1.

The selected key length and algorithm for CA signing key is recognized as being fit for the purposes of digital IDs as issued by the CA.

6.2 Key Pair re-generation and re-installation

The GlobalSign CA for Adobe decommissions and destroys keys and media used in the past as well as the active tamper-resistant devices and all backup or escrowed copies of its private keys.

6.2.1 GlobalSign CA for Adobe Key Generation Devices

The generation of the Private Keys of the GlobalSign CA for Adobe occurs within a secure FIPS 140-1 Level 3 cryptographic device.

6.2.1.1 GlobalSign CA for Adobe Key Generation Controls

The generation of the Private Key of the GlobalSign CA for Adobe requires the control of more than one appropriately authorised member of staff serving in trustworthy positions. This action entails dual control.

6.2.2 GlobalSign CA for Adobe Private Key Storage

The GlobalSign CA for Adobe uses a secure FIPS 140-1 level 2 cryptographic device to store its Private Keys meeting the appropriate requirements of ISO.

When outside the signature-creation device the GlobalSign Private Key for a digital ID is encrypted at all times.

6.2.2.1 GlobalSign CA for Adobe Key Storage Controls

The storage of the Private Key of the GlobalSign CA for Adobe requires multiple controls by appropriately authorised members of staff serving in trustworthy positions. This action entails dual control.

6.2.2.2 GlobalSign CA for Adobe Key Back Up

The GlobalSign CA for Adobe’s Private Keys are backed up, stored and recovered by multiple and appropriately authorised members of staff serving in trustworthy positions. This action entails dual control.

6.2.2.3 Secret Sharing

The GlobalSign CA for Adobe secret shares use multiple authorised holders, to safeguard and improve the trustworthiness of Private Keys and provide for key recovery. The GlobalSign CA for Adobe stores its own Private Keys in several tamper-resistant devices. This action entails dual control.

6.2.2.4 Acceptance of Secret Shares

A secret shareholder receives the secret share within a physical medium, such as a GlobalSign CA for Adobe Approved Hardware Device.

6.2.3 GlobalSign CA for Adobe Public Key Distribution

GlobalSign will make public certificate of GlobalSign for Adobe Subordinate CA available on our support pages.

6.2.4 GlobalSign CA for Adobe Private Key Destruction

GlobalSign CA for Adobe Private Keys are destroyed by at least two trusted operatives present at the end of their lifetime in order to guarantee that they cannot ever be retrieved and used again.

Key destruction process is documented and associated records are archived.

6.3 Private Key Protection and Cryptographic Module Engineering Controls

The GlobalSign CA for Adobe uses appropriate FIPS 140-1 Level 3 cryptographic devices to perform CA key management tasks. Those cryptographic devices are known as Hardware Security Modules (HSMs).

Such devices meet formal requirements, which guarantee, amongst other things, that device tampering is immediately detected; and Private Keys cannot leave devices unencrypted

Hardware and software mechanisms that protect CA Private Keys are documented. The document demonstrates that CA key protection mechanisms are of at least equivalent strength to the CA keys they are protecting.

GlobalSign CA for Adobe custodians are assigned with the task to activate and deactivate the Private Key. The key is then active for a defined time period.

The GlobalSign CA for Adobe Private Keys can be destroyed at the end of their lifetimes.

6.4 Other Aspects of Key Pair Management

The GlobalSign CA for Adobe archives its own Public Keys. The GlobalSign CA for Adobe issues Subscriber digital IDs with usage periods as indicated on such digital IDs.

6.4.1 Computing resources, software, and/or data are corrupted

The GlobalSign CA for Adobe establishes the necessary measures to ensure full recovery of the service in case of a disaster, corrupted servers, software or data.

If resources or services are not retained under the control of the GlobalSign CA for Adobe, the CA ensures that any agreement with the resource owner or services provider is compliant with the requirements for disaster recovery.

6.4.2 CA public key revocation

If a GlobalSign CA for Adobe Public Key is revoked the GlobalSign CA for Adobe will immediately:

- Notify all CAs with which it is cross-certified.
- Notify Adobe Policy Authority

6.4.3 CA private key is compromised

If the Private Key of the GlobalSign CA for Adobe is compromised, the corresponding digital ID will immediately be revoked. Additional measures will be taken including the revocation of all subscriber's digital IDs.

6.5 Activation Data

The GlobalSign CA for Adobe securely stores and archives activation data associated with its own Private Key and operations.

6.6 Computer Security Controls

The GlobalSign CA for Adobe implements computer security controls.

6.7 Life Cycle Security Controls

The GlobalSign CA for Adobe performs periodic development controls and security management controls.

6.8 Network Security Controls

The GlobalSign CA for Adobe maintains a high-level network of systems security including firewalls. Network intrusions are detected. In specific:

- The GlobalSign CA for Adobe encrypts connections to the RA, using dedicated administrative digital IDs.
- The GlobalSign CA for Adobe website provides digital ID based SSL connections and anti-virus protection.
- The GlobalSign CA for Adobe network is protected by a managed firewall and intrusion detection system.
- Accessing GlobalSign CA for Adobe databases from outside the CAs network is prohibited.
- Internet sessions for request and delivery of information are encrypted.

6.9 Time-stamping

All digital signatures created by CDS Subscriber digital IDs will include a trusted time stamp issued from an RFC 3161 compliant Time Stamp Authority (TSA) server. The TSA certificate chains up to the Subordinate CA which issued the Subscriber digital ID used to apply the digital signature.

7.0 Digital ID and CRL Profiles

This section specifies the digital ID format, CRL and OCSP formats.

7.1 Digital ID Profile

Minimum CDS Certificate Profile

X.509 v3 Certificate Attributes/ Extensions	Critical / Non Critical	Value / Notes
Attributes		
Version		v3
SerialNumber		integer; unique to each certificate issued in the GlobalSign CA for Adobe PKI domain
Signature		sha-1 w/ RSAEncryption – {1.2.840.113549.1.1.5}
Issuer		cn=GlobalSign CA for Adobe, o=GlobalSign, c=UK
Validity		• Minimum = 1 day • Maximum = 10 years
Subject		Based application information
SubjectPublicKeyInfo		• rsaEncryption – {1.2.840.113549.1.1.1} RSA public key is 2048 bit public key
Extensions		
AuthorityKeyIdentifier	Non-critical	contains a 20 byte SHA-1 hash of the SUB-Root CA public key
KeyUsage	Critical	Minimum Key Usages • Digital Signature • Non-Repudiation
SubjectKeyIdentifier	Non-critical	contains a 20 byte SHA-1 hash of the subjectPublicKey in this certificate
CertificatePolicies	Critical	1.2.840.113583.1.2.1 Notice Text=This certificate has been issued in accordance with the GlobalSign CDS CPS located at http://www.globalsign.net/repository/
ExtendedKeyUsage	Non-critical	1.2.840.113583.1.1.5
CRLDistributionPoints	Non-critical	http://crl.globalsign.net/globalsigncaadobe.crl

Minimum Test CDS Certificate Profile

X.509 v3 Certificate Attributes/ Extensions	Critical / Non Critical	Value / Notes
Attributes		
Version		v3
SerialNumber		integer; unique to each certificate issued in the GlobalSign CA for Adobe PKI domain
Signature		sha-1 w/ RSAEncryption – {1.2.840.113549.1.1.5}
Issuer		cn=GlobalSign CA for Adobe, o=GlobalSign , c=UK
Validity		• Minimum = 1 day • Maximum = 90 days
Subject		Based application information
SubjectPublicKeyInfo		• rsaEncryption – {1.2.840.113549.1.1.1} RSA public key is 2048 bit public key
Extensions		
AuthorityKeyIdentifier	Non-critical	contains a 20 byte SHA-1 hash of the SUB-Root CA public key
KeyUsage	Critical	Minimum Key Usages • Digital Signature • Non-Repudiation
SubjectKeyIdentifier	Non-critical	contains a 20 byte SHA-1 hash of the subjectPublicKey in this certificate
CertificatePolicies	Critical	1.2.840.113583.1.2.2 Notice Text=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://crl.globalsign.net/globalsigncaadobe.crl

7.2 CRL Profile

GlobalSign issued CRLs conform to all RFC 2459 standards and recommendations.

7.3 OCSP Profile

If a CDS digital ID contains an OCSP extension, then certain Adobe products may make an OCSP request using OID 1.2.840.113583.1.1.9.2 that resides in the CDS Certificate.
The definitive OCSP response message includes the following:

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

The address of the OCSP responder is URI = http://adobe-ocsp.globalsign.com/responder. The Certificate used to sign the OCSP response is issued by the GlobalSign CA for Adobe. The OCSP Certificate DN is: cn=GlobalSign Adobe OCSP Responder
c=UK
o=GlobalSign

When the CA returns an error message in response to a certificate status request, the error message is not digitally signed.

8.0 Compliance Audit And Other Assessment

The GlobalSign CA for Adobe accepts under condition of the Web Trust audit the auditing of practices and procedures it does not publicly disclose. The GlobalSign CA for Adobe gives further consideration and evaluates the results of such audits before possibly implementing them.

Following its own approval with regard to the scope and content the GlobalSign CA for Adobe accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CPS and accreditation schemes it publicly claims compliance with.

8.1 Compliance Audit And Other Assessment

GlobalSign has successfully been audited and currently meets the requirements of the accreditation scheme known as WebTrust for CAs. GlobalSign seeks to maintain its accreditation.

GlobalSign shall also seek accreditation by Qualified Auditors and seek to maintain its accreditation under the WebTrust for CAs scheme on a recurrent basis. Licensed to perform WebTrust for CA audits, Qualified Auditors must be AICPA members and have proficiency in examining PKI technology and related information security tools and techniques.

Information on GlobalSign’s conformance with the requirements of any other accreditation scheme can be sought by the organization of such accreditation scheme directly.
GlobalSign accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CPS. GlobalSign accepts this auditing of its own practices and procedures that it does not publicly disclose under certain conditions such as confidentiality, trade secrets etc. Such audits may be carried out directly or through an agent by a party to which GlobalSign owes duty. The CA evaluates the results of such audits before further implementing them and makes them publicly available.

8.1.1 Audit process conditions

To carry out the audits there will be an independent auditor appointed who will not be affiliated directly or indirectly in any way with GlobalSign nor having any conflicting interests thereof.

An audit is carried out in areas that include but are not limited to the following:

- Compliance of GlobalSign operating procedures and principles with the procedures and service levels defined in the CPS.
- Management of the infrastructure that implements CA services.
- Management of the physical site infrastructure.
- Adherence to the CPS.
- Adherence to relevant laws.
- Asserting agreed service levels.
- Inspection of audit trails, logs, relevant documents etc.
- Cause of any failure to comply with the conditions above.

With regard to conformance audits, GlobalSign undertakes the responsibility of the performance of any subcontractors it uses to carry out certification operations including those described in the section below.

8.1.1.1 Business Partnerships

To better respond to the diverse certification needs of the distributed population of electronic commerce service providers and users, GlobalSign may co-operate with appropriately selected business partners to deliver certain services associated with PKI, including certification and registration. GlobalSign may outsource in part or whole certain aspects of the delivery of its services. Regardless of the partner or agent selected to manage certain parts of the digital ID life cycle or operations, GlobalSign remains ultimately in charge of the whole process. GlobalSign will ensure that compliance audits are also applied to such outsourced services. GlobalSign limits its responsibility thereof according to the conditions in this CPS and the GlobalSign CP. All business partners that are involved in reseller or OEMing CDS certificates shall enter into agreements with GlobalSign that flow Adobe CDS CPS and CP and if applicable RA obligations down.

8.1.1.2 Secure Devices and Private Key Protection

GlobalSign supports the use of secure devices and tamperproof equipment to securely issue, manage and store digital IDs. GlobalSign uses accredited trustworthy hardware to prevent compromise of its Private Key.

9.0 Other Business and Legal Matters

Certain Legal conditions apply to the issuance of the GlobalSign CA for Adobe digital IDs under this CPS as described in this section.

9.1 Fees

The issuance and management of GlobalSign CA for Adobe digital IDs is subject to fees announced on the GlobalSign web site www.globalsign.com or through requested quotes.

9.1.1 Refund policy

GlobalSign accepts requests for refund in writing. Refund requests must be duly justified and addressed to the Legal Services of GlobalSign. GlobalSign reserves its right to endorse or grant and refunds unless they are requested in the framework of a warranty offered by GlobalSign.

9.2 Financial Responsibility

GlobalSign maintains sufficient resources to meet its perceived obligations under this CPS. Other than the warranties provided herein (including, without limitation, those in Section 9.6.5) the GlobalSign CA for Adobe makes this service available on an “as is” basis. GlobalSign may make available a limited warranty plan published on www.globalsign.com.

9.3 Confidentiality of Business Information

The GlobalSign CA for Adobe observes personal data privacy rules and confidentiality rules as described in this GlobalSign CPS. Confidential information includes:

- Any personal identifiable information on Subscribers, other than that contained in a digital ID.
- Reason for the revocation or suspension of a digital ID, other than that contained in published digital ID status information.
- Audit trails.
- Correspondence regarding CA services.
- CA Private Key(s).

The following items are not confidential information:

- Digital ID and their content.
- Status of a digital ID.

GlobalSign does not release nor is it required to release any confidential information without an authenticated and justified request specifying either:

- The party to whom the GlobalSign CA for Adobe owes a duty to keep information confidential is the party requesting such information.
- A court order.

GlobalSign may charge an administrative fee to process such disclosures.

Parties requesting and receiving confidential information are granted permission on the assumption that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third parties.

9.3.1 Disclosure Conditions

Non-confidential information can be disclosed to any Subscriber and Relying Party under the conditions below:

- Only a single digital ID is delivered per inquiry by Subscriber or Relying Party.
- The status of a single digital ID is provided per inquiry by a Subscriber or Relying Party.
- Subscribers can consult the information the CA holds about them.

Confidential information may not be disclosed to Subscribers nor Relying Parties. The GlobalSign CA for Adobe properly manages the disclosure of information to the CA personnel.

The GlobalSign CA for Adobe authenticates itself to any party requesting the disclosure of information by:

- Presenting an authentication digital ID at the request of the Subscriber or Relying Party
- Signing responses to OCSP requests and CRLs.

The GlobalSign CA for Adobe encrypts all communications of confidential information including:

- The communications link between the CA and the RAs.
- Sessions to deliver digital IDs and digital ID status information.

To incorporate information by reference the GlobalSign CA for Adobe uses computer-based and text-based pointers that include URLs, etc.

9.4 Privacy of Personal Information

The GlobalSign CA for Adobe makes available a specific Privacy Policy for the protection of personal data of the applicant applying for a GlobalSign CA for Adobe digital ID that they make available through their web site. The GlobalSign CA for Adobe adheres to the documented Privacy Policy of GlobalSign NV available from www.globalsign.com/repository.

9.5 Intellectual Property Rights

The GlobalSign CA for Adobe owns and reserves all intellectual property rights associated with its databases, web sites, GlobalSign CA for Adobe digital IDs and any other publication whatsoever originating from GlobalSign CA for Adobe including this CPS.

The Distinguished Names of all CAs of the GlobalSign CA for Adobe, remain the sole property of GlobalSign, which enforces these rights.

Digital IDs are and remain property of the GlobalSign CA for Adobe. The GlobalSign CA for Adobe permits the reproduction and distribution of digital IDs on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full, except that digital IDs are not published in any publicly accessible repository or directory without the express written permission of the GlobalSign CA for Adobe. The scope of this restriction is also intended to protect Subscribers against the unauthorised re-publication of their personal data featured on a digital ID.

The GlobalSign CA for Adobe owns and reserves all intellectual property rights associated with its own products and services that it has not explicitly transferred or released to another party.

9.6 Representations and Warranties

Unless otherwise provided in this CPS, the following rules apply as to Representations and Warranties.

The GlobalSign CA for Adobe uses this CPS, associated CPs and a Subscriber Agreement to convey legal conditions of usage of GlobalSign CA for Adobe digital IDs to Subscribers and Relying Parties.

Participants that may make representations and warranties include GlobalSign CA for Adobe, RAs, Subscribers, Relying Parties, and any other participants as it might become necessary.

All parties of the GlobalSign domain, including the GlobalSign CA for Adobe, RAs and Subscribers warrant the integrity of their respective Private Key(s). If any such party suspects that a Private Key has been compromised they will immediately notify the appropriate RA.

9.6.1 Subscriber Obligations

Unless otherwise stated in this CPS, subscribers are responsible for:

- Having knowledge and, if necessary, seeking training on using digital IDs.
- Generating securely their Private-Public Key Pair, using a Trustworthy System.
- Providing correct and accurate information in their communications with the GlobalSign CA for Adobe.
- Ensuring that the Public Key submitted to the GlobalSign CA for Adobe correctly corresponds to the Private Key used.
- Accepting all terms and conditions in the GlobalSign CA for Adobe CPS and associated policies published in the GlobalSign CA for Adobe Repository.
- Refraining from tampering with a GlobalSign CA for Adobe digital ID.
- Using GlobalSign CA for Adobe digital IDs for legal and authorised purposes in accordance with this CPS.
- Notifying GlobalSign CA for Adobe or a GlobalSign RA of any changes in the information submitted.
- Ceasing to use a GlobalSign CA for Adobe digital ID if any featured information becomes invalid.
- Ceasing to use a GlobalSign CA for Adobe digital ID when it becomes invalid.
- Removing a GlobalSign CA for Adobe digital ID when invalid from any applications and/or devices they have been installed on.
- Using a GlobalSign CA for Adobe digital ID, as it may be reasonable under the circumstances.
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their Private Key.
- For any acts and omissions of partners and agents Subscribers use to generate, retain, escrow, or destroy any Private Keys.
- Refraining from submitting to GlobalSign CA for Adobe or any GlobalSign CA for Adobe directory any material that contains statements that violate any law or the rights of any party.
- Requesting the suspension or revocation of a digital ID in case of an occurrence that materially affects the integrity of a GlobalSign CA for Adobe digital ID.
- Notifying the appropriate RA immediately, if a Subscriber becomes aware of or suspects the compromise of a Private Key.

When the applicant is an organization acquiring and managing a digital ID on behalf of an individual Subscriber (in the name of that individual or in the name of the role of that individual within the organization), organization is required to:

(a) maintain processes that assure that the private key can be used only with the knowledge and explicit action of the Subscriber;

(b) maintain information that permits a determination of who signed a particular document;

(c) assure that the digital ID subject has received security training appropriate for the purposes for which the digital ID is issued;

(d) notify the GlobalSign immediately upon any actual or suspected loss, disclosure, or other compromise of the Subscriber's private key;

(e) ensure that the Subscriber named in the digital ID or responsible for the use of the private key corresponding to the public key in the digital ID enters into a binding Subscriber Agreement which obligates the Subscriber to:

- generate a public/private key pair using an Approved Hardware Device, and take all reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key;
- acknowledge that the information identifying the Subscriber in the digital ID is true and accurate, or notify GlobalSign immediately upon any inaccuracies in that information;
- use the digital ID exclusively for CDS purposes
- request digital ID revocation immediately upon any actual or suspected loss, disclosure, or other compromise of the Subscriber's private key.

GlobalSign makes available a Subscriber Agreement in order to ensure that the Subscriber is bound under the following terms:

a) Submit accurate and complete information to GlobalSign in accordance with the requirements of this CPS particularly with regards to registration.
b) Only use the Key Pair for electronic signatures and in accordance with any other limitations notified to the Subscriber according to this CPS.
c) Exercise reasonable care to avoid unauthorized use of its Private Key.
d) Under the GlobalSign model the Subscriber typically generates its own keys, in which case the following terms also apply:
    - Generate Subscriber keys using an algorithm recognized as being fit for the purposes of electronic signatures;
    - Use a minimum 2048 key length and algorithm, which is recognized as being fit for the purposes of electronic signatures.
    - Generate and store Private Key on an Approved Hardware Device.
e) Notify GlobalSign without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the digital ID:
    - The Subscriber's Private Key has been lost, stolen, potentially compromised; or
    - Control over the Subscriber's Private Key has been lost due compromise of activation data (e.g. PIN code).
    - Inaccuracy or changes to the digital ID content, as notified to the Subscriber.

9.6.2 Relying Party Obligations

A party relying on a GlobalSign CA for Adobe digital ID promises to:

- Have the technical capability to use digital IDs.
- Receive notice of the GlobalSign CA for Adobe and associated conditions for Relying Parties.
- Validate a GlobalSign CA for Adobe digital ID by using digital ID status information (e.g. a CRL) published by the GlobalSign CA for Adobe in accordance with the proper digital ID (digital ID) path validation procedure.
- Trust a GlobalSign CA for Adobe digital ID only if all information featured on such digital ID can be verified via such a validation procedure as being correct and up to date.
- Rely on a GlobalSign CA for Adobe digital ID, only as it may be reasonable under the circumstances.
- Notify the appropriate RA immediately, if the Relying Party becomes aware of or suspects that a Private Key has been compromised.

The obligations of the Relying Party, if it is to reasonably rely on a digital ID, are to:

- Verify the validity, suspension or revocation of the digital ID using current revocation status information as indicated to the Relying Party.
- Take account of any limitations on the usage of the digital ID indicated to the Relying Party either in the digital ID or this CPS.
- Take any other precautions prescribed in the Subscriber Agreement, GlobalSign digital ID as well as any other policies or terms and conditions made available in the application context a digital ID might be used.

Relying Parties must at all times establish that it is reasonable to rely on a digital ID under the circumstances taking into account circumstances such as the specific application context a digital ID is used in.

9.6.2.1 Conveying Relying party obligations

In order to give uninhibited access to revocation information and subsequently invoke trust in its own services, GlobalSign refrains from implementing an agreement with the Relying Party instead using this GlobalSign CA for Adobe CPS and the user notification provided in Adobe supported products for the purpose of binding Relying Parties to their obligations.

Much like it applies to any other participant of GlobalSign public services, however, the use of GlobalSign resources that relying parties make is implied to be governed by the conditions set out in GlobalSign policy framework instigated by the Adobe CP and the GlobalSign CA for Adobe CPS.

Relying parties are hereby notified that the conditions prevailing in this CPS are binding upon them each time they consult a GlobalSign resource for the purpose of establishing trust and validating a digital ID.

9.6.3 Subscriber Liability towards Relying Parties

Without limiting other subscriber obligations stated elsewhere in this CP, Subscribers are liable for any misrepresentations they make in digital IDs to third parties that, reasonably rely on the representations contained therein.

9.6.4 GlobalSign CA for Adobe Repository and Web site Conditions

Parties (including Subscribers and Relying Parties) accessing the GlobalSign CA for Adobe Repository and web site agree with the provisions of this CPS and any other conditions of usage that GlobalSign may make available. Notice of this CPS is provided on the GlobalSign repository available on http://www.globalsign.com/repository/. The current and last version will always be available there. Parties demonstrate acceptance of the conditions of usage of the CPS by submitting a query with regard to the status of a digital ID or by anyway using or relying upon any such information or services provided. The GlobalSign CA for Adobe Repositories include or contain:

- Information provided as a result of the search for a digital ID.
- Information to verify the status of digital signatures created with a Private Key corresponding to a public key listed in a digital ID.
- Information to verify the status of a digital ID before encrypting data using the Public Key included in a digital ID.
- Information published on the GlobalSign CA for Adobe web site.
- Any other services that GlobalSign CA for Adobe might advertise or provide through its web site.
- If a repository becomes aware of or suspects the compromise of a Private Key, it will immediately notify the appropriate RA. The party that operates a Repository has exclusive responsibility of all acts or omissions associated with it.

The GlobalSign CA for Adobe maintains a digital ID Repository during the application period and for a maximum of seven years after the expiration or revocation of a digital ID. To verify its integrity the complete repository will be made available to the GlobalSign RAs for queries at any time.

Additionally, the GlobalSign CA for Adobe repository is available to Relying Parties.

9.6.4.1 Reliance at Own Risk

It is the sole responsibility of the parties accessing information featured in the GlobalSign CA for Adobe Repositories and web site to rely on information featured therein. Parties acknowledge that they have received adequate information to decide whether to rely upon any information provided in a digital ID. The GlobalSign CA for Adobe takes steps necessary to update its records and directories concerning the status of the digital IDs and issue warnings about. Failure to comply with the conditions of usage of the GlobalSign Repositories and web site may result in terminating the relationship between the GlobalSign CA for Adobe and the party.

9.6.4.2 Accuracy of Information

The GlobalSign CA for Adobe makes every effort to ensure that parties accessing its repositories receive accurate, updated and correct information. The GlobalSign CA for Adobe, however, cannot accept any liability beyond the limits set in this CPS and the GlobalSign CA for Adobe insurance policy.

9.6.5 GlobalSign CA for Adobe Obligations

To the extent specified in the relevant sections of the CP, the GlobalSign CA for Adobe promises to:

- Comply with this CPS and its amendments as published under https://www.globalsign.com/repository
- Provide infrastructure and certification services, including the establishment and operation of the GlobalSign CA for Adobe Repository and web site for the operation of public digital ID management services.
- Provide trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its own Private Key(s).
- Provide and validate application procedures for the various types of digital IDs that it makes publicly available.
- Issue digital IDs in accordance with this CPS and fulfil its obligations presented herein.
- Revoke digital IDs issued according to this CPS upon receipt of a valid and authenticated request to revoke a digital ID from an RA.
- Publish accepted digital IDs in accordance with this CPS.
- Provide support to Subscribers and Relying Parties as described in this CPS.
- Provide for the expiration and renewal of digital IDs according to this CPS.
- Publish CRLs and/or OCSP responses of all suspended and revoked digital IDs on a regular basis in accordance with this CPS.
- Provide appropriate service levels according to a service agreement.
- Notify Relying Parties of digital ID revocation by publishing CRLs on the GlobalSign CA for Adobe repository.

The liability of GlobalSign CA for Adobe under the above stated article for proven damages is limited to $5,000 for any individual digital ID, directly caused by the occurrences listed above. This limit might be reviewed by GlobalSign. GlobalSign might seek additional insurance coverage against risks emanating from the correctness of the information included in a digital ID.

To the extent permitted by law the GlobalSign CA for Adobe cannot be held liable for:

- Any use of digital IDs, other than specified in this CPS.
- Falsification of transactions.
- Improper use or configuration of equipment, not operated under the responsibility of the CA, used in a transaction involving digital IDs.
- Compromise of Private Keys associated with the digital IDs.

- Loss, exposure or misuse of PIN code(s) etc. protecting Private Keys associated with the digital IDs.
- The submission of erroneous or incomplete data from an RA, including identification data, serial numbers and Public Key values
- Erroneous or incomplete requests for operations on digital IDs by the RA.
- Acts of God.
- The use of digital IDs.
- The use of Public or Private Keys of cross-certified (non-subordinate) CA's and their Relying Parties.

The GlobalSign CA for Adobe acknowledges it has no further obligations under this CPS.

9.6.6 Registration Authority Obligations

A GlobalSign RA operating within the GlobalSign network promises to:

- Generate securely an RA administrator Key Pair, using a Trustworthy System directly or through an agent.
- Provide correct and accurate information in their communications with the GlobalSign CA for Adobe.
- Ensure that the Public Key submitted to GlobalSign CA for Adobe is the correct one (if applicable).
- Generating a new, secure Key Pair to be used in association with a digital ID that they request from GlobalSign CA for Adobe.
- Receive applications for the GlobalSign CA for Adobe digital IDs in accordance with this GlobalSign CPS.
- Carry out all verification and authenticity actions prescribed by the GlobalSign CA for Adobe procedures and this CPS.
- Submit to the GlobalSign CA for Adobe the applicant's request in a signed message (digital ID request).
- Receive, verify and relay to the GlobalSign CA for Adobe all requests for revocation of a GlobalSign CA for Adobe digital ID in accordance with the GlobalSign CA for Adobe procedures and the GlobalSign CA for Adobe CPS.
- Verify the accuracy and authenticity of the information provided by the Subscriber at the time of renewal of a digital ID according to this CPS.

9.6.7 Information incorporated by reference into a digital ID

The GlobalSign CA for Adobe incorporates by reference the following information in every digital ID it issues:

- Terms and conditions of the GlobalSign CA for Adobe CPS.
- Any other applicable digital ID policy as may be stated on an issued GlobalSign digital ID.
- The mandatory elements of the standard X.509.
- Any non-mandatory but customised elements of the standard X.509.
- Content of extensions and enhanced naming that are not fully expressed within a digital ID.
- Any other information that is indicated to be so in a field of a digital ID.

9.6.8 Pointers to incorporate by reference

To incorporate information by reference GlobalSign uses computer-based and text-based pointers. GlobalSign may use URLs, OIDs, etc.

9.7 Disclaimers of Warranties

This section includes disclaimers of express warranties.

9.7.1 Limitation for Other Warranties

The GlobalSign CA for Adobe does not warrant:

- The accuracy of any unverifiable piece of information contained in digital IDs except as it may be stated in the relevant product description below in this CPS and in the GlobalSign CA for Adobe warranty policy, if available.
- The accuracy, authenticity, completeness or fitness of any information contained in free, test or demo digital IDs.

9.7.2 Exclusion of Certain Elements of Damages

In no event (except for fraud or wilful misconduct) is the GlobalSign CA for Adobe liable for:

- Any loss of profits.
- Any loss of data.
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of digital IDs or digital signatures.
- Any transactions or services offered or within the framework of this CPS.
- Any other damages except for those due to reliance on the verified information in a digital ID, except for information featured on free, test or demo digital IDs.
- Any liability incurred in any case if the error in such verified information is the result of fraud or wilful misconduct of the applicant.

9.8 Limitations of Liability

The total liability of the GlobalSign is limited as per below.

Except as otherwise specified in writing between partiers. notice is hereby given that a digital ID can only be relied upon for transactions involving a monetary value equal or lower than as follows:

Maximum limits in the GlobalSign Limited Warranty Plan for Subscribers	
PersonalSign Digital ID for Adobe	5,000 USD
PersonalSign Pro Digital ID for Adobe	5,000 USD
DepartmentSign Digital ID for Adobe	5,000 USD

9.9 Indemnities

This section contains the applicable indemnities.

To the extent permitted by law the Subscriber agrees to indemnify and hold the GlobalSign CA for Adobe harmless for any and all third party liability, claims, demands (including direct, indirect, special and consequential damages), losses or damages, and all costs and expenses, including reasonable attorney's fees, caused by any breach of the Subscriber Agreement, including, without limitation, as a result of reliance on any misrepresentation of a material fact by that Subscriber including

- Failure to protect the Subscriber's Private Key,
- Use a Trustworthy System as required
- Taking precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the Subscriber's Private Key
- Attend to the integrity of the GlobalSign Root.

To the extent permitted by law the Relying Party agrees to indemnify and hold the GlobalSign CA for Adobe and Adobe harmless from any third party losses or damages caused by any breach of this CPS and requires the Relying Party to indemnify the Root CA and the CDS Subordinate CA for any third party losses or damages caused by any breach of any Relying Party Agreements, EULAs, or PKI Disclosure Statement, including, without limitation any failure to check the digital ID status prior to any reliance on a digital signature from a Subscriber.

9.10 Term and Termination

This CPS remains in force until notice of the opposite is communicated by the GlobalSign CA for Adobe on its web site or Repository.

Notified changes are appropriately marked by an indicated version. Following publications, changes become applicable 30 days thereafter.

9.11 Individual notices and communications with participants

The GlobalSign CA for Adobe accepts notices related to this CPS by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from GlobalSign CA for Adobe the sender of the notice deems its communication effective. The sender must receive such acknowledgment within twenty (20) business days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows. Individual communications made to the GlobalSign CA for Adobe must be addressed to legal@GlobalSign.com or by post to the GlobalSign in the address mentioned in the introduction of this document.

9.12 Amendments

Changes to this CPS are indicated by appropriate numbering.

9.13 Dispute Resolution Procedures

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) parties agree to notify GlobalSign of the dispute with a view to seek dispute resolution.

Upon receipt of a Dispute Notice, GlobalSign convenes a Dispute Committee that advises GlobalSign management on how to proceed with the dispute. The Dispute Committee convenes within twenty (20) business days from receipt of a Dispute Notice. The Dispute Committee is composed by a counsel, a data protection officer, a member of GlobalSign operational management and a security officer. The counsel or data protection officer chair the meeting. In its resolutions the Dispute Committee proposes a settlement to the GlobalSign executive management. The GlobalSign executive management may subsequently communicate the proposed settlement to the resting party.

9.13.1 Arbitration

If the dispute is not resolved within twenty (20) business days after initial notice pursuant to CPS, parties submit the dispute to arbitration, in accordance with art. 1676-1723 of the Belgian Judicial Code.

There will be 3 arbitrators of whom each party proposes one while both parties of the dispute choose the third arbitrator. The place of the arbitration is Leuven, Belgium and the arbitrators determine all associated costs.

For all technology related disputes and disputes related to this CPS the parties accept the arbitration authority of the Belgian branch of Stichting Geschillenoplossing Automatisering (Foundation for the Settlement of Automation Disputes) with registered offices in:
J. Scheepmansstraat 5,
3050 Oud-Heverlee, Belgium.
Tel.: +32-47-733 82 96, Fax: + 32-16-32 54 38.

9.14 Governing Law

This CPS is governed, construed and interpreted in accordance with the laws of Belgium. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of GlobalSign digital IDs or other products and services. The law of Belgium apply also to all GlobalSign commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to GlobalSign products and services where the GlobalSign acts as a provider, supplier, beneficiary receiver or otherwise.

Each party, including GlobalSign partners, subscribers and relying parties, irrevocably submit to the jurisdiction of the district courts of Leuven, Belgium.

9.15 Compliance with Applicable Law

GlobalSign CA for Adobe complies with applicable laws of Belgium. Export of certain types of software used in certain GlobalSign CA for Adobe public digital ID management products and services may require the approval of appropriate public or private authorities. Parties (including the GlobalSign CA for Adobe, subscribers and relying parties) agree to conform to all applicable export laws and regulations.

9.16 Miscellaneous Provisions

9.16.1 Survival

The obligations and restrictions contained under section “Legal Conditions” survive the termination of this CPS.

9.16.2 Severability

If any provision of this CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CPS shall be interpreted in such manner as to effect the original intention of the parties.

10.0 List of definitions

ACCEPT (A DIGITAL ID)
To approve of a digital ID by a digital ID applicant within a transactional framework.
ACCREDITATION
A formal declaration by an approving authority that a certain function/entity meets specific formal requirements
ACCREDITED EDUCATIONAL INSTITUTION
An educational institution that is accredited by the Council of Higher Education Accreditation.
ADOBE
Adobe Systems Incorporated.
ADOBE POLICY AUTHORITY
Selected members of Adobe’s management that define, review and approve polices related to the Adobe PKI.
ADOBE ROOT CA
Adobe’s root Certification Authority.
APPLICATION FOR A DIGITAL ID
A request sent by a digital ID applicant to a CA to issue a digital ID
APPLICATION SOFTWARE VENDOR
A developer of Internet browser software or other software that displays or uses digital IDs and distributes root digital IDs, such as KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.
APPROVED HARDWARE DEVICE
Hardware devices that securely generate and store either a Certification Authority's or a Subscriber's key pair and certificate chain and perform signing, encryption and/or authentication. Both hardware security modules and tokens are forms of cryptographic hardware.
In the case of end entity private key protection, approved hardware is defined as minimum FIPS-140-1 level 2 and the case of subordinate CA, approved hardware is minimum FIPS 140-1 level 3 Cryptographic hardware.
ARCHIVE
To store records for period of time for purposes such as security, backup, or audit.
AUDIT
Procedure used to validate compliance with formal criteria or controls.
AUTHENTICATION
A process used to confirm the identity of a person or to prove the integrity of specific information by placing them within the right context and verifying such relationship.
AUTHORISATION
Granting of rights.
AVAILABILITY
The rate of accessibility of information or resources.
HARDWARE MODULE
The complete system of the hardware module used to keep the digital IDs and securely generate a Key Pair.
BINDING
A statement by an RA of the relationship between a named entity and its Public Key.
CERTIFICATE REVOCATION LIST OR CRL
A list maintained by the CA of digital IDs that are revoked before their expiration time.
CERTIFICATION AUTHORITY OR CA
An entity that is trusted to associate a Public Key to the information on the Subject, contained in the digital ID. Unless explicitly specified, the CA described herein is the GlobalSign CA for Adobe.
CERTIFICATION PRACTICE STATEMENT OR CPS
A statement of the practices in the management of digital IDs during all life phases.
CERTIFICATE STATUS SERVICE OR CSS
A service, enabling relying parties and others to verify the status of digital IDs.
CERTIFICATE CHAIN
A hierarchical list digital IDs containing an end-user Subscriber digital ID and CA digital IDs.
DIGITAL ID EXPIRATION
The end of the validity period of a digital ID.
CERTIFICATE EXTENSION
A field in the digital ID used to convey additional information on issues that include: the Public Key, the certified subscriber, the digital ID issuer, and/or the certification process.
DIGITAL ID HIERARCHY
A level based sequence of digital IDs of one (root) CA and subordinate entities that include CAs and Subscribers.
DIGITAL ID MANAGEMENT
Actions associated with digital ID management include storage, dissemination, publication, revocation, and suspension of digital IDs.
CERTIFICATE REVOCATION LIST (CRL)
A list issued and digitally signed by a CA that includes revoked and suspended digital IDs. Such list is to be consulted by Relying Parties at all times prior to relying on information featured in a digital ID.
DIGITAL ID SERIAL NUMBER
A sequential number that uniquely identifies a digital ID within the domain of a CA.
CERTIFICATE SIGNING REQUEST (CSR)
A machine-readable application form to request a digital ID.
CERTIFICATION
The process to issue a digital ID.

CERTIFICATION AUTHORITY (CA)
An authority, such as the GlobalSign CA for Adobe that issues, suspends, or revokes a digital ID.

CERTIFICATE POLICY (CP)
A statement of the practices of a CA and the conditions of issuance, suspension, revocation , etc. of a digital ID. A CP is also used as guidance to establish the trustworthiness of a certification services infrastructure.

DIGITAL ID
The public key of a subject and the associated information, digitally signed with the Private Key of the issuer of the digital ID. Unless explicitly specified, the digital IDs described here are the subscriber's ones. Sometimes referred to as digital certificate.

DIGITAL ID ISSUANCE
Delivery of X.509 v3 digital IDs for authentication and digital signature based on personal data and Public Keys provided by the RA and compliant with RFC 3647 and RFC 3039

DIGITAL ID REVOCATION
Online service used to permanently disable a digital ID before its expiration date

CERTIFICATE REVOCATION LISTS
Online publication of complete and incremental digital IDs revocation lists compliant with RFC 2459

COMMERCIAL REASONABLENESS
A legal term from Common Law. In electronic commerce it means the usage of technology that provide reasonable assurance of trustworthiness.

COMPROMISE
A violation of a security policy that results in loss of control over sensitive information.

CONFIDENTIALITY
The condition to disclose data to selected and authorised parties only.

CONFIRM A DIGITAL ID CHAIN
To validate a digital ID chain in order to validate an end-user subscriber digital ID.

DIGITAL ID
A formatted piece of data that relates an identified subject with a Public Key the subject uses.

DIGITAL SIGNATURE
To encode a message by using an asymmetric cryptosystem and a Hash function such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the Private Key that corresponds to the signer's Public Key and whether the initial message has been altered since the transformation was made.

DISTINGUISHED NAME
A set of data that identifies a real-world entity, such as a person in a computer-based context.

DIRECTORY SERVICE
Online publication of digital IDs allowing the retrieval of a digital ID based on its digital ID identifier.

END-USER SUBSCRIBER
A Subscriber other than another CA.

ENHANCED NAMING
The usage of an extended organization field (OU=) in an X.509 v.3.0 digital ID.

EXTENSIONS
Extension fields in X.509 v.3.0 digital IDs.

GENERATE A KEY PAIR
A trustworthy process to create Private Keys during digital ID application whose corresponding Public Key are submitted to the applicable CA during digital ID application in a manner that demonstrates the applicant's capacity to use the Private Key.

GLOBALSIGN CA FOR ADOBE REGISTRATION AUTHORITY
An entity that verifies and provides all subscriber data to the GlobalSign CA for Adobe.

GLOBALSIGN CA FOR ADOBE PUBLIC CERTIFICATION SERVICES
A digital certification system made available by GlobalSign CA for Adobe as well as the entities that belong to the GlobalSign CA for Adobe domain as described in this CPS.

GLOBALSIGN CA FOR ADOBE PROCEDURES
A document describing the GlobalSign CA for Adobe's internal procedures with regard to registration of end users, security etc.

HASH
An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:

- A message yields the same result every time the algorithm is executed using the same message as input.
- It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.
- It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

IDENTIFICATION
The process to confirm the identity of an entity. Identification is facilitated in Public Key cryptography by means of digital IDs.

INCORPORATE BY REFERENCE
To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.

KEY GENERATION PROCESS
The trustworthy process of creating a Private/Public Key Pair. The Public Key is supplied to a CA during the digital ID application process.

KEY PAIR
A Private Key and its corresponding Public Key in asymmetric encryption.

LEVEL 2 CA

A CDS Subordinate CA that has been issued its Certificate by a Level 1 Root CA or a CDS Level 1 Subordinate CA.

LETTER OF AUTHORIZATION OR LOA

Provided by a duly authorized Organization Representative who is authorized to contractually enroll in the Service, on behalf of the Organization

NOTICE

The result of notification to parties involved in receiving CA services in accordance with this CPS.

NOTIFY

To communicate specific information to another person as required by this CPS and applicable law.

OBJECT IDENTIFIER OR OID

A sequence of integer components that can be assigned to a registered object and that has the property of being unique among all object identifiers within a specific domain.

ORGANIZATIONAL REPRESENTATIVE

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

PKI HIERARCHY

A set of CAs whose functions are organised according to the principle of delegation of authority and related to each other as subordinate and superior CA.

PRIVATE KEY

A mathematical key to create digital signatures and sometimes (depending upon the algorithm) to decrypt messages in combination with the corresponding Public Key.

PUBLIC KEY

A mathematical key that can be made publicly available that is used to verify signatures created with its corresponding Private Key. Depending on the algorithm, Public Keys can also be used to encrypt messages or files which can then be decrypted with the corresponding Private Key.

PUBLIC KEY CRYPTOGRAPHY

Cryptography that uses a Key Pair of mathematically related cryptographic keys.

PUBLIC KEY INFRASTRUCTURE (PKI)

The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a digital ID-based public key cryptographic system.

REGISTRATION AUTHORITY OR RA:

An entity that has the responsibility to identify and authenticate subscribers. The RA does not issue digital ID. It merely requests the issuance of a digital ID on behalf of applicants whose identity it has verified. The RA may be a GlobalSign employee, agent, or customer.

RELATIVE DISTINGUISHED NAME (RDN)

A set of attributes that distinguishes the entity from others of the same type.

RELIANCE

To accept a digital signature and act in a way that shows trust in it.

RELYING PARTY

Any entity that relies on a digital ID for carrying out any action.

REPOSITORY

A database and/or directory listing digital IDs and other relevant information accessible on-line.

REVOKE A DIGITAL ID

To permanently end the operational period of a digital ID from a specified time forward.

SECRET SHARE

A portion of a cryptographic secret that has been divided among a number of physical tokens, such as smart cards etc.

SECRET SHARE HOLDER

A person that holds a secret share.

SHORT MESSAGE SERVICE (SMS)

A service for sending messages of up to 160 characters (224 characters if using a 5-bit mode) to mobile phones that use Global System for Mobile (GSM) communication.

SIGNATURE

A method that is used or adopted by a document originator to identify himself or herself, which is either accepted by the recipient or its use is customary under the circumstances.

SIGNER

A person who creates a digital signature for a message, or a signature for a document.

SMART CARD

A hardware token that contains a chip to implement among others cryptographic functions.

STATUS VERIFICATION

Online service based on the Online Digital ID Status Protocol (RFC 2560) used to determine the current status of a digital ID without requiring CRLs

SUBJECT (OF A DIGITAL ID)

The named party to which the Public Key in a digital ID is attributable, as user of the Private Key corresponding to the Public Key.

SUBORDINATE CA

Certification Authority whose digital IDs are signed by the Root CA, or another Subordinate CA.

SUBSCRIBER

The subject of a digital ID, or a party designated by the Subject to apply for the digital ID.

SUBSCRIBER AGREEMENT

The agreement between a Subscriber and a CA for the provision of public certification services.

.

TRUSTED POSITION
A role within a CA that includes access to or control over cryptographic operations that may allow for privileged access to the issuance, use, suspension, or revocation of digital IDs, including operations that restrict access to a repository.
TRUSTWORTHY SYSTEM
Computer hardware, software, and procedures that provide an acceptable level against security risks, provide a reasonable level of availability, reliability, and correct operation and enforce a security policy.
WEBTRUST PROGRAM FOR CAS: The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities, available at http://www.webtrust.org/certauth fin.htm.
WEB -- WORLD WIDE WEB (WWW)
A graphics based medium for the document publication and retrieval of information on the Internet.
WRITING
Information accessible and usable for reference.
X.509
The standard of the ITU-T (International Telecommunications Union-T) for digital IDs.

11.0 List of acronyms

CA: Certification Authority

RA: Registration Authority

LRA: Local Registration Authority

CEN/ISSS: European Standardisation Committee / Information Society Standardisation System

CP: Digital ID Policy

CPS: Certification Practice Statement

ETSI: European Telecommunications Standards Institute

GSCA: GlobalSign Certification Authority

IETF: Internet Engineering Task Force

ISO: International Standards organization

ITU: International Telecommunications Union

OCSP: Online Certificate Status Protocol

PKI: Public Key Infrastructure

RFC: Request for Comments

SSCD: Secure Signature Creation Device

SSL: Secure Socket Layer

VAT: Value Added Tax