KEYNECTIS

▪ CERTIFICATION PRACTICE STATEMENT

SUPPORT OF KEYNECTIS CDS ELECTRONIC CERTIFICATION SERVICES

Date:05/11/2010

Réf : CPS_KEYNECTISCDS_CA_GB-V1.2.doc

CERTIFICATION PRACTICE STATEMENT FOR KEYNECTIS CDS ELECTRONIC CERTIFICATION SERVICES

Document Version	1.2		Total No. of Pages:		75
Document Status	☐ Project			☒ Final Version	
Document Author	Dominique MANENC			KEYNECTIS	

Distribution List:	☒ External		☐ Internal	

Document History:

Date	Version	Author	Comments	Verified by
10/10/2007	1.00	DM	Version to publish Adobe Acceptation	Manenc
05/11/2009	1.1	DM	Change in subca name figure and adress	Manenc
05/11/2010	1.2	DM	Change in subca name figure and logo	Manenc

Publication date: 05/11/2010
Effective date: 05/11/2010

Ref : CPS_KEYNECTISCDS_CA_GB-V1.2.doc
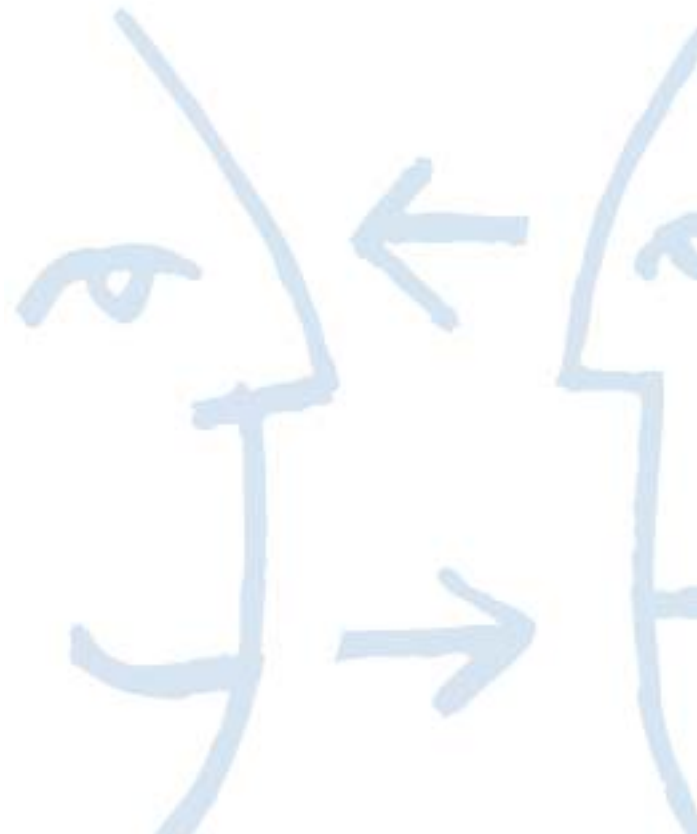
Preamble

Without limiting the rights reserved and except as authorized below, no part of this publication may be reproduced, recorded, or transmitted in any form or by any means (electronic, mechanical, photocopy, recording, or other), without prior written permission from the KEYNECTIS Corporation.

Notwithstanding the above, permission is granted to reproduce and distribute this Certification Practice Statement (CPS) on a non-exclusive, royalty-free basis provided that:

▪ The copyright notice above and beginning paragraphs are prominently displayed at the beginning of each copy and that,
▪ This document is accurately reproduced in full, complete with attribution to the KEYNECTIS Corporation.

Requests for any other permission to reproduce this KEYNECTIS Certification Practice Statement must be addressed to KEYNECTIS, 11 13 rue René Jacques 92131 Issy les Moulineaux Cedex France

Comment: The KEYNECTIS Certification Practice Statement may be granted under license by KEYNECTIS to commercial entities who wish to use it as part of their own electronic certification services.

KEYNECTIS is a brand filed by the KEYNECTIS Corporation.

KEYNECTIS, a company created in 2004 from the merger between the Certplus and PK7 companies, has acquired an expertise in marketing electronic certification services.

This Certification Practice Statement governs the delivery and use of KEYNECTIS electronic certification services, which include certification request, request validation, certificate issuance, acceptance, use and revocation.

This CPS and any all amendment thereto are incorporated by reference into all of the issued certificates.
The CPS and this certificate are copyrighted: Copyright © KEYNECTIS. All rights reserved.

OVERVIEW

You the user, acknowledge that KEYNECTIS or RA organization has advised you to seek training and obtain adequate information to become familiar with digital signatures and certificates before requesting, using and trusting a certificate. It is your responsibility to decide whether or not the certificate offered by KEYNECTIS meets your needs.

Before submitting a certificate request, you must generate a key pair and protect the private key from any violation using a reputable method, as further described herein. Approved external devices and software programs are responsible for providing this security.

You must accept a certificate as specified in section 4 before releasing it to others or using it in any way. By accepting a certificate you acknowledge that you are making important representations.

If you are the recipient of a digital signature of certificate, it is your responsibility to decide if you can trust the signature or certificate. Before doing so, you must check the KEYNECTIS publicized information to make sure that the certificate is valid and unrevoked. Then, use the certificate to verify that the digital signature was created during the certificate's active validity date using the private key corresponding to the public key

listed on the certificate. This verification will also ensure that the message related to the digital signature was not changed.

You agree to notify the appropriate certification authority if your private key is violated, as further described herein.

This Certification Practice Statement contains different guarantees and promises made by KEYNECTIS . Beyond that, any guarantee is refused and the responsibility of KEYNECTIS and certification authorities is limited.

The Certification Practices Statement includes a series of various provisions and prohibits infringements.

To find out more, visit the KEYNECTIS website at http://www.keynectis.com.

COMMENTS AND SUGGESTIONS

KEYNECTIS gladly welcomes comments and suggestion for future revisions of this CPS.
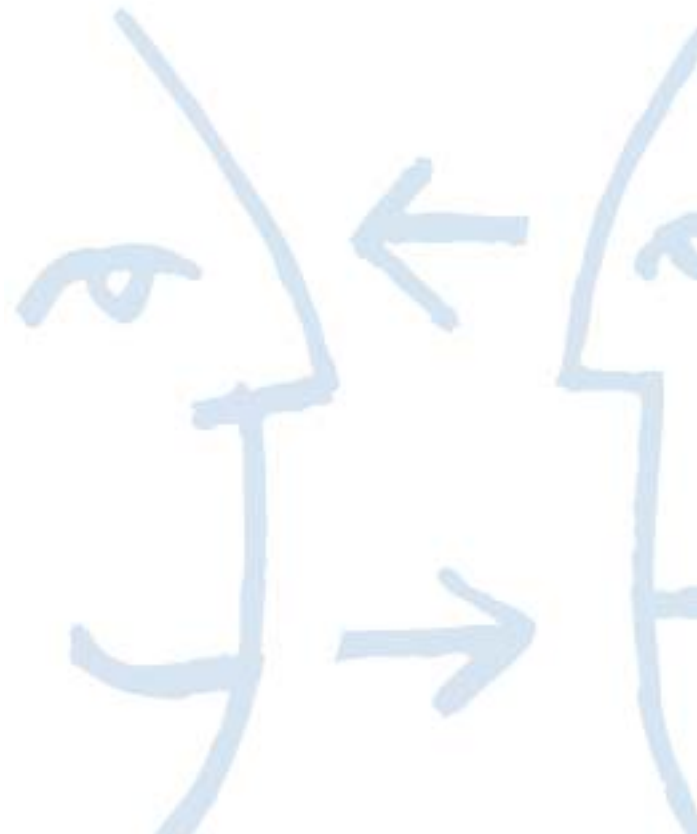Please send comments to: info@keynectis.com.

TABLE OF CONTENTS

FIGURES INDEX

INDEX OF TABLES

Ref : CPS_KEYNECTISCDS_CA_GB-V1.2.doc

1   INTRODUCTION

This chapter presents the KEYNECTIS Certification Practice Statement (CPS) and describes its structure and underlying conventions. It concludes with a list of abbreviations and acronyms used in the CPS to make it easier to read and understand.

1.1   Overview

This KEYNECTIS Certification Practices Statement presents the practices that KEYNECTIS, its KEYNECTIS-CDS Certification Authorities (CA) and authorized non-KEYNECTIS Sub Certification Authorities participating in the provision of KEYNECTIS CDS electronic certification services employ in issuing and managing certificates and in maintaining a certificate-based public key infrastructure (PKI).

The CPS details and controls the certification process, from establishing certification authorities, implementing operations, to registering certificate applicants.

CDS Electronic certification services provide for issuing, managing, using, revoking, and renewing of CDS certificates. The CPS is intended to legally bind and provide notice to all parties that create, use, and validate certificates within the context of the CDS electronic certification services.

Certified Document Services (CDS) is a new platform offering first available in the Acrobat 6.0 product family. Using digital signature technology, CDS provides recipients with assurances that certified PDF documents are authentic – that they did originate from their stated author and the portions of the document signed by the author have not been modified since authoring.

Adobe Systems Incorporated (Adobe) has contracted with KEYNECTIS as 3rd party to provide Certification Authority (CA) services including all registration authority (RA) functionality, for Certified Document Services.

The Certification Authority "KEYNECTIS–CDS" is governed by the following policy in compliance with the following upper level CA Certificate Policy named "CDS Certificate" Policy whom attributed Object Identifier (OID) of the policy is: 1.2.840.113583.1.2.1.

KEYNECTIS CDS electronic certification services (ECS) are designed to support secure document exchange and other general services to meet users' technical, business, and personal needs for electronic signatures and other network security services. To accomplish this, KEYNECTIS-CDS CA is issuing, managing, and revoking certificates in compliance with published practices.
KEYNECTIS CDS CERTIFICATION SERVICES' management and administration features are designed to handle a large, widely distributed community of users with different needs for communications and information security.

1.2   Identification

This Certification Practice Statement (CPS) is called the KEYNECTIS-CDS CPS.
The Attribute Object Identifier (OID) for this CPS is 1.3.6.1.4.1.22234.2.8.2.1.1.

1.3   Citing the CPS

This Certification Practices Statement should be cited in other documents as the "KEYNECTIS-CDS CPS" or the "KEYNECTIS-CDS Certification Practice Statement". It is internally cited as the "CPS" or as "CPS Section x", and its appendices are cited as "Appendix Section 1.x". The CPS is updated regularly.

Versions of the CPS are indicated by a version number following "CPS" (e.g., "version 1.0" or "CPS 1.0").

1.4 Community and Applicability

The community for this CPS includes all KEYNECTIS-CDS Subordinate CAs, RAs, and Subscribers whose digital IDs chain, via the KEYNECTIS-CDS CA, to the Adobe Root CA embedded in Acrobat®, Reader®, and LiveCycle® products by Adobe, along with all Relying Parties who rely on such digital IDs.

The community for this CPS is part of ADOBE's CDS Community and all Digital IDs issued within the CDS PKI community have the certificate policy extension populated with the OID identified in Section 1.2.

Subscriber certificates issued by KEYNECTIS CDS CA and all Sub-CAs are to be used only for digitally signing Adobe PDF documents and the verification of these documents, in Supported Platforms.
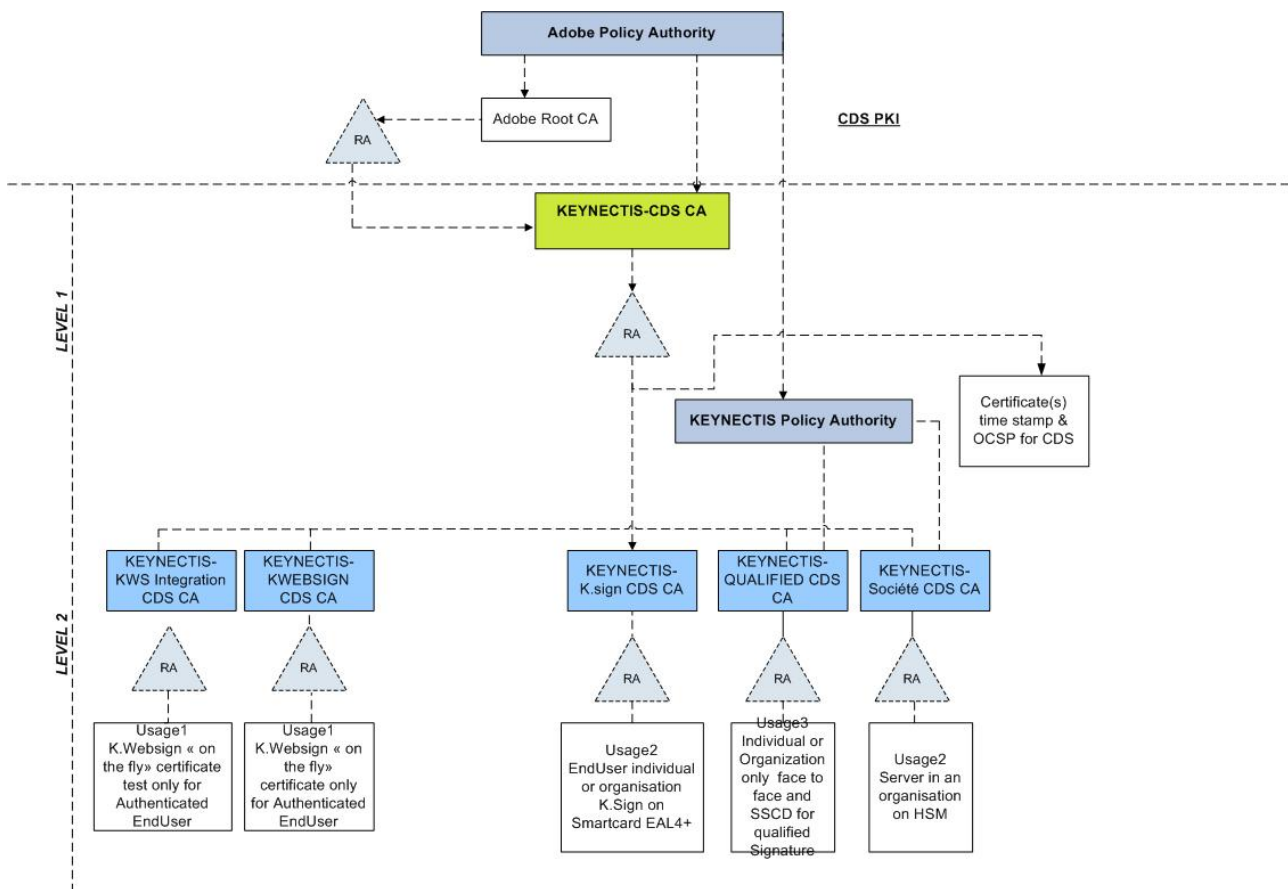
Figure 1: CDS PKI with KEYNECTIS-CDS CAs

1.5 Certification Authorities

KEYNECTIS CDS-CA is an Adobe authorized 3rd party that creates and issues CDS digital IDs to Subscribers under this Policy. In this document KEYNECTIS-CDS CAs refers to CA level 1 and Level 2.

1.6 Registration Authorities

Registration Authorities (RAs) manage the certificate lifecycle for their respective CAs. RAs are responsible for requesting the CA to issue and revoke digital IDs in accordance with this Policy, as well as any additional relevant policies and procedures including their respective CPSs, operating procedures, etc.

1.7 End entities

End Entities are Subscribers and Relying Parties.
A Subscriber is any authorized individual or organization that has a CDS digital ID issued to it and uses that digital ID to sign or Cosign a CDS document.
Relying Parties are recipients of CDS documents who wish to verify the Subscriber's signature.

1.8 Applicability

CDS signing digital IDs may only be issued by authorized CAs to Subscribers in accordance with this CPS.
CDS digital IDs may only be used to digitally sign and verify Adobe PDF documents On Supported Platforms

1.9 Policy Authority

This Policy is managed by the KEYNECTIS Policy Authority. The KEYNECTIS Policy Authority consists of selected members of KEYNECTIS' management team. .

1.10 Policy Authority Contact

KEYNECTIS Policy Authority, 11 13 rue René Jacques 92131 Issy les Moulineaux Cedex France

1.11 Underlined Text

Underlined text represents the first instance of defined terms used in this document. The CPS is published by KEYNECTIS:

▪ in electronic form at the following address: www.keynectis.com/PC
▪ in paper format from 11 13 rue René Jacques 92131 Issy les Moulineaux Cedex France
▪ The "unprotected" mode (http://) must be used to access the official version of all of the documents open through the Web. If a "protected" mode is required, replace http:// with https:// invoking the Secure Socket Layer (SSL) security protocol.

For any additional information, please send an email to info@keynectis.com.

1.12 Customer Service Assistance, Education, and Training

This CPS assumes that the reader is familiar with digital signature, PKIs and KEYNECTIS' electronic certification services. If not, we advise some training in the use of public key techniques before the reader applies for a certificate.

Educational and training information is available from KEYNECTIS.

KEYNECTIS customer service (service.clients@keynectis.com) can also provide additional assistance.

All electronic certification services applicants and subscribers acknowledge this CPS (incorporated as reference in the subscriber agreement) and that:

▪ They have been advised to receive proper training in the use of public key techniques before requesting a certificate and that,
▪ The documentation and training about digital signatures, certificates, PKI, and electronic certification services are available from KEYNECTIS.

1.13 Table of Acronyms and Abbreviations

CA	Certification Authority
CDS	Certified Document Services by ADOBE
RCA	Root Certification Authority
RA	Registration Authority
CSR	Certificate Signing Request
CPS	Certification Practice Statement
DAM	Draft Amendment
GMT	Greenwich Meridian Time
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
HSM	Hardware Security Module
PKI	Public Key Infrastructure
UVI	Unverified Information
CRL	Certificate Revocation List
RDN	Relative Distinguished Name
PGP	Politique de gestion de preuves
PIN	Personal Identification Number (activation data)
PKCS	Public Key Cryptography Standards
PRISV1/2	Politique de référencement intersectoriel de sécurité Version ½
SCP	KEYNECTIS Security Procedures
RSA	A cryptographic system
CSR	Certificate Signature Request.
S/MIME	Secure Multipurpose Internet Mail Extensions
ECS	Electronic Certification Services
SSL	Secure Socket Layer
URL	Uniform Resource Locator (standardized resource locator on the WWW)
EU	End User
WWW or WEB	World Wide Web
X.509	The ITU-T standard for certificates and the corresponding authentication framework

Table 1 – Acronyms and abbreviations

2   GENERAL PROVISIONS

2.1   CA Obligations

2.1.1   KEYNECTIS–CDS CA obligations (level 1)

KEYNECTIS-CDS CA represent and warrant to all Relying Parties placing reasonable reliance on a CDS CA-issued Digital ID that chains up to KEYNECTIS-CDS CA that the (a) KEYNECTIS-CDS CA took reasonable steps (no less than the procedures set forth in Section 3.1.7 of this document and in Sections 3.1.8 and 3.1.9 of the Document Adobe CDS Certificate Policy to verify the information contained in the Digital ID is accurate, (b) information in the Digital ID accurately reflects the information provided to KEYNECTIS-CDS CA by the Subscriber, (c) Subscriber has accepted the Digital ID according to the provisions of this policy, (d) KEYNECTIS-CDS CA has complied with Adobe CDS Policy and its CPS, and (e) KEYNECTIS-CDS CA has auditing procedures in place to ensure that all Level 2 CAs signed by KEYNECTIS-CDS CA complied with this applicable CPS.

KEYNECTIS-CDS CA, to the extent specified in the referenced CPS sections, represents and warrants that it will:
▪ Establish the infrastructure and certification services, including the installation and management of the KEYNECTIS reference archives, as stated in this CPS.
▪ Respect the Adobe CDS PKI Policy established for the Root CA,
▪ Perform validation procedures for the specified certificate usage, as defined in this CPS.
▪ Issue certificates according to the CPS and honor the various representations to subscribers and relying parties according to the CPS;
▪ Publish accepted certificates in accordance with the CPS
▪ Ensure that each potential Subscribers is notified that a certificate has been Issued
▪ Perform the obligations of a CA and support the rights of subscribers and relying parties who use the certificates according to the CPS;
▪ Revoke certificates in accordance with the CPS; upon revocation of a certificate, ensure that the subscribers is notified of the revocation by email, postmail, telephone or facsimile
▪ Provide notification of certificate revocation via CRLs in repository in accordance with this CPS.
▪ Ensure the expiration, re-enrollment, and renewal of certificates in accordance with the CPS;
▪ Comply with the CPS provisions,
▪ Ensure that all potential Subscribers are bound to a Subscriber Agreement applicable to usage of certificate (see section 4)
▪ Maintain records (including without limitations CRLs) of the users and documents necessary to respond to requests concerning its operation for as long as the applicable record or document is valid but in no event less than three (3) years

KEYNECTIS-CDS CA further represents and warrants that all Level 2 CAs are and will be compliant with the Adobe CDS Certificate Policy.

KEYNECTIS-CDS CA guarantees that their own private keys will not have not been violated or compromised and unless they provide notice to the contrary through the KEYNECTIS reference archives and have provided immediate notice to Adobe upon becoming aware of any such violation or compromise.

2.1.2   KEYNECTIS–CDS Sub-CA obligations (level 2)

Each KEYNECTIS-CDS Sub-CAs, to the extent specified in the referenced CPS sections, represents and warrants that it shall:
▪ Establish the infrastructure and certification services, as stated in this CPS.
▪ Comply with the KEYNECTIS-CDS CA CPS for the level 1 state in the ADOBE CDS Certificate policy
▪ Perform validation procedures for the specified certificate usage, no less as defined in this CPS.
▪ Ensure that all potential Subscribers are bound to a Subscriber Agreement applicable to usage of certificate (see section 4)

- Issue certificates according to the CPS and honor the various representations to subscribers and relying parties according to the CPS;
- Publish accepted certificates in accordance with the CPS
- Maintain records (including without limitations CRLs) of the users and documents necessary to respond to requests concerning its operation for as long as the applicable record or document is valid but in no event less than three (3) years
- Ensure that each potential Subscriber is notified that a certificate has been Issued
- Perform the obligations of a CA and support the rights of subscribers and trusted parties who use the certificates according to the subca CP and CPS;
- Revoke digital IDs that it issues according to the provisions in this policy regarding revocation including without limitation the provisions of section 4
- Upon revocation of a digital ID, ensure that the subscriber is notified of the revocation by email, postmail, telephone or facsimile
- Provide notification of certificate revocation via CRLs in repository, as more fully in accordance with this CPS
- Provide renewal and replacement of digital IDs,
- Publish and adhere to a privacy policy

2.2   RA Obligations

In compliance with the Adobe CDS Certificate Policy, KEYNECTIS-CDS CA, as a CDS subordinate CA, delegates specific registration activities to one or more RAs in accordance with the usage of the Digital ID to issue and RA agreement entered into with KEYNECTIS.

As described in section 4 below 3 RAs are identified:

Organization RA implemented in the Usage1 certificate live cycle management

KEYNECTIS RA implemented in the Usage 2 certificate live cycle management

External RA implemented in the Usage 3 certificate live cycle management.

KEYNECTIS CDS CA remains responsible for the services provided by its CDS RA in accordance with this CPS. KEYNECTIS-CDS CA OR SUBCA warrants that the activities of its CDS RA are conducted in accordance with the Adobe's CDS certificate policy.

2.3   End Entity Obligations

2.3.1   End entity in Trusted roles for SubCA generation process

Any end entity involved in a KEY ceremony process in a trusted role must:

- Maintain its private keys in a secure manner according to this CPS.
- Not disclose to anyone any information needed to access its private keys, including without limitation, the PINs, passwords, passphrases or other information or mechanisms used to protect their private keys;
- Request revocation of its certificate if it has any reason to suspect that its private keys or any information used to access its private keys have been compromised
- Conform to all requirements and follow all instructions during the KEYNECTIS-CDS CAs key ceremony
- Conform to all other requirements as may be specified from time to time by KEYNECTIS.

2.3.2   Subscribers

In general and as specified in a Subscriber Agreement between the KEYNECTIS-CDS CA or Subordinate CA and the Subscriber for each usage of Digital IDs issued by KEYNECTIS-CDS CA or Subordinate CA, a Subscriber must:

- Accurately represent itself in all communications with the KEYNECTIS-CDS CA or Subordinate CA;
- At all times, protect the private key associated with the public key in any digital IDs issued by KEYNECTIS-CDS CA or Subordinate CA in accordance with this policy;
- Notify, in a timely manner, the KEYNECTIS-CDS CA or Subordinate CA that issued its digital ID of suspicion that its private key is compromised or is reasonably believed to have been compromised. Such notification shall be made with the KEYNECTIS-CDS CA or Subordinate CA as specified in the CA's CPS;

▪ Abide by all the terms, conditions, and restrictions in this policy and in the applicable Subscriber Agreement.

The Root CA, KEYNECTIS-CDS CA and Subordinate CAs reserve the right to revoke the digital ID of any Subscriber who violates the obligations specified in this Section or in the applicable Subscriber Agreement. If such a violation occurs, the digital ID of the Subscriber shall immediately be revoked by the KEYNECTIS-CDS CA or Subordinate CA and other appropriate actions taken.

Subscribers may either apply for digital IDs directly or organization acting on behalf of a Subscriber or group of Subscribers may apply for digital ID(s).

2.3.2.1 Applicant is an organization acquiring a certificate on behalf of an individual subscriber

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), the KEYNECTIS-CDS CA OR SUBCA requires the organization 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 the specific person that 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 KEYNECTIS-CDS CA or Subordinate CA 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:

   (i)generate or use a key pair generated in accordance with section 4 & 6 of this CP by the KEYNECTIS-CDS CA or Subordinate CA or its RA and take all reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key;

   (ii) Acknowledge that the information identifying the Subscriber in the digital ID is true and accurate, or notify the KEYNECTIS-CDS CA or Subordinate CA immediately upon any inaccuracies in that information;

   (iii) Use the certificate exclusively for CDS purposes, consistent with this policy; and

   (iv) Request Certificate revocation immediately upon any actual or suspected loss, disclosure, or other compromise of the Subscriber's private key.

2.3.2.2 Applicant is an organization acquiring a certificate on behalf of the organization

When the applicant is an organization acquiring and managing a digital ID on behalf of the organization (i.e., an organizational digital ID), the CDS CA or Subordinate CA shall require the organization to:

(a) maintain processes, including, without limitation, 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 digital ID custodian);

(b) maintain information that permits a determination of the specific person that signed a particular document;

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

(d) prevent sharing of organizational digital IDs amongst members of the organization;

(e) acknowledge that the information identifying the organization in the digital ID is true and accurate, or notify the KEYNECTIS-CDS CA OR SUBCA immediately upon any inaccuracies in that information;

(f) ensure that the digital ID custodian enters into a binding Subscriber Agreement which obligates the digital ID custodian to:

(i) generate or use a key pair generated in accordance with section 4 & 6 of this CP by the CDS CA or Subordinate CA or its RA and take all reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key;

(ii) use the digital ID exclusively for CDS purposes, consistent with this policy;

(iii) not share the digital ID nor any activation data related to the private key corresponding to the public key in the organizational digital ID; and

(iv) request digital ID revocation immediately upon any actual or suspected loss, disclosure, or other compromise of the Subscriber's private key;

(g) notify the KEYNECTIS-CDS CA OR SUBCA immediately upon any actual or suspected loss, disclosure, or other compromise of the private key corresponding to the public key in the organizational digital ID; and

(h) request revocation of an organizational digital ID upon any actual or suspected loss, disclosure, or other compromise of the private key corresponding to the public key in the organizational digital ID.

2.4   Relying Party Obligations

In addition to any other Relying Party obligations in the Acrobat End User License Agreement, the KEYNECTIS-CDS CA uses commercially reasonable efforts to notify all relying parties, including, without limitation, via the user Notice field within each Digital ID it publishes, that reliance on a CDS-signed document is only permitted if the signature is verified on a Supported Platform. For the purposes of this policy, Supported Platform means those applications specified on the CDS information web page, currently **http://www.adobe.com/security/partners_cds.html**

2.5   Repository obligations

See section 2.10

2.6   Liability

2.6.1   Adobe Root CA liability

Warranty disclaimers and limitations on Adobe Root CA liability are described in the CDS Certificate policy referenced with OID= 1.2.840.113583.1.2.1 in the chapter named Adobe Root CA Liability.

2.6.2   KEYNECTIS-CDS CA and subordinate CA liability

KEYNECTIS-CDS CA provides the limited warranty at the time of Certificate Issuance:

(i)   it has complied with the CDS Certificate Policy (OID= 1.2.840.113583.1.2.1) and this CPS

(ii)   the information contained within the certificate accurately reflects the information provided to KEYNECTIS-CDS RA by the applicant

(iii)   it has taken reasonable steps to verify that the information within the certificate is accurate; and

(iv)   it has required the subscriber to accept the Subscriber Agreement. The nature of the steps KEYNECTIS takes to verify the information contained in a CDS certificate is set forth in section 4.

Except as expressly stipulated above, KEYNECTIS-CDS CA and subordinate CA disclaim all warranties and obligations of any type including any warranty of merchantability or special use, and any warranty of the accuracy of information provided, and also disclaim any and all liability for negligence or lack of reasonable care.

2.6.2.1   Limitations on KEYNECTIS-CDS CA liability

Except for that which has been expressly stipulated in the CPS, CAs:

▪ Do not guarantee the accuracy, authenticity, reliability, completeness, correctness, merchantability, or fitness of any information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of certification authorities or KEYNECTIS;

Assume no responsibility for the information contained in a certificate, provided that the certificate and the population of that content by the KEYNECTIS-CDS CA comply with this CPS;

▪ Do not guarantee "non repudiation" of a certificate or message (non repudiation is determined exclusively by law and the applicable dispute resolution mechanisms);

▪ Do not warrant any software.

2.6.2.2   Exclusion of Certain damage elements

Except for any indemnification obligations to Adobe under the Adobe CDS CP or in any agreements between KEYNECTIS and Adobe,no event shall KEYNECTIS-CDS CAs be held liable for any indirect, special, incidental, consequential, or penal damage in connection with the use, delivery, effectiveness, or nonperformance of certificates, digital signatures, or any other transaction or services offered or expected by this CPS, even if the issuing authorities or KEYNECTIS, or both, have been notified of the possibility of these damages.

2.6.2.3   Damage and loss limitations

Under no circumstances shall the accumulated liability to all parties (including, but not limited to, an applicant, recipient or a trusting party) of a certification authority and all superior CAs in the certification chain to which the CA certificate belongs, exceed the liability cap specified in KEYNECTIS-CDS subordinate CA Certificate Policy.

The accumulated liability of all certification authorities to any and all individuals affected by a certificate, for all digital signatures and transactions related to such certificate, is limited to the cap indicated in KEYNECTIS-CDS CA or subordinate Certificate Policy incorporated by reference in the Subscriber Agreement.

The cap on damages applies to loss and direct damages of all types, including but not limited to an applicant, recipient, or a trusting party, that are caused by trust in or use of a certificate that is issued, managed, used, suspended, or revoked by a CA or the expiration of such certificate.

2.6.3   Applicant liability to Trusting Parties

Without limiting other subscriber obligations under this CPS, subscribers are liable for any misrepresentations they make in certificates to third parties who, having verified one or more digital signatures with the certificate, reasonably trust the content of such certificate.

2.6.4   RA liability

See section 2.2

2.7   Financial responsibility

2.7.1   Indemnifications

2.7.1.1   By subscribers

By accepting a certificate from KEYNECTIS-CDS CA, the subscriber agrees to indemnify the Root CA to which subscriber's digital ID chains, the KEYNECTIS-CDS CA, and their contractors harmless from any act or omissions resulting in liability, any damage or loss, legal actions, or expenses of any kind, including reasonable attorney's fees, that the CAs, KEYNECTIS, and their contractors may incur due to the use or publication of a certificate following:

▪ A false statement made by the subscriber (or by a person acting upon instruction from anyone authorized by the subscriber),

▪ Failure by the subscriber to disclose a material fact if the false statement or omission was made negligently or with the intent to deceive the CA, KEYNECTIS, or any individual receiving or trusting the certificate or,
▪ The subscriber's failure to protect his/her private key, use of hardware Security module or otherwise take the necessary precautions to prevent the violation, loss, disclosure, modification, or unauthorized use of the subscriber's key.

2.7.1.2 By relying parties

In addition to any Relying Party agreements (including, without limitation the Adobe Acrobat EULA), when a Relying Party accepts a digitally signed CDS document from a Subscriber, the KEYNECTIS-CDS CA shall use all reasonable efforts to require 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 certificate status prior to any reliance on a digital signature from a Subscriber.

2.7.2 No fiduciary relationship

CAs and KEYNECTIS are not the fiduciary agents, nominees, or other representatives of subscribers or trusting parties.
The relationship between CAs (or KEYNECTIS) and trusting parties is not that of an agent and principal. Neither subscribers nor trusting parties have the authority to bind a CA (or KEYNECTIS) by contract or otherwise. CAs and KEYNECTIS shall make no representation to the contrary, either expressly, implicitly, by appearance, or otherwise.

2.7.3 Dangerous Activities

KEYNECTIS' electronic certification services are not designed or authorized for resale as monitoring equipment in hazardous conditions or for uses requiring fail-safe performance (for example, nuclear facilities, aircraft navigation or communication, or air traffic control systems), where failure could lead directly to death, injury or severe environmental damage.

2.7.4 Administrative process

No stipulation

2.8 Interpretation and enforcement

In the event of a conflict between this CPS and other rules, guidelines or contracts, the subscriber shall be bound by the provisions of this CPS, unless the other contract (i) predates the first publication of this CPS; or (ii) specifically takes precedence over this CPS, for which such contract shall be valid against parties of said CPS, except to the extent that the provisions of this CPS are prohibited by law.

2.8.1 Governing law

Except as otherwise specified in other applicable agreements between CDS participants, this CPS, its implementation, interpretation, and its validity are governed by CEE laws, notwithstanding any other choice of applicable law in the contract or otherwise, and without the requirement of a commercial establishment in France. The choice of CEE law aims at the uniformity of procedures and interpretation for all users, no matter where they reside or how they use their certificates.

2.8.2 Compliance with export Laws and regulations

Export of certain software used as part of the KEYNECTIS certification services may require the authorization of the appropriate government authorities. The parties shall comply with the export laws and regulations in effect.

2.8.3 Dispute resolution and procedures

2.8.3.1 Notification among parties of a dispute

Except as otherwise specified in other applicable agreements between CDS participants, before invoking any dispute resolution mechanism (including arbitration) with respect to a dispute involving any aspect of this CPS or a certificate issued by an RA, aggrieved individuals shall notify KEYNECTIS, the CA concerned, and any other party affected by the resolution of a dispute.

2.8.3.2 Official resolution of legal disputes

Except where each directly involved party agrees to an alternative dispute resolution (arbitration for example), any action aimed at applying a provision of this CPS or arising in connection with the CPS or any other business relationship between the parties concerned, shall be brought before a courts of IRELAND. Each person hereby agrees that such courts shall have exclusive personal jurisdiction over him/her and each person hereby submits to the exclusive personal jurisdiction of these courts. The parties hereby waive any right to a jury trial regarding any action brought in connection with this CPS or KEYNECTIS certification services. If the parties choose an alternative resolution method, French law shall govern the arbitration and procedure.

2.8.3.3 Succession and Assignment

This CPS grants and binds successors, executors, heirs, representatives, administrators, and assignees of the parties, regardless of whether they are explicit, implicit or apparent. The rights and obligations explained in this CPS are assignable to the parties by operation of law (including after a merger or the transfer of a controlling interest in share ownership) or otherwise, provided that the assignment complies with the CPS on the termination or suspension of the CA's operations, and provided further that the assignment is not a novation of any other debt or obligation that the assigning party owes to other parties at the time of such assignment.

2.8.3.4 Merger

No term or provision of this CPS directly affecting the rights and obligations of KEYNECTIS or any CA may be orally amended, waived, supplemented, modified, or terminated without an authenticated message or document from the affected party; unless authorized by the CPS.

2.8.3.5 Severability

If any of this CPS, or its application, is found to be invalid or unenforceable for any reason or any extent, the remainder of this CPS (and the application of the invalid or unenforceable provision to other individuals or circumstances) shall be interpreted so as to best comply with the intention of its parties.

It is expressly agreed that each and every provision of this CPS that stipulates a limit of liability, disclaimer, or limitation of warranty of another obligation, or exclusion from damages is severable and independent of any other provision and is to be enforced as such.

2.8.4 Interpretation and translation

Unless otherwise stipulated or in areas where an absolute requirement exists (including, without limitation, any timing requirements related to revocation or publication of information), this CPS shall be interpreted in conformance with what is commercially reasonable under the circumstances. The interpretation of this CPS shall take into account its international scope and application, in view of the uniformity of its application and observance of good faith.

Translated versions of this CPS are available in some languages and are found in the archives. In the event of a conflict between the French and non-French versions, this original english version shall be retained.

2.8.5 No waiver

Failure by an individual to comply with a CPS provision shall not be deemed a waiver of future compliance with that or any other provision.

2.8.6 Communications

Any party who would like to, or is required to, issue a notice, demand, or request as part of this CPS shall do this using a digitally-signed message that complies with the requirements of this CPS, or in writing.

Electronic communications shall be effective upon the sender's receipt of a digitally-signed acknowledgement of receipt from the recipient. The acknowledgement of receipt must be received within five (5) days; or else written notice must be sent.

Communications in writing shall be delivered by registered mail with acknowledgement of receipt, to the following address: KEYNECTIS, 11 13 rue René Jacques 92131 Issy les Moulineaux Cedex France

2.9 Fees

KEYNECTIS may charge subscribers for the use of its electronic certification services, as described in contract entered with KEYNECTIS.

2.10 Publication and repository

2.10.1 Publication of KEYNECTIS-CDS CA and Subordinate CA information
KEYNECTIS maintains a repository that contains the following
- One or more certificate revocation list (ARL/CRLs) issued by the KEYNECTIS-CDS CA or SUBCA, such that notice is provided of all revoked digital IDs within the CDS PKI
- Copies of past and current versions of its CPS indicating the effective period of each copy of the CPS

2.10.2 Frequency of Publication
Each certificate shall be published in the Repository by the KEYNECTIS-CDS CA OR SUBCA following issuance and acceptance of the certificate in accordance with section 4 of this policy.
A CRL shall be published by the KEYNECTIS-CDS CA OR SUBCA in its Repository at least every 24 hours in accordance with Section 4 of this policy.
KEYNECTIS retains copies of all Certificates online for two years, but does not archive or retain expired or superseded CRLs. KEYNECTIS may provide other online status mechanisms such as Online Certificate Status Protocol (OCSP) for checking certificate status requests.

2.10.3 Access controls
KEYNECTIS uses reasonable efforts to make the Repository available to all parties 24 hours per day, seven days per week, subject to routine maintenance.

2.10.4 Repository
No stipulation

2.11 Compliance Audit and Reporting
KEYNECTIS-CDS CA OR SUBCA is operated in the KEYNECTIS high security Bunker and is governed by the Audit policy of this infrastructure.

2.11.1 Frequency of entity compliance Audit
KEYNECTIS CA operations are subject to annual compliance audits as part of the qualification of KEYNECTIS as Certification Service Provider (CSP) under the French scheme that enforces compliance to the European Directive on electronic signature (EC 1999/93).

To do so, France has set up a qualification scheme where voluntary CSP (such as KEYNECTIS) are audited by an accredited body. Audits are performed yearly as follows:

- an initial qualification audit is performed on year 1 to issue a compliance certificate to KEYNECTIS,

- maintenance audits are performed on year 2 and 3 to check that KEYNECTIS operations are still compliant and that recommendations issued from the previous audit, if any, are implemented in a proper way,
- an initial audit has to be performed on year 4 to issue a new compliance certificate to KEYNECTIS and so on.

In case audits are not performed as required, the compliance certificate is withdrawn and the CSP is no longer referenced on the qualification body website (**http://www.lsti.fr/** item "Organisms certifiés").

This audit process is governed by a technical document issued from COFRAC (the French committee for accreditation: **http://www.cofrac.fr/**), reference of the document is CEPE REF 21 "Specific requirements for CSP qualification".

2.11.2 Identity/qualifications of Auditor

Compliance auditors have competence in the field of compliance audits.

Auditors are BS7799 "lead auditors" qualified (trained for Information Security Management System (ISMS) implementation) in accordance with ISO 27001:2005, i.e able to conduct audits for Certification Bodies. In addition, they are familiar with PKI operation and requirement similar to the one is the present CPS.

Compliance auditor performs such compliance audits as a primary responsibility on behalf of the qualification body.

2.11.3 Auditor's relationship to audited party

The qualification body and compliance auditor is a private company accredited by the French accreditation body, and is totally independent from KEYNECTIS.

The qualification body is LSTI SAS - 30 bis, rue du Vieil Abreuvoir 78100 Saint-Germain-en-Laye - Phone/Fax : +33 1 30 61 50 60 – **www.lsti.fr**

2.11.4 Topics covered by Audit

The purpose of a compliance audit shall be to verify that a component operates in accordance with the present CPS.

Topics covered by the annuals audits are issued from the ETSI standard TS 011 456 "Security requirement for certification authorities issuing qualified certificates" and includes

7.2   Public key infrastructure - Key management life cycle
7.2.1   Certification authority key generation
7.2.2   Certification authority key storage, backup and recovery
7.2.3   Certification authority public key distribution
7.2.4   Key escrow
7.2.5   Certification authority key usage
7.2.6   End of CA key life cycle
7.2.7   Life cycle management of cryptographic hardware used to sign certificates
7.2.8   CA provided subject key management services
7.2.9   Secure-signature-creation device preparation
7.3   Public key infrastructure - Certificate Management life cycle
7.3.1   Subject registration
7.3.2   Certificate renewal, rekey and update
7.3.3   Certificate generation
7.3.4   Dissemination of Terms and Conditions
7.3.5   Certificate dissemination
7.3.6   Certificate revocation and suspension
7.4   CA management and operation
7.4.1   Security management
7.4.2   Asset usage and management
7.4.3   Personnel security

7.4.4   Physical and environmental security
7.4.5   Operations management
7.4.6   System Access Management
7.4.7   Trustworthy Systems Deployment and Maintenance
7.4.8   Business continuity management and incident handling
7.4.9   CA termination
7.4.10   Compliance with Legal Requirements

2.11.5 Actions taken as a result of deficiency

When the compliance auditor finds a discrepancy with the requirements of this CPS, the following actions shall be performed:
- The compliance auditor notes the discrepancy.
- The compliance auditor notifies KEYNECTIS of the discrepancy.
- KEYNECTIS determines with the auditor, at the end of the audit, what further notifications or actions are necessary pursuant to the requirements of this CPS and establish a planning for the implementation of such actions in commercially reasonable period of time,
- KEYNECTIS shall notify Adobe Policy Authority promptly of such necessary actions and associated planning for review and approval.

When all corrective actions are completed, KEYNECTIS shall notify Adobe Policy Authority that the correction plan is completed.

2.11.6 Communication of results
A summary of the Audit Compliance Report including identification of corrective measures taken or being taken by KEYNECTIS and a copy of the compliance certificate is provided to the Adobe Policy Authority.

The overall Compliance Audit Report may be reviewed by the Adobe Policy Authority at KEYNECTIS' facility in accordance with applicable policy for information protection.

2.12 Confidentiality

2.12.1 Types of information to be kept Confidential
The following information shall be considered received and generated confidentially by KEYNECTIS and the CAs concerned, and may not be disclosed except as provided below:

- CA application records, approved or disapproved
- Subscriber agreements and certificate application documents (except for information placed in a certificate or reference archives as defined in this CPS).
- Transaction records (full records and audit logs).
- Certification services audit log records created or retained by KEYNECTIS or a CA
- Certification services audit reports created by KEYNECTIS, a CA, the KEYNECTIS reference archive (to the extents to which these reports are maintained), or the respective auditors (internal or public).
- Emergency planning and disaster recovery plans
- Security measures that control the operation of CA hardware and software and the administration of certification services and designated enrollment services.

Neither CAs nor KEYNECTIS shall disclose or sell applicants' names or other identification information, nor shall they share this information, except in accordance with this CPS. Note, however, that the KEYNECTIS reference archives shall contain certifications, revocations, and other data.

Neither CAs nor KEYNECTIS shall disclose or be required to disclose any confidential information without a prior authentic request from:
- The individual for whom the CA or KEYNECTIS must maintain confidentiality.
- If the information is required by court order.

2.12.2 Types of information not considered confidential
All information located inside the Digital ID is not confidential

2.12.3 Disclosure of certificate revocation/suspension information
No stipulation in this CPS

2.12.4 Release to law enforcement officials
Notwithstanding the foregoing, KEYNECTIS may make such information available to (a) courts, law enforcement agencies or other third parties (including release in response to civil discovery) upon receipt of a court order or subpoena or upon the advice of KEYNECTIS' legal counsel, (b) law enforcement officials and others as may be necessary for the purpose of investigating suspected fraud, misrepresentation, unauthorized access, or potential illegal activity by the Subscriber (as determined by KEYNECTIS), (c) to an acquirer of KEYNECTIS or substantially all of the assets related to any portion of its business, to the extent that such information pertains to the acquired assets or line(s) of business, and (d) to third party service providers and vendors performing functions related to the KEYNECTIS products and services or as otherwise necessary for KEYNECTIS to perform its responsibilities under this Agreement, subject to such third parties' agreement to maintain the confidentiality of personally identifiable Subscriber information.
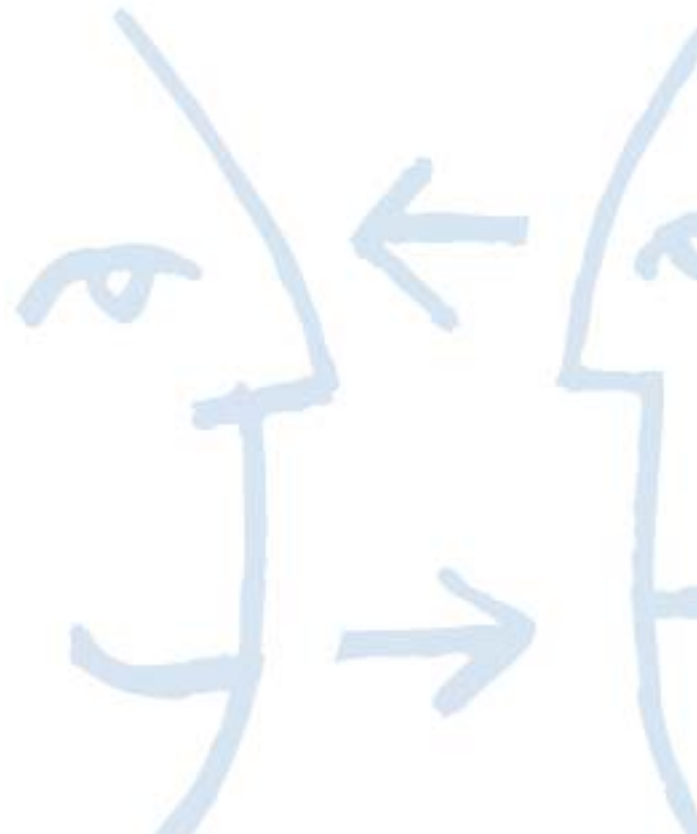
3 IDENTIFICATION AND AUTHENTIFICATION

KEYNECTIS-CDS CA issues Subordinate CA certificates. Each subordinate CA may issue different usages of certificate to different kind of applicants to be used for CDS .

	CDS usage1	CDS Usage2	CDS USAGE3	CDS UH
Applicant is individual in organization	Yes	Yes	No	No
Applicant is organization acquiring certificate on behalf of individual subscriber	Yes	Yes	Yes	No
Applicant is an organization acquiring a certificate on behalf of the Organization	No	Yes	Yes	Yes

The following rules will be applied to all the previously defined applicant and will be enforced by the applications procedures described in Section 4 for each usage of Issued certificates.

3.1 Initial Registration

3.1.1 Name agreement

The subscriber's name appears in the certificate's "Subject" field, under the CN ("Common Name") section. This mention is required.

For individual certificates, it is comprised of the usual first name and last name. This name is that of the subscriber as it appears in Civil Status documents (as Government-supplied).

3.1.2 Need for names to be meaningful

Names used in the certificate must have an association with the entity (person or object) for which they are used.

Information in the "Subject" field of the certificate is meaningful:
- Subscriber's name (CN section)
- Subscriber's email
- Corporate name of the organization represented by the subscriber, as it appears on the company registration certificate.
- The SIREN number of the organization represented by the subscriber, as it appears in the company registration certificate or Identity name (government supplied) .
- The country in which the headquarters of the organization represented by the subscriber is located, as it appears in the company registration certificate and created according to the international naming agreement.

If the client changes any of the information contained in the "subject" field, he/she must inform the CA. The CA will then verify the new identity before reissuance of certificate.

Based on the changes made, the subscriber may be asked to have his or her public key re-certified.

3.1.3 Rules for interpreting various name forms

There is to be no special interpretation of the information contained in certificates' "Subject" field.

3.1.4 Uniqueness of name

All certificates issued by the CA have a unique identity. The RA ensures this uniqueness through the registration process. Any technical contact that requires certificate from the CA must demonstrate that they have the right to use the name in question for identity.

In case of a dispute concerning the use of a name for a certificate, the CA is responsible for resolving the dispute in question.

The uniqueness of a user certificate is established through a serial number within the Certification Authority. The CA shall ensure that the "Subject" field also has a unique character using the subscriber's email, with the exception of certificate renewal or the subject field is reused.

3.1.5 Name claim dispute resolution procedure

The CA will ensure that the names of its subscribers are unique and will be responsible for resolving name claim disputes.

3.1.6 KEYNECTIS' right to investigate violations

KEYNECTIS may (but is not legally obligated) to investigate any violation within the limits permitted by law. By submitting a CA application or certificate application, all applicants accept the undertaking and scope of such investigations and agree to help in determining all facts, circumstances, and other pertinent information that KEYNECTIS deems appropriate and consistent with the CPS, provided that these investigations respect all privacy and data protection laws.

The investigation of a CA may include- but is not necessarily limited to - interviews, review of applicable books, documents and procedures, and inspection of the facilities concerned. An investigation of subscribers or certificate applicants may include but are not necessarily limited to interviews and requests for examination of documents.

3.1.7 Authentication of organization and individual identity

Organization identity

Authentication is the sole responsibility of the Registration Authority, although the KEYNECTIS CDS CA remains responsible to Adobe for the services provided by the RA (per Section 2.2 of this CPS).

The RA will confirm that the organization listed on the certificate application (Name, SIREN) exists and that it has the exclusive right to use its name. This is done by cross-checking the information provided with the information gathered by the RA from the databases of the appropriate official organizations or authorities who can confirm the existence of the organization.

The client's technical contact will submit the certificate application form to the RA. Communications between the technical contact and the RA are protected to ensure the integrity and origin of the transmitted data. It is the RA's responsibility to verify that the information contained in the certificate application is correct and confirm the organization and identity of the technical contact The RA verifies everything needed for authentication through a procedure under the dual control of two people in trusted positions within the RA.

The RA records all of the information used to confirm the client's identity as it is listed on the certificate application, and as applicable, any special attribute, including any reference numbers contained in the documentation used for verifications, and any validity limitations.

Individual identification

The RA confirms during telephone interviews that the RA initaites that the identity of contacts listed on the certificate applications is correct. During these interviews, various client information is verified. These verifications include confirmation of secret information sent by the client with the certificate application (see section 4.3)

In addition, the RA records the steps taken to issue each certificate.

Validation of a legal representative

A certificate application containing either an explicit or implicit affiliation with an organization is only issued after it has been confirmed that the technical contact has the authorization to act on behalf of this organization. If technical contact provides Information (confirmation of employment and authorization from the employer, existence and identity of the cited service, job assignment, etc.), the RA will authenticate this information and/or the legal representative issuing it .

3.1.8 **Unverified Information**

Unverified information is not included in certificates.

3.1.9 **Proof of private key possession**

At the time of the certificate application (standard PKCS#10), the Certification Authority requires applicants to provide proof of possession of the private key corresponding to the public key to be certified.

3.1.9.1 KEYNECTIS-CDS Subordinate CA

CDS Subordinate CAs are required to prove possession of the private key that corresponds to the public key included in their certificate request. This is to be done by using the CDS Subordinate CA's private key to sign a certificate request and providing that request to the Issuing CA. The Issuing CA will validate the signature using the CDS Subordinate CA's public key included in the certificate request. This validation will be processed during a Key Ceremony in the KEYNECTIS Bunker by KEYNECTIS' Security Personnel.

3.1.9.2 Subscriber

Subscribers generating their own private keys must prove possession of that private key by using it to sign a certificate request and providing that request to the Issuing CA. The Issuing CA will validate the signature using the Subscriber's public key.
For Subscribers, Use of Cryptographic Hardware control of CSP process is implemented.
Private keys generated outside the control of Subscribers (CDS USAGE1; CDS USAGE2) are generated through the use of Cryptographic Hardware and delivered to the certificate subject or an authorized representative via a secure and traceable method (see Section 4 Application).

3.2 **Routine Rekey**

Key pairs are periodically renewed in order to minimize cryptographic attacks.

3.2.1 **Rekey of KEYNECTIS–CDS subordinate CA and Time stamping Unit**

KEYNECTIS-CDS Subordinate CAs may use their current signature key to sign a request for rekey. Upon receipt of a valid Rekey Request, the KEYNECTIS-CDS CA will issue a new certificate that includes the new key pair for the KEYNECTIS-CDS Subordinate CA. All such operation are performed during a Key Ceremony

3.2.2 **Rekey of subscribers**

Subscribers may use their current valid signature key to sign a request for rekey in the same usage of certificate. Upon receipt of a valid Rekey Request, the KEYNECTIS-CDS CA that issued the original certificate will issue a new certificate that includes the new key pair for the Subscriber this process is limited to twice (the third times a complete verification procedure applies).

3.3 Rekey after revocation

For KEYNECTIS-CDS Subordinate CAs', Time Stamping units and Subscribers' Certificates that have been revoked, rekey is not be permitted. The KEYNECTIS-CDS subordinate CA, the time stamping unit CA's and Subscriber's identity must be re-established through the existing registration process.

3.4 Revocation request

Revocation requests must be authenticated prior to any action being taken except for CDS USAGE1 which has no revocation process due to the short time life cycle (1 to 5 minutes) nevertheless the CRL is published

When the subscribers are individual, a revocation request is authenticated by presenting a revocation code. This code could be Known by the company representative or subscriber;.

Regarding all other applicants, the RA authenticates revocation requests. The verification procedure requires the same trust level as that of the initial registration in order to ensure that the certified client has really made a revocation request.

Consequently, the RA shall confirm the identities of organizations and individuals requesting a revocation according to the applicable steps of the initial registration.

4 OPERATIONNAL REQUIREMENTS

4.1 Overview of KEYNECTIS role

KEYNECTIS-CDS CA or SUBCA acts as a trusted third party to facilitate the confirmation of the relationship between a public key and a named entity ("naming"). This confirmation is represented by a certificate; in other words, a digitally-signed message issued by a CA.

High-level management of this certification process includes registration, naming, applicant authentication, issuance, revocation, and generation of audit status. Naming is performed primarily by KEYNECTIS, but can also be done by another party. Naming of Certification Authorities follows a registration process that is different from the process used to manage certificates, which determines when certificates are valid and operational.

KEYNECTIS-CDS CA currently offers distinct levels of electronic certification services. Each certificate level, or usage, provides specific security functions and features. Certificate applicants must choose from these different service qualities according to their needs and indicate which certificate usage they would like. Depending on the usage of certificate desired, certificate applicants may send their application to a CA electronically, or they may have to apply in person by contacting a registration authority (RA).

In response to a certificate application and appropriate authentication of the identity of the applicant, a certificate is then issued to the applicant, or a draft of the certificate contents is sent to the applicant. The applicant must review the certificate or draft, determine if it meets his/her needs, and if satisfied, accept the certificate through the certificate registration process. The new subscriber agrees to be bound by the continuing obligations of this CPS.

Certificate management also includes the deactivation of certificates and the decommission of the corresponding private keys through a certificate revocation process. Other CA services may include printing, distributing, publication, storage, and retrieval of certificates according to their particular intended use.

The KEYNECTIS electronic certification services support a variety of security mechanisms to protect communications and information. Certificates alone do not constitute a security mechanism. KEYNECTIS' CERTIFICATION SERVICES provide a framework in which security services may be used by other communicating parties. This framework uses digital signatures and their verification to facilitate the protection of communication and computer-based commerce over open networks; it provides a way for determining whether security services are providing the intended assurances.

Certificate-based security services may be used to counter security threats in a user-defined environment. Users select security mechanisms, security technology, and security service contracts, as well as the electronic certification services that suit the users' anticipated level of risk, in order to protect users' communication environments from compromise.

KEYNECTIS' CERTIFICATION SERVICES currently use the RSA public key system for all certification needs. However, KEYNECTIS is committed to supporting other digital signature standards when the market demands alternative solutions.

The application process for subscriber and Subordinate CA in the CDS PKI has been approved by the Adobe Policy Authority and includes completing and submitting an application and agreeing to any required Subscriber Agreement.

4.2 Classification of certificate

As part of the framework of its certification services, KEYNECTIS currently supports 5 distinct certificate types issued under the KEYNECTIS-CDS CA or SUBCA..

4.2.1 CDS USAGE1 certificates

Usage1 certificates are issued only to individuals through the K.Websign® service. Usage1 certificates confirm that the name of a user or his/her alias and/or email address form a subject. Usage 1 certificates are generated by a specific application named K.Websign® which is performing the operational RA function on behalf an Organization which name will be in the certificate (OU). The certificate has a short time life duration and is used for only one approval signature or cosignature to a CDS document previously signed by a CDS usage3 Digital ID of the Organization. K;websign application checks, at time of application request for USAGE1, the signature validity of the CDS document received from the RA Certificate will be set in the KEYNECTIS repository and will be available in the archive of the file Proof in the external Archival facility in conformity with the proof management policy document (PGP) referenced OID (1.3.6.1.4.1.22234.2.4.6.1.2). The reference of the electronic PROOF is unique and will stays in the DN part of the CDS Usage1 (OU).
Organization acts as RA for CDS Usage 1 certificates and accepts full responsibility of identification and Authentication of the final subscriber as a RA in conformity with this CPS and specific contract describing obligation and responsibility in use of the K.Websign application.

CDS usage1 Key pair generation is performed by KEYNECTIS Operation Trust Center, using HSM FIPS 140 level 2 or higher.

CDS Usage 1 Certificates may significantly ensure the applicant's identity based on a process that checks the requestor's name, email address and other information provided to the Organization acting as RA. They are solely used for Approval Electronic signature of previously Signed (with usage3 certificate) CDS PDF document between the Organization and the applicant.

4.2.2 CDS Usage 2 Certificates

Usage 2 certificates are issued to individuals in an organization and to an organization's representative. Usage2 certificates verify that information provided by the applicant is consistent with information available in

declared <u>databases</u> like Organization's Human resources or Organization's customer database (i.e Bank), database recognized by government approved association etc.). Any validation database must be referenced in the subscriber agreement. Usage2 Certificates are used by KEYNECTIS customers exclusively for CDS purposes and strong authentication.

After submitting a Usage2 Certificate application online to a registration authority (KEYNECTIS RA or ORGANIZATION RA), the certificate applicant's registration information is checked against third-party databases (KEYNECTIS-RA) or internal database (ORGANIZATION RA). Based on this information, the RA will either approve or reject the request. When Organization RA is implemented, electronic document (Approval or rejection) signed with CDS Usage 2 certificate must be used by the RA and archived during the procedure.

CDS usage2 Certificate for French PRIS V1 or PRIS V2 certificate owner.
French government program for signature named PRIS has described rules for specific certificate Issuance. Usage2 Applicant, owner of a valid certificate issued by a French government accredited CA (Following PRIS V1 or PRIS V2 regulation) can request CDS usage2 certificate. Such application will follow a verification procedure based on the accredited PRIS certificate usage and hardware compliance.

Usage 2 Certificates may significantly ensure the applicant's identity based on a process that checks the requestor's name, address, and other information provided in the certificate application by comparing it to information in referenced databases. Direct phone calls are also made by KEYNECTIS RA to confirm the applicant's identity, company, etc. Confirmation is based on KEYNECTIS matching criteria of third-party databases against the information in the application.

CDS usage2 certificate key pair generation is performed on HSM FIPS 140 level 2 or higher..

Although KEYNECTIS uses an advanced authentication method to verify and validate the certificate applicant's identity for a Usage 2 Certificate, it does not require the applicant's personal appearance in front of a trust authority (such as an RA). Consequently, the decision to obtain, use or rely on a Usage 2 certificate should take into account its advantages and limitations, and the certificate should be used accordingly.

4.2.3 CDS Usage 3 Certificates

Usage 3 Certificates are issued through different procedures in order to prove the identity of the individual applicant or Organization in a probative manner.
Usage 3 organization certificates are issued to organizations. These certificates significantly guarantee the identity of individual applicants or a legal representative.

Usage 3 individual <u>certificate type</u> is known as the "Usage 3 <u>administrator</u> certificate (registration authority)."
It is only issued to <u>authorized, permanent, and salaried</u> of organization and approved by an legally recognized person of the <u>organization</u> to perform authorized RA administrator functions. This RA administrator must be authorized by KEYNECTIS RA through a physical appearance before the administrator certificate can be approved. The private key <u>corresponding</u> to the public key contained in a Usage 3 administrator certificate must be generated and stored in a secure manner in an external cryptographic device certified to FIPS 140-1 level 2 at the least. After issuance of the certificate the organization's RA can use this certificate to sign a PDF Application form for Individual requests for its organization.
Usage 3 Organization certificate type is the USAGE 3 signing server certificate issued to an organization through a multi-parts validation process including:
    -Signed documents,
    -Phone communication with the business organization.
    -Confirmation of its related information through legal document.
The private key must be installed in a secure HSM of FIPS 140-1 level 2 or higher.

Usage3 certificates require the Applicant's (individual or organization representative) Appearance

4.2.4 Time stamp Certificate

KEYNECTIS issues time stamping certificates only to its own organization through the level 1 "KEYNECTIS CDS CA". Those certificates are only issued for KEYNECTIS Time Stamping services hosted in the KEYNECTIS Trust CENTER or a specific Audited Facility center working under delegation to the KEYNECTIS Time Stamp services.

The Time Stamp Certificate uses different procedures during a KEY Ceremony in order to prove the identity of the organization applicant in a probative manner including a Face-to-face communication with the business organization and the confirmation of its related information through third-parties to provide additional reasons for trust.

Time stamp certificate key pair generation is performed on an HSM certified to FIPS 140 level 2 or higher

4.2.5   Sub-CA Certificate

KEYNECTIS issues Sub-CA certificates to organizations. Those certificates are only issued in order to be operated under control of KEYNECTIS Operation inside KEYNECTIS facilities in the Highly Secured KEYNECTIS BUNKER.
Sub-CA certificate key pair generation is performed on an HSM certified to FIPS 140 level 3 (EAL4+) located in the Key Ceremony room (see chapter 7).

4.2.6   Test Certificate

KEYNECTIS may issue test certificates for authorized testing purposes only. Test certificates include specific OID (used by Adobe CDS platform to generate warning message) and in the subject specific information regarding test usage and purpose as well as in the certificate Policies information. Only authorized individuals may use test certificates.

4.3   Validation principles and Certificate CDS Usage Properties

4.3.1   Validation process principle

Upon receipt of certificate applications, CAs shall perform all required validations before issuing certificates. The CA shall establish that:

▪ The certificate applicant is the person identified in the application (in agreement with and within the limits of the certificate usage description).
▪ The certificate applicant has the right to hold the private key corresponding to the public key listed on the certificate.
▪ The information to be listed on the certificate (except for unverified applicant information) is correct;
▪ Any organization that requests a certificate listing the public key of the certificate applicant (permitted for Usage 2 and 3 certificates) is duly authorized to make this request.

Once the certificate is issued, the CA is no longer obligated to monitor or check the accuracy of certificate information, unless the CA is notified of the certificate's violation, in accordance with the CPS.

Subject to the provisions of sections 8.1 & 8.3 herein, KEYNECTIS reserves the right to update its validation procedures in order to improve the validation process. Updated validation procedures may be obtained from KEYNECTIS, 11 13 rue René Jacques 92131 Issy les Moulineaux Cedex France.

4.3.2   CDS Certificate usage properties

Table below describes certain characteristics of each certificate usage.

	Overview of identity confirmation	CA private key protection	Applicant private key protection	Applications implemented or contemplated by users
CDS Usage 1	Automated, unambiguous name and email address search	CA: trustworthy hardware (HSM)	HSM located in the KEYNECTIS Trust Center security level 5.	K.WebSign® application to cosign CDS Document previously signed with supported platforms.
CDS Usage 2	• Unambiguous name, contact, and email address search; Email documents or business records for organizations, SIREN no, company registration certificate, etc. • Confirmation of registration information by phone call or PrisV1 or PrisV2 certificate check.	CA: trustworthy hardware (HSM)	Cryptographic hardware required Fips 140-1 level 2	CDS Signing using supported platforms.
CDS Usage 3	• Unambiguous search for names, contacts, physical addresses and email documents or business records for organizations, SIREN no, company registration certificate, etc. • Confirmation of registration information by phone call. • Face to Face issuance.	CA: trustworthy hardware (HSM)	Cryptographic hardware required. FIPS certified to 140-1 level2 or higher	CDS Signing using supported platform Services of electronic signature by servers using supported platforms etc.
CDS UH	• KEYNECTIS key ceremony	CA: trustworthy hardware (HSM)	Cryptographic hardware required. FIPS 140-1 level 2	KEYNECTIS K.Stamp® Application

4.3.3 Third-party confirmation of company information

Where required (Usage2 and Usage3 certificates) a third-party designed in the subscribers' agreement confirms the company's name, address, and other contact information by comparing it with its database and consulting the appropriate official organizations. Confirmation of information about companies and banks require certain customized (and possible localized) procedures focusing on legal criteria (such as proof of business registration). The third-party also provides telephone numbers used for out of band communications with the company to confirm certain information (for example, to confirm an agent's position in the company or that the person listed on the application is indeed the applicant). If the database does not contain all of the information required, the third-party may conduct an investigation upon request by the CA, or the certificate applicant may be asked to provide additional information and proof.

4.3.4   Postal address confirmation

Once Usage 2 certificates are issued, the CA must send a confirmation letter (by mail with acknowledgement of receipt performed through postal organization) to the postal address indicated on the certificate application and confirmed through third-party databases. This confirmation procedure provides additional proof that the applicant is who he or she claims to be and that the address listed on the certificate application is correct. When localized in France the French Postal named "lettre recommandée avec accusé reception" grants the identity and organization.

4.3.5   French PRIS V1 or PRIS V2 certificate owner confirmation

During validation process for CDS Usage 2 certificate, a simplified procedure for a third party verification identity is based on the check of electronic signature of a document with such certificate.

4.4   Application requirement for CDS USAGE 1 Certificate

4.4.1   Enrolment of organization

Before Issuance of CDS Usage 1 certificate, organization in charge of the identification of the applicant must be the owner of a Usage3 certificate for that organization and under K.WebSign licence contract. Organization fulfils the RA function in the CDS Usage 1 certificate issuance model.

4.4.2   Registration of Applicants

Organization is in charge of determining and verifying information required to generate the content of the DN. All information must be complete and will be transmitted using Signed and encrypted data, providing a way to KEYNECTIS-CDS CA OR SUBCA to verify the identity of organization and integrity of information.

4.4.3   Certification Information

See section 7

4.4.4   Procedure for Processing Certificate Applications

KEYNECTIS K.WebSign platform receives online applicant's information from Organization together with a PDF CDS document. K.websign platform verifies
- Completeness and integrity of request
- The CDS signature validity of the document

The K.WebSign platform then generates key pair inside the High secured operation bunker through a Cryptographic device certified to FIPS 140-1 level 2 t, builds a CSR including DN with a unique reference of the received CDS Document (TransNUM) and sends it to the KEYNECTIS CDS CA using XML signed and encrypted data.

4.5   Issuance of Certificate CDS USAGE 1

KEYNECTIS-CDS CA at the time of reception of the application from K.WebSign platform, issues a CDS Certificate Usage1 which includes unique information (identity and TransNum) in the DN.

4.6   Acceptance of Certificate CDS USAGE 1

Once the applicant receives and approve the CDS Usage, the K.WebSign platform will add an approval signature to the CDS Document and archive it for at least 3 years at least.

4.7 Suspension and Revocation of Certificate CDS USAGE 1

Because of the short lifecycle of the CDS Usage1 Certificate, no revocation process is stipulated.

4.7.1 Circumstances for revocation
No stipulation

4.7.2 Who can request a revocation
No stipulation

4.7.3 Procedure for Revocation request
No stipulation

4.7.4 Revocation request grace period
No stipulation

4.7.5 Circumstances for suspension
No stipulation

4.7.6 Who can request a suspension
No stipulation

4.7.7 Procedure for suspension request
No stipulation

4.7.8 Limits on suspension Period
No stipulation

4.7.9 CRL Issuance Frequency
In order to permit any relying party to verify certificate validity, a CRL publication is performed every day with a 7 day period of validity.

4.7.10 ARL/CRL Checking requirement
Relying parties must retrieve ARL/CRLs at least once every 24 hours before relying on a document signed using a CDS digital ID except for CDS digital IDs issued for the purpose of time-stamping services.

4.7.11 Online revocation Status checking availability
OCSP provides a method to obtain timely information about a CDS Certificate's revocation status when on-line signing and/or validation is performed via certain Adobe products. OCSP requests contain the following data:
- Protocol Version
- Service Request
- Target Certificate Identifier

If a CDS Certificate contains an OCSP extension, then certain Adobe products may make an OCSP request using the OID: 1.2.840.113583.1.1.9.2 that resides in the CDS Certificate.

4.7.12 Online revocation checking requirements
The definitive OCSP responses message includes the following
- Version of the response syntax
- Name of the responder
- Responses for each of the certificates in a request
- Signature computed across hash of the response

The address of the OCSP responder is URL = http://k-valid.keynectis.com/ds-server/process. The Certificate used to sign the OCSP response is issued by the KEYNECTIS-CDS CA or subordinate CA .

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

4.7.13   Other forms of revocation Advertisements Available
No stipulations

4.7.14   Checking requirements for other forms of revocation advertisements
No stipulations

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

4.8   Application requirement for CDS USAGE 2 Certificate

The following process is applicable to applicants requesting CDS Usage2 certificates for use in their roles on behalf of the organization either on an individual basis or in connection with a function.

4.8.1   Enrolment of individual in organization

Before any applicant in affiliation with an organization can request a CDS certificate the Organization must enroll in a CDS Service contract.The Organization Representative, on behalf of the Organization, shall complete a KEYNECTIS CDS enrolment form in a format prescribed by KEYNECTIS. All enrolment forms are subject to review, approval and acceptance by KEYNECTIS.

The KEYNECTIS-CDS customer services perform the following verifications:
▪ Establish the identity of the organization (Commercial contract signed in face to face)
▪ Confirm the right of the future RA to represent the company through the issuance of Usage3 certificate with physical appearance of the RA Administrator.

4.8.2   Registration of applicants in organization

Applicants to an individual Certificate in the organization shall complete a KEYNECTIS Form which will be validated by Authorized Organization RA through its PDF format transformation.
The designated RA (Owner of a CDS Usage 3 certificate) on behalf the organization will perform the verification steps inside the organization to validate the authority of the Applicant to request a CDS Certificate or verify accuracy of the information contained in the Applicant's CDS Certificate request or otherwise check for errors and omissions. Designated RA then performs a signed CDS of the application and uploads it to KEYNECTIS.
Tracking of application certificate must be done using CDS signed document by the RA.

4.8.3   Enrolment of individual in small organization (Individual)

The information to be provided is that which is sent in the certificate application file. A small organization is a self-employed organization structure and verification process can be based on governmental information available in "French registre du commerce" database.

A certificate application is done in three steps:
▪ Step 1: The applicant sends the certificate application file and postmail Government identity document below.
▪ Step 2: The documents and application file that are received, are validated by KEYNECTIS-CDS RA
▪ Step 3: The subscriber retrieves the certificate

The KEYNECTIS-CDS RA shall process certificate applications only if they are in a certificate application file with all of the credentials described below:

Document 1: Signed Letter from the organization's representative. This refers to the written (and signed) request from the legal representative. This letter designates the individual to whom the certificate shall be issued. The letter must include the following:
▪ Co-signature of acceptance from the recipient individual (applicant)
▪ A revocation code (comprised of an alphanumeric chain) known by the company representative so that he/she can revoke the applicant's certificate when the mandate is no longer in effect for whatever reason.
▪ Email address of the customer to inform of the certificate's revocation.

Document 2: Company registration certificate. The original certificate is to be provided, dated within less than three months, and must include the company's SIREN number and address.

Document 3: One form of identity for the authorized applicant. The authorized individual's identity credentials must be certified copies in compliance with French or European regulations on the certified Copy process. In France standard certified copies of two out of the four possible forms of identity may be selected: registration certificate, standard certified photocopy of the national identity card, standard certified photocopy of a passport,driving license. Certified Copy are performed in French government location (Police department, cityHall etc..)

Document 4: Letter from the authorized applicant. The letter from the authorized individual must contain the following information:
▪ Work phone number
▪ Cell phone number (personal or business)
▪ Personal code for withdrawal and revocation (hereinafter called the revocation and withdrawal code).
▪ Email address
▪ Declaration accepting the CA's general sales conditions and stated obligations.

Document 5: Purchase order and payment method. This is from the applicant'sorganization for the issuance of one or more certificates, and states the desired payment method (a completed and signed check is included if needed).

The KEYNECTIS-CDS RA shall perform the following verifications:
▪ Establish the identity of the future subscriber (based on document 3 validation)
▪ Confirm the right of the future subscriber to represent the company.(based on document 1)
▪ Confirm the relationship between the public key to be certified and the future subscriber (technical control of CSR)
▪ Ensure that the future subscriber has been informed of the terms and conditions for certificate use (Phone Call to the applicants and legal representative).

4.8.4 Registration of Applicants

KEYNECTIS- CDS RA performs the authentication steps listed below (and checks generally for errors and omissions relevant to the authentication steps).

KEYNECTIS will not include an Individual Name in a CDS Certificate for a small company without first ensuring the individual's name, country and locality provided on the enrolment form matches that which is shown on the Identification and second ensuring the validity of the identification of the small organization.

In order to avoid errors and fraudulent issuance of certificates, the process is based on the principle of "separate tasks". The individual who verifies organization identity document may not verify applicants' identity through the phone call and vice-versa.

The process works through a "buddy system" (person no. 1 / person no. 2) in which tasks shall be broken down as follows:
▪ Validation of purchase order receipt and fulfillment of the form (person N°.1)
▪ Verification of the existence of the company and its contact information (person N°.1).
▪ Verification of the phone number (Person N° 2)

For the organization's name, the objective is to verify that:
▪ The organization actually exists (see its SIREN no. or DUNS for overseas companies).

For French companies, the organization's name can be verified on official sites such as www.dnb.com.

If reference sites show during verification that the SIREN No. (DUNS N° for companies outside of France) corresponds to the O (Organization) listed on the application, customer service may validate this step and continue verification.

If the SIREN N°. or DUNS does not correspond to the organization, customer service must ask the client to provide what is called the "Proof of Right Document" – an official document proving the existence of the company (ex: company registration certificate, official journal, etc.).

It is imperative that this document include:
▪ The organization's name
▪ Its official brand (stamp, logo, etc.)
▪ Its company number (or registration number)
▪ The name of the department where the document was issued.
▪ The signature of the agent from the department that issued the document.

The telephone verification procedure ensures the following points:
▪ The Individual indeed works for the company that made the request.
▪ He/she knows about the request.
▪ He/she confirms email addresses.
▪ He/she is authorized to request a certificate, receive it, and install it.

The telephone number may be verified on official sites (French operator and public Phone book for wired phone) or through telephone information.

When the telephone number entered is a cell phone number: the applicant contact must provide legal proof that there is an association between this individual and the organization in document 1 co-signed by the organization representative).
During the telephone call, customer service asks a certain number of questions to validate the merits of the request made online:

▪ If customer service obtains all of the answers, it validates this verification step and issues the certificate.
▪ If some of the information is missing, customers must correct their request.

Applicant already owns a PrisV1 or PrisV2 certificate
The French government has already accredited and referenced CAs for the issuance of certificates following the PrisV1 or PrisV2 protocols. If the applicant is an owner of such a certificate, he/she will have a simplified verification process based on the validation of the certificate used at the time of the application request transmission. In such case the CN of the CDS certificate will be the same as the PrisV1 or PrisV2 CN.

4.8.5   Certification Information
See section 7

4.8.6   Procedure for Processing Certificate Applications

Applicant connects at the Public KEYNECTIS-CDS Web site and completes a form for the application request. The Applicant and owner of PRISV1 and PRISV2 will have the validity of their certificate performed during this application request during a dual time separated check (CRL refresh control)

KEYNECTIS-CDS RAs or Organization's RA are notified of the request and process the Validation steps described in previous §.

KEYNECTIS–CDS RA or Organization's RA connects on an administrator site using an individual certificate under a different KEYNECTIS CA (Access and role check) and is able to accept or reject the application request if it does not match with the verification process. At the end of the validation an email is sent to the applicant for certificate delivery.

4.9 Issuance of Certificate CDS USAGE 2

If KEYNECTIS or Organization's RA finds that the Applicant's CDS Certificate enrolment form was verified, then the Applicant's Certificate will be signed by KEYNECTIS-CDS SUBCA. KEYNECTIS shall deliver the CDS Certificate by invoking the Applicant's web browser to generate a Public and Private Key Pair onto an Approved Hardware Device by limiting the available Cryptographic Service Provider ("CSP") drivers that enable an Applicant to generate a Key Pair.

The Public Key material will be sent to KEYNECTIS for signing and the Applicant's CDS Certificate will be signed by KEYNECTIS and delivered back to the Applicant. The Applicant may utilize his/her own Approved cryptographic Device certified to Fips140-1 level2 or, if the Applicant does not already have one, the Applicant may purchase one from KEYNECTIS. If the Applicant, or Organization on behalf of the Applicant, purchases an Approved Hardware Device from KEYNECTIS then the Applicant shall have the option of requesting KEYNECTIS to generate a Public and Private Key Pair onto the Approved Hardware Device at KEYNECTIS' facilities and deliver the Approved Hardware Device containing the Certificate to Subscriber. In such case, the Approved Hardware Device shall be delivered to the Subscriber by Post mail or other delivery service or by courier or other in-person delivery and may require signature for delivery. KEYNECTIS shall obtain and keep all receipts for delivery. In certain circumstances the delivery may include a KEYNECTIS customer service representative telephone number and e-mail address for any technical or customer service problems. KEYNECTIS, in its sole discretion, may provide such technical or customer support to the Applicants/Subscribers.

4.10 Acceptance of Certificate CDS USAGE 2

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

4.11 Suspension and Revocation of Certificate CDS USAGE 2

This revocation process describes the premature End of the Operational Period of a CDS Certificate.

4.11.1 Circumstances for revocation

A CDS USAGE2 certificate must be revoked, and the serial number placed on a list of revoked certificates (CRL), if one of the following circumstances is identified:
▪ Information about the subscriber listed on his/her certificate changes before the certificate's "normal" expiration.
▪ Failure to follow the certificate's rules of use
▪ The subscriber's private key is suspected of being compromised, lost, or stolen.
▪ The Organization makes the request using the revocation code.
▪ The CA's certificate is revoked (which leads to the revocation of all of the certificates signed by the corresponding private key).
▪ The organization's activity is discontinued.

4.11.2 Who Can request a revocation
The only parties permitted to request revocation of or revoke a CDS Certificate issued by KEYNECTIS are:
-    Organization representative
-    Registration Authority
-    KEYNECTIS and the ADOBE Policy Authority.

4.11.3 Procedure for Revocation request
Organization representative initiates the revocation request:
-    By using the revocation code chosen at time of enrolment or

- By contacting the KEYNECTIS-CDS RA, either by e-mail, a national/regional postal service, facsimile, or overnight courier, to request revocation of a CDS Certificate and must identify the reason for the request.

Upon receipt of a revocation request, KEYNECTIS to notify the Organization Representative of the request by e-mail. KEYNECTIS will seek confirmation of the request by e-mail to the Subscriber. The message will state that KEYNECTIS will revoke the CDS Certificate and that posting the revocation to the appropriate CRL will constitute notice to the Subscriber and Relying Parties that the CDS Certificate has been revoked. Notification will not be sent to anyone other than the Subscriber.

4.11.4 Revocation request grace period
There is no grace period available to the Subscriber prior to revocation, and KEYNECTIS shall revoke such CDS Certificate within the next business day and post the revocation to the next published CRL.

4.11.5 Circumstances for suspension
There is no suspension

4.11.6 Who can request a suspension
No stipulation

4.11.7 Procedure for suspension request
No stipulation

4.11.8 Limits on suspension Period
No stipulation

4.11.9 CRL Issuance Frequency
CRL publication is performed every day with a 7 day period of validity

4.11.10 ARL/CRL Checking requirement
Relying parties must retrieve ARL/CRLs at least once every 24 hours before relying on a document signed using a CDS digital ID except for CDS digital IDs issued for the purpose of time-stamping services.

4.11.11 Online revocation Status checking availability
OCSP provides a method to obtain timely information about a CDS Certificate's revocation status when on-line signing and/or validation is performed via certain Adobe products. OCSP requests contain the following data:
- Protocol Version
- Service Request
- Target Certificate Identifier

If a CDS Certificate contains an OCSP extension, then certain Adobe products may make an OCSP request using the OID: 1.2.840.113583.1.1.9.2 that resides in the CDS Certificate.

4.11.12 Online revocation checking requirements
The definitive OCSP responses message includes the following
- Version of the response syntax
- Name of the responder
- Responses for each of the certificates in a request
- Signature computed across hash of the response

The address of the OCSP responder is URL = http://k-valid.keynectis.com/ds-server/process. The Certificate used to sign the OCSP response is issued by the KEYNECTIS-CDS SubCA.

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

4.11.13 Other forms of revocation Advertisements Available
No stipulations

4.11.14 Checking requirements for other forms of revocation advertisements
No stipulations

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

4.12 Application requirement for CDS USAGE 3 Certificate

CDS Usage 3 certificate are issued when the applicants is an organization acquiring and managing a digital ID on behalf of an individual Subscriber (in the name of the individual with a RA role) and on behalf of the organization itself in order to use it on a server. The CDS USAGE3 certificate are delivered in a face to face processus between KEYNECTIS RA and organization.

4.12.1 Enrolment
Organization representative brings all identity documents to KEYNECTIS RA which verify near Registrer of commerce and/or dun and Bradstreet Database validity of the Organization Identity. The Organization representative, on behalf of the organisation, will complete a KEYNECTIS CDS Certificate Enrolment form in a format prescribed by KEYNECTIS. All enrolment forms are subject to review, approval and acceptance by KEYNECTIS. Enrolment forms include the reference of the cryptographic Hardware module in use for the key pair generation.

4.12.2 Registration of Applicants

KEYNECTIS will first request the following credential described below:

Document 1: Letter from the Organization. This refers to the written (and signed) request from the subscriber. This letter designates the individual to whom the certificate (RA or technical contact for server) shall be issued. The letter must include the following:
- Co-signature of acceptance from the recipient individual (future subscriber)
- A revocation code (comprised of an alphanumeric chain) known by the company representative so that he/she can revoke the applicant's certificate when the mandate is no longer in effect for whatever reason.
- Email address of the customer if they would like to be informed of the certificate's revocation.

Document 2: Company registration certificate. The original certificate is to be provided, dated within less than three months, and must include the company's SIREN number and address.

Document 3: Letter of Authorization for RA registration certificate. The LOA is signed by the Organization representative and includes the following: RA Names and title or technical contact name (Server), and a statement that the applicant listed are members of the organization and are authorized to request a CDS Certificate for RA or server purpose.

Document 4: Letter from the applicant RA (or Technical contact). The letter from the individual must contain the following information:
- Work phone number
- Cell phone number (personal or business)
- Personal code for withdrawal and revocation (hereinafter called the revocation and withdrawal code).
- Email address
- Declaration accepting the CA's general sales conditions and stated obligations.

Document 5: Purchase order and payment method. This is from the company for the issuance of one or more certificates, and states the desired payment method (a completed and signed check is included if needed).

The KEYNECTIS RA shall perform the following verifications:

- Establish the identity of the future subscriber and organization.
- Confirm the right of the future subscriber to represent the company.
- Confirm the relationship between the public key to be certified and the future subscriber.
- Ensure that the future subscriber has been informed of the terms and conditions for certificate use.

4.12.3 Registration procedure for CDS Usage3 certificates

The following information must be included in the CDS Usage 3 certificate application:

- Personal identification of the technical contact: Last name, first name, email, position, complete mailing address, telephone numbers (standard and direct line).
- Organization identification: Name, first names and legal status, as well as any other information useful for registration (for example, company's SIREN no.).
- PKCS#10-standard public key.
- Validity period for the certificate
- "Secret" customer information for the authentication process during identity verification (question/answer pair is provided).

Before issuance of RA or server Certificate and inclusion of Organization Name in a CDS Certificate for Organization, KEYNECTIS first ensures the validity of the identification of the Organization.

In order to avoid errors and fraudulent issuance of certificates, the process is based on the principle of "separate tasks". The individual who authenticates may not verify and vice-versa.

The process works through a "buddy system" (person no. 1 / person no. 2) in which tasks shall be broken down as follows:
- Validation of purchase order receipt and fulfillment of the form (person N°.1)
- Verification of the existence of the company and its contact information (person N°.1).
- Verification of the phone number of(RA or server Applicant) (Person N° 2)

For the Hardware cryptographic module the verification is based on the compliance of the Module to FIPS 140-1 level 2.

For the organization's name, the objective is to verify that:
The organization actually exists (see its SIREN no. or DUNS for overseas companies).

For French companies, the organization's name can be verified on official sites such as www.dnb.com.

If reference sites show during verification that the SIREN No. (or DUNS for companies outside of France) corresponds to the O (Organization) listed on the application, customer service may validate this step and continue verification.

If the SIREN N°. or DUNS does not correspond to the organization, customer service must ask the client to provide what is called the "Proof of Right Document" – an official document proving the existence of the company (ex: company registration certificate, official journal, etc.).

It is imperative that this document include:
- The organization's name
- Its official brand (stamp, logo, etc.)
- Its company number (or registration number)
- The name of the department where the document was issued.
- The signature of the agent from the department that issued the document.

- The face to face verification ensures the proof of identity of the Applicant or technical contact.

4.12.4 Export controls confirmation

In addition to other verifications performed for Usage 3 certificates, KEYNECTIS shall perform the following checks prior to issuing export control certificates for installation on a server.

KEYNECTIS shall require the certificate applicant to identify the country in which the server will be installed. This information provided by the applicant through the subscriber agreement shall be a guarantee that the server shall be installed in the country indicated.

If the certificate applicant guarantees that the server shall be installed in France, KEYNECTIS shall confirm that the "Country" field on the certificate applications contains the "FR" value (ISO standard). KEYNECTIS shall confirm that information obtained from a third-party database indicates that the entity indicated in the "Contact Information" field is located in EEC. KEYNECTIS shall verify that the activity code contained on the certificate application identifies the certificate applicant as a bank, financial institution, insurance company, or medical/health organization. If this is not the case, the certificate applicant shall provide the credentials authorizing it to perform the activities of a bank, financial institution, financial company, or medical/health organization.

4.12.5 Certification Information
See section 7

4.12.6 Procedure for Processing Certificate Applications
Applicant connects to the Public KEYNECTIS-CDS Web site and completes a form for the application request (A revocation code can be chosen at this moment) .. If the request is for an organization Server the CSR (PKCS#10) will be transmitted at the same time with information regarding the Hardware module used and its Compliance with FIPS 140-1 level 2 or higher
KEYNECTIS-CDS RAs are notified of the request and process the Validation steps described in previous §.

KEYNECTIS–CDS RA connects to an administrator site using an individual certificate issued by specific KEYNECTIS CA (Access and role check) and is able to accept or reject the application request if it does not match with the verification process. At the end of the validation an email is sent to the applicant for delivery in face to face operation.

4.13 Issuance of Certificate CDS USAGE 3
If KEYNECTIS finds that the Applicant's CDS Certificate enrolment form was verified, then the Applicant's Certificate will be signed by KEYNECTIS-CDS SUBCA. KEYNECTIS shall deliver the CDS Certificate:
- by invoking the Applicant's web browser to generate a Public and Private Key Pair onto an Approved Hardware Device by limiting the available Cryptographic Service Provider ("CSP") drivers that enable an Applicant to generate a Key Pair.
- By copying a CSR (PKCS#10) containing the Public Key.

The issuance is realized in a face to face procedure with the applicant AR or Technical control in presence of KEYNECTIS Personnel (Geographic localisation can be applicant site or KEYNECTIS site).

4.14 Acceptance of Certificate CDS USAGE 3
The Applicant expressly indicates acceptance of a CDS Certificate by using such CDS Certificate and signing the subscriber' agreement.

4.15 Suspension and Revocation of Certificate CDS USAGE 3

The revocation process describes the premature End of the Operational Period of a CDS Certificate.

4.15.1 Circumstances for revocation

A CDS USAGE 3 certificate must be revoked, and the serial number placed on a list of revoked certificates (CRL), if one of the following circumstances is identified:

- Information about the subscriber listed on his/her certificate changes before the certificate's "normal" expiration.
- Failure to follow the certificate's rules of use
- The subscriber's private key is suspected of being compromised, lost, or stolen.
- The subscriber makes the request himself.
- The CA's certificate is revoked (which leads to the revocation of all of the certificates signed by the corresponding private key).
- The organization's activity is discontinued.
- Requested change in the length of the key or algorithm (signature and/or hashing) recommended by an appropriate international or national organization.
- Change in the organization's name and the technical contact is no longer authorized to use the domain name.
- The DN included in the certificate is wrong.
- The technical contact used an inaccurate DN in the initial request.
- End of the relationship between the CA and client.

4.15.2 Who Can request a revocation
The only parties permitted to request revocation of or revoke a CDS Certificate issued by KEYNECTIS are:
- Organization representative
- Technical contact
- Registration Authority
- KEYNECTIS and the ADOBE Policy Authority.

4.15.3 Procedure and processing of online certificate revocation request

Online service is available to the subscriber 24/7 in order to revoke certificates as quickly as possible. Subscribers connect to the CA's site and may revoke their certificate by entering their email and withdrawal and revocation code, which was sent to the CA when they signed a Revocation. Requests must contain identification information about the certificate and its owner.

4.15.4 Procedure and processing of offline certificate revocation request

Offline service is available to subscribers or their representatives, from 9:00 a.m. to 5:00 p.m. during the business week. Certificates are revoked with the subscriber's withdrawal and revocation code, or the representative's revocation code.

The technical contact or RA sends a revocation request to the KEYNECTIS-CDS RA with the following information at least:
- His/her personal identification.
- "Secret" information that he/she sent when applying for the certificate for which he/she is requesting revocation.

The KEYNECTIS-CDS RA authenticates the authorized revocation request and sends it to the CA. The CA authenticates the RA and revokes the certificate by activating its private signature key.

Information from the RA is sent to the CA by a secure line for protection. All of the certificate revocation operations are protected in a way to guarantee the integrity, confidentiality (if needed), and the origin of the data that is sent and processed.

The technical contact is notified of the change in the validity status of his/her certificate. Once revoked, a certificate is not recertified.

4.15.5 Revocation request grace period
There is no grace period available to the Subscriber prior to revocation, and KEYNECTIS shall revoke such CDS Certificate within the next business day and post the revocation to the next published CRL.

4.15.6 Circumstances for suspension
There is no suspension

4.15.7 Who can request a suspension
No stipulation

4.15.8 Procedure for suspension request
No stipulation

4.15.9 Limits on suspension Period
No stipulation

4.15.10 CRL Issuance Frequency
CRL publication is performed every day with a 7 day period of validity

4.15.11 ARL/CRL Checking requirement
Relying parties must retrieve ARL/CRLs at least once every 24 hours before relying on a document signed using a CDS digital ID except for CDS digital IDs issued for the purpose of time-stamping services.

4.15.12 Online revocation Status checking availability
OCSP provides a method to obtain timely information about a CDS Certificate's revocation status when on-line signing and/or validation is performed via certain Adobe products. OCSP requests contain the following data:
-   Protocol Version
-   Service Request
-   Target Certificate Identifier
If a CDS Certificate contains an OCSP extension, then certain Adobe products may make an OCSP request using the OID: 1.2.840.113583.1.1.9.2 that resides in the CDS Certificate.

4.15.13 Online revocation checking requirements
The definitive OCSP responses message includes the following
-   Version of the response syntax
-   Name of the responder
-   Responses for each of the certificates in a request
-   Signature computed across hash of the response
The address of the OCSP responder is URL = http://k-valid.keynectis.com/ds-server/process. The Certificate used to sign the OCSP response is issued by the KEYNECTIS-CDS SubCA.

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

4.15.14 Other forms of revocation Advertisements Available
No stipulations

4.15.15 Checking requirements for other forms of revocation advertisements
No stipulations

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

4.16 Application requirement for CDS UH and CDS Sub-CA Certificates

CDS UH (Unite d'Horodatage) and Sub-CA certificates are issued during a KEY Ceremony inside KEYNECTIS' Bunker.

4.16.1 Enrolment of organization
Same as for CA creation using:
- naming document,
- script of ceremony,
- Physical witness and secret share holder authentication
- Legal notarization

4.16.2 Registration of Applicants
Through naming document and Key Ceremony

4.16.3 Certification Information
See section **Erreur ! Source du renvoi introuvable.** and section **Erreur ! Source du renvoi introuvable.**

4.16.4 Procedure for Processing Certificate Applications
During KEYNECTIS' Key Ceremony

4.17 Issuance of Certificate CDS UH and Sub-CA
Key pair generation and certification performed in level 5 security room, networkless computer, Cryptographic module FIPS 140 level 3 (Eal4+), M of n secret share principle as described in § 6

4.18 Acceptance of Certificate CDS UH and Sub-CA
Legal notarization with witnesses at the end of Ceremony

4.19 Suspension and Revocation of Certificate UH and Sub-CA
Key pair and certificate are stored during their Life cycle in the high secured bunker of KEYNECTIS. Access and control are under the Security policy governing operation team describe in § 5.
The revocation process describes the premature End of the Operational Period of a UH or Sub-CA Certificate.

4.19.1 Circumstances for revocation

A CDS UH or Sub-CA certificate must be revoked, and the serial number placed on a list of revoked certificates (CRL/ARL), if one of the following circumstances is identified:
- Failure to follow the certificate's rules of use
- The private key is suspected of being compromised, lost, or stolen.
- The CA's certificate is revoked (which leads to the revocation of all of the certificates signed by the corresponding private key).
- The KEYNECTIS organization's activity is discontinued.
- Requested change in the length of the key or algorithm (signature and/or hashing) recommended by an appropriate international or national organization.
- End of the relationship between the CA and client.

4.19.2 Who Can request a revocation
The only parties permitted to request revocation of or revoke a CDS Certificate UH or Sub-CA issued by KEYNECTIS are:
- Organization representative
- Registration Authority
- KEYNECTIS and the ADOBE Policy Authority.

4.19.3 Procedure and processing certificate revocation request
During a Key Ceremony process

4.19.4 Revocation request grace period

There is no grace period available to the Subscriber prior to revocation, and KEYNECTIS shall revoke such CDS Certificate within the next business day and post the revocation to the next published CRL..

4.19.5 Circumstances for suspension

There is no suspension

4.19.6 Who can request a suspension

No stipulation

4.19.7 Procedure for suspension request

No stipulation

4.19.8 Limits on suspension Period

No stipulation

4.19.9 CRL Issuance Frequency

CRL publication is performed every day with a 7 day period of validity for UH certificate.
KEYNECTIS-CDS issues routine ARLs for CDS Sub-CA once every year and CRLs at least once every 24 hours. In the case of a digital ID being revoked due to a private key being compromised, the KEYNECTIS-CDS SUBCA issues an updated ARL/CRL within 24 hours of the revocation.

4.19.10 ARL/CRL Checking requirement

Relying parties must retrieve ARL/CRLs at least once every 24 hours before relying on a document signed using a CDS digital ID except for CDS digital IDs issued for the purpose of time-stamping services.

4.19.11 Online revocation Status checking availability for UH and Sub-CA Certificate

Same as CDS USAGE 1, 2 & 3 for UH certificate
No stipulation for Sub-CA certificate.

4.19.12 Online revocation checking requirements

Same as CDS USAGE 1, 2 & 3 for UH certificate.
No stipulation for Sub-CA certificate.

4.19.13 Other forms of revocation Advertisements Available

No stipulations

4.19.14 Checking requirements for other forms of revocation advertisements

No stipulations

4.19.15 Special Requirement Key Compromise

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

4.20 Security Audit Procedures

4.20.1 Trustworthy Systems

KEYNECTIS-CDS CAs, RAs, and KEYNECTIS reference archives use only trustworthy systems in providing their respective services.

4.20.2 Time Stamping

Time stamping is intended to improve the integrity of KEYNECTIS' electronic certification services and the trustworthiness of certificates. It also assists in the non repudiation of digitally signed messages. Time stamping creates a notation that shows (at the least) the correct date and time of an action (explicitly or

implicitly), as well as the identity of the person or system that created the notation. All time stamps adopt GMT time (Greenwich Meridian Time) and adopt the UTC (Universal Time Convention). For this CPS' purposes, any year written between 00 and 69 means 2000-2069, and any year between 70 - 99 means 1970-1999.

The KEYNECTIS-CDS CA OR SUBCA time stamps the following data either directly on the information, or on a trustworthy audit report:
▪ Certificates
▪ CRL and other suspension and revocation database information.
▪ Each version of the CPS
▪ Customer service messages
▪ Other information, according to the provisions of this CPS.

Comment: Cryptographic time stamping will be implemented incrementally by the CA for all relevant messages.

4.20.3 Types of event recorded

KEYNECTIS-CDS CA OR SUBCA generates automatically records in a trustworthy manner, and certain documents such as:
▪ Documents proving compliance with CPS rules
▪ Documentation of actions and information that is relevant to each certificate application and to the creation, issuance, use, revocation, expiration, and renewal of each issued certificate.

These records contain all information in the CA's possession regarding:

▪ The identity of the subscriber named in each certificate (except for CDS Usage 1 Certificates for which only the subscriber's unambiguous name is maintained and document reference name).
▪ The identity of the individuals requesting certificate revocation (except for Usage 1 Certificates, for which only the subscriber's unambiguous name is maintained).
▪ Other facts represented in the certificate
▪ Time stamps
▪ Certain foreseeable material facts related to certificate issuance.

Documents may be kept in the form of computer-based messages or paper documents, provided that their indexing, storage, preservation, and reproduction are accurate and complete. CAs may ask a subscriber or its agent to provide documents that will enable the CA to comply with this chapter.

4.20.4 Document retention Schedule

KEYNECTIS-CDS CAs save all Usage 2 and Usage 3 records and related documents in a trustworthy manner for at least three (3) years after the date a certificate is revoked or expires. These documents shall be retained either electronically or on paper. For CDS usage 1 electronic document are retained for at least three (3) years after issuance.

4.20.5 Frequency of processing log
Access logs are reviewed on a daily basis (during business days) or as required by any event.

4.20.6 Retention Period for audit log
Audit logs are retained onsite for 1 year at a maximum after the event occurred. According to French law, physical access logs and video surveillance recordings are not kept more than one month.

4.20.7 Protection of Audit Log
Audit logs and recorded information are stored in secure areas according to sensitive items storage policy. Access to theses areas is restricted to authorized KEYNECTIS employees under dual control.

4.20.8 Audit log Backup procedures
All logs automatically generated are duplicated before audit collection.

4.20.9 Audit collection system (internal vs External

All audit logs are manually collected by KEYNECTIS trusted employee(s).

4.20.10 Notification to event-causing Subject

Event-causing notifications are automatically transmitted to KEYNECTIS staff in charge of system operation during business and non business hours, using SMS and Emails.

4.20.11 Vulnerability Assessments

All security policies and operational procedures are reviewed on a yearly basis.

4.20.12 Audit for Sub-CA

KEYNECTIS set up and maintain trustworthy systems for keeping an audit log of all material events, such as key generation, certificate application, validation, and revocation. In order to evaluate its compliance with this CPS and other applicable agreements, guidelines, procedures, and standards, the Annual Recurring Audit shall follow the then-current Webtrustcfor CAs audit program as published by the AICPA or the appropriate certification criteria for alternate equivalent audits approved by the Adobe Policy Authority.

KEYNECTIS' receipt of third-party audit reports does not constitute acceptance or approval of the content, conclusions, or recommendations of these reports on the part of KEYNECTIS. KEYNECTIS may review these reports to protect its electronic certification services. KEYNECTIS is not the author of such audit reports and is therefore not responsible for their content. KEYNECTIS does not express any opinion of these audit reports and shall not be held responsible for any damages resulting from KEYNECTIS reliance on these audit reports.

4.21 Records Archival

4.21.1 Types of event Recorded

KEYNECTIS-CDS CA OR SUBCA archives following records with sufficient detail so that proper operation of the CA can be established

Item / Data to Archived	Required (Yes/No)
Certificate Policy	Yes
Certification Practice Statement	Yes
Contractual Obligations	Yes
System & Equipment Configurations	Yes
Modification & Updates to System or Configuration (Scripts)	Yes
Revocation Requests	Yes
Subscriber Identity Authentication (per Section 3.1.9)	Yes
Documentation of Receipt and Acceptance of Certificates	Yes
Documentation of Receipt of Tokens	Yes
All Certificates Issued or Published	Yes
A Complete Listing of All Certificates Revoked	Yes
All Audit Logs	Yes
Other Data or Applications Needed to Verify Archive Contents	Yes
Documentation Required by Compliance Auditors	Yes

4.21.2 Retention period for Archive
Retention period is 10 years for data that are archived.

4.21.3 Protection of Archive
Audit logs and recorded information are stored in secure areas according to sensitive items storage policy. Access to theses areas is restricted to authorized KEYNECTIS employees under dual control.

4.21.4 Archive Backup Procedures
Audit logs are duplicated before audit collection. A set of audit logs is then ready for transfer to archiving.

4.21.5 Requirements for time stamping of records
Records are time stamped using external multi source clock synchronization

4.21.6 Archive collection system (internal vs. external)
All audit logs are manually collected and handled by KEYNECTIS trusted employee(s).

4.21.7 Procedure to obtain and Verify Archive information
Archive information are subject to KEYNECTIS information protection policy. Access to archive information is granted to external person at KEYNECTIS CEO Level, after a written request has been formulated.

Archive information made available to authorized people at KEYNECTIS premises.

4.22 Key Changeover
KEYNECTIS-CDS CA OR SUBCA uses the key ceremony Key Changeover procedure which describe the security process and script used.

4.23 Compromise and disaster recovery

4.23.1 Computing resources Software and/or data are corrupted
If KEYNECTIS-CDS CA OR SUBCA equipment is damaged or rendered inoperative, the operation is re-established as quickly as possible, giving priority to the ability to generate certificate status information.

4.23.2 Entity Public Key is revoked
KEYNECTIS-CDS CA OR SUBCA uses a new key ceremony procedure in order to reestablish a secure environment after its Public Key would be revoked. These procedures are similar to the initial key pair generation and Public Key submission to the Upper level to recertify. Such revocation process will be performed with control of ADOBE ROOT CA, before any specific procedure would be built up regarding . the End users notification.

4.23.3 Entity key is compromised
If KEYNECTIS-CDS CA OR SUBCA signature Key is compromised; KEYNECTIS will immediately the Adobe Policy Authority.

4.23.4 Emergency Planning and disaster recovery

KEYNECTIS-CDS CA OR SUBCA establishes, documents, and periodically tests emergency and disaster recovery capabilities and procedures, in accordance with the CPS and KEYNECTIS security procedures.

4.24 Termination of CA activities

4.24.1 Termination or cessation of CA Activities
The following obligations are intended to reduce the impact of a discontinued service by providing timely notice, transfer of responsibilities to succeeding entities, record maintenance and certain compensations.
For KEYNECTIS-CDS CA the procedure is described on the CDS Certificate Policy and for KEYNECTIS-CDS Sub-CA the following process is implemented.

4.24.2 Requirements prior to cessation

Before ceasing CA activities, KEYNECTIS-CDS will:

▪ Notify their superior CA (ie Adobe) of their intention to stop acting as a CA. This notification must be made at least ninety (90) days before discontinuance. The superior CA may ask for additional statements in order to verify compliance with this provision.
▪ Provide the subscriber of each unrevoked or unexpired certificate issued by them with ninety (90) days notice of their intention to discontinue their RA activities.
▪ Revoke all of the certificates that remain unrevoked or unexpired at the end of the ninety-day period (90), regardless of whether the subscriber requested revocation or not.
▪ Notify each affected subscriber of the revocation.
▪ Do what they are reasonably able to ensure that discontinuing their certification services will cause minimum disruption for subscribers and individuals who must verify digital signatures by reference to the public key contained in outstanding certificates.
▪ Take reasonable steps to retain their records.
▪ Pay reasonable restitution (without exceeding the certificate's purchase price) to subscribers for revoking their unexpired certificates.

4.24.3 Reissuance of certificates by a CA successor

In order to provide uninterrupted CA services to certificate applicants, CAs that are being discontinued must arrange with another similar authority, subject to the other CA's written agreement and approval by Adobe, the re-issuance of their outstanding subscriber certificates. By reissuing a CA certificate, the successor CA assumes the rights and restrictions of the discontinued CA, and to the extent agreed in writing between the two authorities as approved by Adobe, also assumes the obligations and responsibilities related to unexpired certificates. Unless otherwise stipulated between the discontinued CA and the applicant, and under written agreement from the successor CA, the CPS will remain in effect under the successor CA as it did under the original CA.

The requirements stated here may vary from one contract to another, provided that (a) the changes only affect the contracting parties and (b) Adobe approves all such changes.

5 PHYSICAL PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 Physical controls

5.1.1 Site location and construction
KEYNECTIS-CDS CA OR SUBCA critical and sensitive information processing facilities are housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They are physically protected from unauthorized access, damage and interference. The protections provided are commensurate with the identified risks in the KEYNECTIS-CDS CA OR SUBCA risk analysis.
The KEYNECTIS-CDS CA OR SUBCA is located at KEYNECTIS Trust Center. Disaster recovery facility is protected as primary trust center, using same set of security and protection measures.

5.1.2 Physical Access
All access controls are securely monitored with regard to the "KEYNECTIS Physical security policy".
Access to production rooms requires positive authentication process based on dual access with strong authentication, using a combination of badges and biometrics (what you have and what you are).
All KEYNECTIS employees own badges that allow them to access KEYNECTIS security perimeter in accordance with their privileges.
All physical access rights are defined in a way not to allow a single person to have access to any sensitive data or proceed to a sensitive operation.
KEYNECTIS physical security policy is described in the document referenced [DSQ_NT_KEYNECTIS Physical Security Policy_Tier 7].

5.1.3 Power and air conditioning

KEYNECTIS ensures that power and air conditioning facilities are sufficient to support the operation of the KEYNECTIS-CDS CA OR SUBCA systems, using primary and back up installations according to its physical security policy.

5.1.4 Water exposures
KEYNECTIS ensures that KEYNECTIS-CDS CA OR SUBCA systems are protected in a way that minimize from water exposure consequences according to its physical security policy.

5.1.5 Fire prevention and protection
KEYNECTIS ensures that KEYNECTIS-CDS CA OR SUBCA systems are protected with fire detection and suppression systems according to its physical security policy.

5.1.6 Media Storage
Media used within KEYNECTIS to support KEYNECTIS-CDS CA OR SUBCA are securely handled to protect them from damage, theft and unauthorized access. Media management procedures are implemented to protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

All media are handled securely in accordance with KEYNECTIS sensitive items management policy,
, information protection scheme.

Media containing sensitive information are securely disposed of according to KEYNECTIS sensitive items storage policy.

KEYNECTIS regularly transfer copies or back-ups of sensitive items in an offsite storage location that provides them with security measures equivalent to these at its main premises.

5.1.7 Waste disposal
All media used for the storage of sensitive information such as keys, activation data or KEYNECTIS-CDS CA OR SUBCA files shall be zeroized or destroyed before released for disposal according to KEYNECTIS sensitive item management policy and its destruction policy [DSQ_NT_Destruction des supports d'information].

Back-up tokens that had contained KEYNECTIS-CDS CA OR SUBCA private key material are physically destroyed when no longer used.

5.1.8 Off-Site backup
Full system backups of KEYNECTIS-CDS CA, sufficient to recover from system failure, are made periodically. Back-up copies of essential business information and software are made regularly. Adequate back-up facilities are provided to ensure that all essential business information and software can be recovered following a disaster or media failure. At least one full backup copy of the private key is stored at an offsite location (location separate from KEYNECTIS-CDS CA OR SUBCA material).

The backup is stored at a site with physical and procedural controls commensurate to that of the operational KEYNECTIS-CDS CA OR SUBCA according to KEYNECTIS physical security policy.

5.2 Procedural controls

5.2.1 Trusted roles
All of a CA's employees, contractors, and consultants (collectively called "personnel") who have access to or control over cryptographic operations that may materially affect the CA's issuance, use, or revocation of certificates, including access to restricted operations of the KEYNECTIS reference archives, shall be considered, for the purposes of this CPS, to be in a trusted position. These personnel include (but are not limited to) customer service personnel, system administration personnel, designated technical personnel, and managers who supervise the trustworthy system of the CA's infrastructure.

5.2.2 Number of persons Required per task
KEYNECTIS-CDS CA OR SUBCA sensitive operation that requires multi-person control are all operationally related to CA private key life cycle management. These operations include:

- CA key generation,
- CA key revocation,

- CA certificate generation,
- CA certificate renewal,
- CA key activation,
- CA key deactivation,
- CA key destruction
- Operations on all activation data, from creation to destruction.

All these operations are recorded and realized in accordance with KEYNECTIS-CDS CA procedures by people in trusted roles.

5.2.3   Identification and Authentification for each Role

Identification and authentication of all people involved during a key ceremony is done by KEYNECTIS employees. Identification and authentication personnel who have privileges on KEYNECTIS-CDS CA HSMs is restricted by the possession of physical items (PED keys). These items are required to set up functionality on HSMs. Only cleared people can enter the key ceremony room to activate the HSM that contains the KEYNECTIS-CDS CA OR SUBCA private key.

The list of people cleared to access KEYNECTIS security perimeter and associated access rights is available in the document [DSQ_NT_Droits d'accès zones KEYNECTIS].

5.3   Personnel controls

5.3.1   Personnel management Procedures

KEYNECTIS-CDS CAs devise and follow personnel management procedures that provide reasonable assurance of the credibility and competence of their employees, and of the satisfactory performance of their duties.

5.3.1.1   Personnel in trusted positions

Personnel shall not have access to the trusted functions until any necessary checks are completed. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation according [DSQ_NT_KEYNECTIS trusted employee policy].

KEYNECTIS Back-ground checks include at least:

- *Personal Identity;*
- *Place of residence;*
- *Social Security Tracing Number;*
- *Criminal Conviction Records;*
- *Bank coordinates;*
- *Previous Employment;*
- *Professional References;*
- *Education.*

This provision does not apply to members of the KEYNECTIS board of directors or CAs, unless they occupy an operational position within the electronic certification services.

5.3.1.2   Removal of individuals in trusted positions

Any individual who fails an initial or periodic investigation shall be removed from the trusted position. The removal of someone in a trusted position shall be left to the sole discretion of the CA concerned (or KEYNECTIS, in the case of KEYNECTIS personnel).

5.3.1.3   Retraining frequency and requirements

KEYNECTIS employees are regularly informed and kept aware regarding security procedures according to [DSQ_NT_KEYNECTIS_Trusted Employee Policy]. In addition, KEYNECTIS employees are trained on a yearly basis as part of the internal company training plan.

5.3.1.4   Job Rotation frequency and Sequence

No stipulation.

5.3.1.5   Sanctions for unauthorized Actions

All KEYNECTIS employees are subject to sanctions according to Article 22 "Sanctions disciplinaires" of KEYNECTIS internal regulation statement.

5.3.1.6   Contracting Personnel requirements

KEYNECTIS-CDS CAs conducts an initial investigation of all personnel who are candidates for trusted positions in order to determine their trustworthiness and competence as reasonably as possible. KEYNECTIS-CDS CAs conducts a periodic investigation of all personnel who occupy a trusted position to confirm their continued trustworthiness and competence, in accordance with KEYNECTIS' employee practices or the equivalent.

5.3.1.7   Documentation Supplied to personnel

KEYNECTIS trusted employees are provided with documentation related to the task(s) they have to perform during KEYNECTIS-CDS CA OR SUBCA operation. This documentation is provided either during training, through KEYNECTIS corporate network or a need to know basis.

6   TECHNICAL SECURITY CONTROLS

6.1   Approval of software and Hardware devices

All software and hardware related to electronic certification services shall be approved by KEYNECTIS, an authorized KEYNECTIS consultant, or other recognized authorities (periodically designated by KEYNECTIS), based on need, in accordance with this CPS.

6.2   Key pair Generation, installation and protection

6.2.1   KEYNECTIS-CDS CA and Sub-CA key pair Generation

KEYNECTIS-CDS CAs securely generate and protect their own private keys through a trustworthy hardware security module that exceeds FIPS 140-1 level 3 and take the necessary precautions to prevent loss, disclosure, modification, or unauthorized use.
KEYNECTIS currently employs the ITS Luna Card CA 3 from Chrysalis (common criteria EAL 4+ and FIPS 140-1 Level 2 &3)
To be able to provide multi-provider solution KEYNECTIS employs the Bull Trustway HSM device (EAL4+ and FIPS 140-3) as the hardware cryptographic signing units. All the tokens have been developed with custom software to allow for tamper-resistant capacity.
CA and Sub-CA private key generation is performed during an official **key ceremony**:
  ▪ Using approved cryptographic hardware;
  ▪ Using special offline dedicated computers;
  ▪ Under dual-control;
  ▪ In a dedicated secure room located at the KEYNECTIS facility, under video surveillance / recording and with notary public services.

6.2.2   Private Key pair delivery

KEYNECTIS-CDS CA and Sub-CA generate their own private keys and therefore, no delivery is necessary outside the KEYNECTIS Bunker
Subscribers private keys are provided to the subscriber or authorized representative in accordance with the section operational requirements above.

6.2.3   Public Key delivery to certificate Issuer

Public keys are delivered to the digital ID issuer via a PKCS#10 requests. The PKCS#10 request is signed using the Subscriber's private key. The Subscriber's signature is authenticated by the Issuing CA prior to issuing the Subscriber a digital ID.

6.2.4   Key Sizes
KEYNECTIS-CDS CA and Sub-CA use RSA KEY pair 2048 bits length
CDS Subscriber digital Id shall use an RSA key pair with at least 2048 bits.

6.3   Private KEY Protection

6.3.1   Protection using cryptographic hardware

KEYNECTIS-CDS CAs use trustworthy hardware cryptographic modules for all operations requiring the use of their private key. The procedure for creating private keys is published in the KEYNECTIS reference archives.
All cryptographic tokens and other hardware related to the certificate issuing process are kept in secure rooms protected by both electronic key access and biometric readers. All of the secure rooms are (physical security) level 4 (of 7) security area, fire protected using automatic extinguishing systems and access privileges are limited to those trusted employees with job responsibilities inside the rooms.

6.3.2   Secret sharing

KEYNECTIS-CDS CAs use secret sharing using authorized secret share holders to improve the trustworthiness of their private key(s) and ensure their keys' recovery, as shown in Table 4 – Distribution of secret shares – below:

Entity	Secret share required to enable CA's private key to sign end user certificates	Secret share needed to generate keypair CA certificate	Total secret shares distributed	Shares recovered from disaster	
				Needed	Total
KEYNECTIS–CDS CA (RCA)	2	3	5	3	5
KEYNECTIS-CDS Sub-CA CA (RCA)	2	3	5	3	5
KEYNECTIS-CDS UH	2	3	5	3	5

Table 2 – Distribution of secret shares

6.3.2.1   Protecting the secret share

The secret share holder shall use trustworthy systems to protect its secret share from violations. Unless stated otherwise in this CPS, the secret share holder agrees that he or she shall not:

▪ Disclose, publish, copy, share with third parties, or participate in any unauthorized use the secret share;
▪ Reveal (explicitly or implicitly) to anyone outside of the company that he or she, or anyone else, is a secret share holder;
▪ Store the secret share in a location where it cannot be recovered in the event that the secret share holder becomes incapacitated or unavailable (unless the secret share is being used for other purposes).

6.3.2.2   Availability and Release of Secret Shares

The secret share holder shall make the secret share available to authorized entities (list included in the secret share acceptance form) only after obtaining proper authorization through an authenticated record (see next paragraph).

In case of an accident (declared by the secret share issuer), the secret share holder shall contact a recovery site in accordance with the instructions from the secret share issuer.

Before reporting to an emergency or recovery site and releasing the secret share, the secret share holder shall authenticate the declaration of the secret share issuer according to the instructions on the secret share acceptance form (unless prohibited by law or legal process; for example, in the case of a criminal investigation).

This procedure shall include the use of a Challenge Phrase (given by the secret share issuer to the secret share holder) to ensure that the secret share holder is not tricked into going to the wrong site, thus preventing the secret share issuer from recovering. On the recovery site, the secret share holder shall deliver (in person) the secret share in order to participate in the recovery process after the accident.

The secret share holder may rely on any instruction, document, message, record, instrument, or signature he or she feels with reasonable certainty to be authentic, provided that he or she authenticates the secret share issuer's declaration in accordance with the preceding paragraph. The secret share issuer shall provide the secret share holder with a sample of all of the signatures used to authenticate the secret share issuer's instructions.

6.3.2.3   Records to be kept by secret share issuers and holders

Secret share issuers and holders shall keep records of their secret-share related activities. The secret share holder shall provide information about secret share status to the secret share issuer or designated representative upon authenticated request.

6.3.3   Private key escrow

KEYNECTIS-CDS Private keys are escrowed during KEY Ceremony and stored in a manual process in security level 7 of the KEYNECTIS bunker.
KEYNECTIS-CDS for UH private keys are escrowed during KEY Ceremony and stored in a manual process in security level 7 of the KEYNECTIS bunker.

CDS subscriber's private keys are not escrowed

6.3.4   Private key backup

Backup of CDS subscriber's private keys shall not be made
Backup of KEYNECTIS-CDS CA and Sub-CA's private keys is described below

6.3.5   Private key Archival

Secret shares and back-up CA private keys are kept in an level 7security area that enforces dual control access proceures:.
- Authorised personnel escort shareholders (people owning the secret share) into a special-purpose secure room (trusted individuals with biometric/electronic key access privileges).
- A one-hour fire resistant media safe located in a secure room provides protective storage to safe deposit boxes located inside the media safe. These boxes are placed under dual control and provide individual storage location for each secret key shareholder.

Note: Disaster recovery keys are kept in safe deposit boxes off-site in a bank vault under dual trusted-party control.

6.3.6 Private key Entry into cryptographic Module

Private keys of KEYNECTIS-CDS CAs are generated by the cryptographic Module Only.
Private Keys of subscriber are either generated by the cryptographic Module or imported to it.

6.3.7 Method of Activating Private Key

In order to activate a private key, Subscribers or Trusted Roles must authenticate to the medium housing the private key. Forms of authentication include but are not limited to passwords, PINs, pass-phrases, and biometrics.

6.3.8 Method of Deactivating Private Key
Deactivation of crypto modules containing the CA private key is automatic each time they are disconnected from their system readers. Reactivation of the private key stored in the HSM requires 6 people under dual control.

6.3.9 Method of Destroying Private Key

KEYNECTIS-CDS CA and Sub-CA private key destruction may be performed using different mechanisms including erasure of CA private key using the reset and or deletion functions of the crypto modules, or physical destruction of the crypto modules.

6.4 Other aspect of key Pair management

6.4.1 Public Key archival
No stipulation

6.4.2 Usage periods for the public and Private keys
CDS USAGE 1 Certificate may use Private Key usage periods.
No stipulation for other usage.

6.5 Activation data

6.5.1 Activation data generation and Installation
KEYNECTIS-CDS activation data to unlock private keys in cryptographic module are performed during the KEY CEREMONY.
Secret shares allowing activation of CA private key under an 6-level split are generated using the hardware crypto modules containing the private key, during the key ceremony. Activation of crypto modules containing the customer CA private key requires these secret shares to be available at any time.

6.5.2 Activation Data Protection
Activation data are protected from disclosure and use a manual n of m secret share principle.

6.6 Computer security controls

6.6.1 Communications security

All communications pursuant to this CPS between KEYNECTIS and other parties involved with electronic certification services must use an application that provides the appropriate security mechanisms with measured risk. Without limiting their scope, computer notices, the acknowledgments of receipt for these notices, and any other communication affecting the security of the certification services shall also be protected in the appropriate manner.

6.6.2 Facilities security

KEYNECTIS-CDS CAs use trustworthy facilities that substantially comply with KEYNECTIS security procedures or the equivalent standards.

6.7 Life cycle Technical Controls

6.7.1 System development controls
System development and software builds and modifications are documented and controlled by KEYNECTIS Quality Department

6.7.2 Security management Controls
Initial CA system (hardware, application, operating system) builds and modifications thereafter are documented and controlled by KEYNECTIS Quality Department

6.7.3 Life cycle security Rating
All KEYNECTIS-CDS CA components software at KEYNECTIS trust center have been developed following the requirements of CEN CWA 14167-1 "Security requirement for trustworthy systems managing digital certificates for electronic signatures".

6.8 Network Security Controls Computer security controls
Network accessible PKI components are connected to the Internet via boundary protections and provide continuous service (except, when necessary, for brief periods of maintenance or backup).
KEYNECTIS-CDS CA components employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of guards, firewalls and filtering routers. Unused network ports and services are turned off. Any boundary control devices used to protect the network on which PKI equipment is hosted deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network. All security principles ansd measures that apply are identified in KEYNECTIS information system security policy.

6.9 Cryptographic Module Engineering Controls
The HSM used for KEYNECTIS-CDS CA purposes are either FIPS..

7 CERTIFICATE AND CRL PROFILES

7.1 Extensions and Naming rules

7.1.1 Extension mechanisms and authentication framework

Certification services facilitate the use of X.509 v3 certificates. X.509 v3 certificates expand the capabilities of v1 and v2 and allow adding extensions to a certificate. This capability, a standard component of KEYNECTIS certification services, rounds out the standard authentication services model.

7.1.2 Standard and specific extensions

The X.509 "*Amendment 1 to ISO/IEC 9594-8:1995*" defines a series of extensions. These extensions provide management and administration controls that are useful for large-scale and multipurpose authentication. KEYNECTIS certification services use several of these controls for purposes identified in X.509. (Comment: user software compliant with X.509 is assumed to apply the validation rules of the CPS.

In addition, the CPS enables users to define additional "private" extensions for purposes or methods specific to their application environment. The definition for service-based extensions to and practices for processing this information during certification application, approval, and issuance, are specified in the KEYNECTIS security procedures as well as publicly available documents from the organizations sponsoring these extensions.

7.1.3 Identification and criticality of special extensions

The function of each extension is indicated by a standard "object identifiers" value. In addition, each certificate extension is assigned a criticality value of true or false. This value is determined by the CA, possibly based on information provided by the applicant on the certificate application. This value must comply with certain constraints imposed by the organization responsible for the extension definition.

The presence of a "true" criticality value in a given extension requires anyone validating the certificate to consider it invalid if they do not know the purpose and requirements for any specific extension with a criticality value of *true*. If this value is false, these individuals shall process the extension in compliance with the applicable definition during validation or else ignore the extension.

7.1.4 Certificate chains and types of CAs

KEYNECTIS electronic certification services use chains of certificates. Each CA of a KEYNECTIS certificate chain performs particular procedures based on its assigned role in the ADOBE hierarchy. One CA may have two different roles.

- "Sub-CA of the ADOBE Root CA" certification authority (CA) and,
- CA for another CA.

7.1.5 End user certificate extensions

CAs for end users may issue certificates containing extensions defined in the document "*X.509 Amendment 1 to ISO/IEC 9594-8:1995".* ISO extensions used in the KEYNECTIS certification services, whose content is assigned by the CA concerned, are currently limited to the following:

- Basic constraints
- Key usage
- Extended key uses
- Certificate policy
- AKI (authority key identifier / SKI (subject key identifier)

The use of these extensions controls the process of issuing and validating certificates.

7.1.6 ISO basic constraint extensions

The basic constraints extension is used to limit the role and position of a CA or end user certificate in a chain of certificates. For example, certificates issued to CAs and subordinate CAs contain a basic constraint extension that identifies them as CA certificates. End user certificates have an extension that constrains the certificate from being a CA certificate.

7.1.7 ISO "Key Usage" and "Extended Key Usage" extensions

The "Key Usage" extension limits the technical purposes for which a public key listed in a valid certificate can be used within the KEYNECTIS electronic certification services. CA certificates may contain a key usage extension that restricts the use of the key to signing certificates, certificate revocation lists, and other information.

7.1.8 ISO "Certificate Policy" extension

The "Certificate Policy" extension limits a certificate to the practices required by (or indicated for) trusted parties. The "Certificate Policy", such as the one implemented in the certification services, refers its users to the CPS and indicates appropriate usages.

Extensions and enhanced naming are either fully provided in a certificate or partially provided with the remainder in an external document included by reference in the certificate.

Information contained in the» Organizational Unit" field is also found in the certificate Policy extension, when included in the certificate. This CPS constitutes a "certificate policy" according to the terms in the "*X.509 Amendment 1 to ISO/IEC 9594-8:1995*". A CA, acting as an authority authorized to form policies, assigns to the CPS an object identifier value (OID) that is present in the certificate Policy extension.

7.1.8.1 Pointers to the CPS

User-readable text and computer pointers (URL-based or other identifiers and mechanisms) are used so that certificate users can easily locate and access the CPS and other pertinent information.

7.1.8.2 Warnings, liability limitations, and warranty disclaimers

Each certificate may contain a brief statement explaining applicable liability limitations and warranty disclaimers, with a pointer to the full text of these warnings, disclaimers, and limitations in the CPS.

This information may also be displayed through the certificate viewing function, possibly through a hypertext link to a message accessible by users or agents, instead of being included in the certificate. The method used to share information (to be presented to users) is a CA qualifier to a certificate policy registered with KEYNECTIS (using a standard v3 extension).
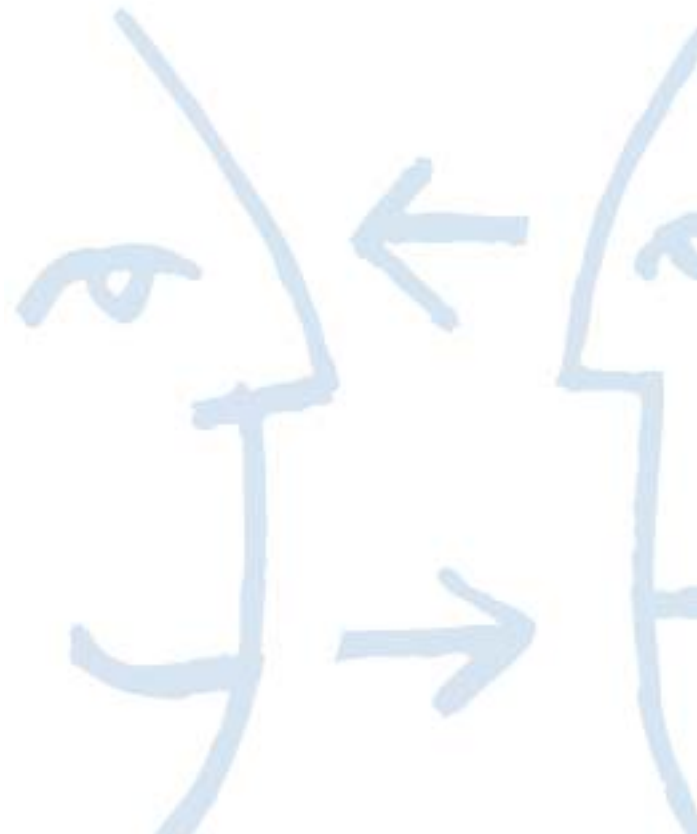
8 SPECIFICATION ADMINISTRATION

8.1 CPS change procedures

KEYNECTIS-CDS CA CPS must be reviewed and approved by the Adobe Policy Authority prior to its application and publication. KEYNECTIS will also:

- Provide any new CPS changes with highlights changes,
- Wait for approval of the New CPS,
- Publish and apply the new CPS.

8.2 Publication and notification policy

The KEYNECTIS Policy Authority maintains this Policy. All proposed changes to this Policy shall be communicated to all CDS Subordinate CAs ninety (90) days prior to the change being made. The KEYNECYTIS Policy Authority will consider comments in favor or opposition of the proposed changes as long as they are submitted in writing and within 30 days of the proposed change being published.

8.3 CPS Approval procedure

This KEYNECTIS-CDS CA CPS has been approved by the Adobe Policy Authority prior to reception of the Adobe ROOT CA certificate in accordance with the Adobe CDS policy.

9 APPENDIX

This document contains acronyms and abbreviations. The glossary below provides a reference for the most commonly used terms:

A / B

Adobe PKI
The policy, process and technology required to manage, use and rely on certificates that chain to the Adobe Root CA.

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.

Accept (a certificate)
Certificate applicants demonstrate that they approve a certificate while knowing or having notice of the information that it contains in accordance with the CPS.

Access
A specific type of interaction between a request and communications or information sources that results in a flow of information, exercise of control, or the activation of a process.

Accreditation / Accredited
A formal declaration by an authorized KEYNECTIS representative that a given information system, professional, employee, subcontractor, or company is approved to perform certain operations and to operate in a specific security mode, using a defined set of security of measures.

Affirm / Affirmation
To recognize or indicate that data is correct or information is true.

Alias
Synonym of pseudonym

ARL
Authorithy Revocation List, Also known as CAEL or Certification Authority Revocation List

Archive
To store records and corresponding logs during a given period for security, backup, or auditing purposes

Audits
A procedure used to demonstrate that controls are in place and are suitable for their purpose. An audit records and analyzes operations to monitor intrusions or uses within an information system. Anomalies detected by an audit are reported to the appropriate department.

Authentication
A process that is implemented to confirm the identity of an individual or the integrity of information. A message is authenticated by determining its origin and verifying that it has not been modified or replaced in route.

Authenticate
See Authentication

Authorization
The granting of rights, particularly the ability to access specific information or resources.

Availability
The extent to which information or processes may be reasonable accessed or used, upon demand, by an authorized entity. Availability allows authorized access to resources and ensures the timely performance of urgent operations.

Binding
Confirmation by a registration authority of the relationship between a named entity and its public key.

C

CA Certificate
Certificate issued by a CA to a subordinate CA.

CA Certificate Application
A request sent by a non-KEYNECTIS entity to KEYNECTIS electronic certification services to become a CA and to receive a CA certificate.

CDS
Certified Document Services.

CDS Certificate
A signing certificate issued within the CDS PKI for the purposes of digitally signing PDF documents.

CDS document
AnAcrobat document signed using a CDS Certificate.

CDS Pki

The policy, process and technology required to manage, use and rely on certificates that chain to a root CA embedded in Acrobat, Reader, and LiveCycle products by Adobe and used in connection with Certified Document Services.

CDS Subordinate CA
Any authorized Certification Authority that chains to a root CA embedded in Acrobat by Adobe.

Certificate
A message that, at least, states a name or identifies the applicant, contains the applicant's public key, identifies the certificate's validity period, contains a certificate serial number, and carries the CA's digital signature. Any reference to a "usage certificate" (1, 2, 3…) without another qualifier shall mean a "normal" or "provisional" certificate, unless the context requires otherwise. References to a certificate refer exclusively to certificates issued by a CA.

Certificate Applicant
A person or authorized agent that requests the issuance of a public key certificate by a CA.

Certificate Applicant
Authorized person who requests the issuance of a certificate from a CA.

Certificate Application
A request from a certificate applicant to a CA for the issuance of a certificate.

Certificate of Authenticity
A document issued by an authorized official authority of the jurisdiction in which an acknowledgement by a notary was made to authenticate the status of a notary.

Certificate Chain
A sequenced list of certificates containing a certificate applicant (end user) and CA certificates.

Certificate Expiration
The date and time specified in a certificate, marking the end of the validity period, without including a possible earlier revocation.

Certificate Extension
An extended field of a certificate, which may provide additional information about the certified public key, the certificate subscriber, certificate issuer, and/or the certification process. Standard extensions are defined in Amendment 1 of ISO/IEC 9594-8: 1995 (X.509).

Certificate Hierarchy
Within the electronic certification services, all of the CAs usageified by category based on their role in the CA tree structure. A CA issues and manages certificate for end-user subscribers and/or for one or more subordinate CA(s). A CA in a trust hierarchy must observe uniform procedures, particularly naming, and the maximum number of levels, etc., to assure integrity of the domain and thereby ensure uniform accountability, auditability, and management through trustworthy operational processes.

Certificate Issuance
The actions performed by a CA in creating a certificate and notifying the certificate applicant (anticipated to become a subscriber) listed in the certificate.

Certificate Revocation
See Revoke a Certificate.

Certificate Revocation List (CRL)
A periodically issued list, digitally signed by a CA, of certificates that have been identified as suspended or revoked before their expiration date. The list generally includes the CRL issuer's name, date of issue, the

date of the next edition, the serial number of the revoked certificates, and specific times and reasons for revocation.

Certificate Serial Number
A value that unambiguously identifies a certificate issued by a CA.

Certificate Signing Request (CSR)
A machine-readable form a certificate application.

Certification Authority (CA)
Also called the Certificate Authority. The entity who issues digital certificates. It sets the terms and conditions related to managing a certificate life cycle (issuance, renewal, revocation, etc.). To do this, the certification authority is responsible for writing a certificate policy (CP) explaining these terms and conditions.

Certification / Certify
The process of issuing a certificate by a registration authority.

Certification Policy (CP)
Also called a Certificate Practice Statement. Defines the procedures for generating and managing certificates. It defines the trust relationship between the end user and certificate holder.

Certification Practice Statement (CPS)
A document, revised from time to time, that represents the statements of practices a CA uses in issuing certificates.

Certified Document Services
A service offered by Adobe partners in which an Adobe PDF document can be digitally signed by its author using a Digital ID generated within the CDS PKI.

Challenge Phrase
A set of numbers and/or letters selected by a certificate applicant, sent to the registration authority with a certificate request, and used by this authority to authenticate the applicant as required by this CPS.

Usage 1, 2, and 3 Certificates
A certificate for a specified level of trust.

Commercial reasonableness
In the context of e-commerce, installation, and use of technology, controls, and administrative and operational procedures that reasonably ensure system and message trustworthiness.

Compromise
A violation (or suspected violation) of a security measure, in which confidential information may have been disclosed or loss of control may have occurred (see data integrity).

Confidentiality
The status in which important information is kept secret and only disclosed to authorized parties.

Confirm
To declare or indicate through an action (examination, investigation) that data is true and information is accurate.

Controls
Measures taken to ensure the integrity and quality of a process.

Correspond
To belong to the same key pair.

Cosign

Sign a previously signed ,with a CDS certificate, Adobe PDf document.

Credible database
Database created under government control and/or approval. These database can be created shared with government program (ie Used in PRIS program or health) or group of approved association (ie Banking, industrial group of identified members)

Cross-Certification
A situation in which a KEYNECTIS CA and/or an RA other than KEYNECTIS (representing another certification domain) issues a certificate with the other as the subject of that certificate.

Cryptographic Algorithm
A clearly specified calculation process for resolving a problem. A set of rules that produce a prescribed result.

Cryptographic Hardware
Security hardware devices that contain the user's private key, public key certificate and, as an option, a cache of other certificates, including all of the certificates in the user's certification chain.

Cryptographic Resource
Material resource that stores private keys.

Cryptography
There are two types of cryptography: the symmetrical cryptography of a private key and the asymmetrical cryptography of a public key.

Cryptomodule
A trustworthy implementation of a cryptosystem, which safely encrypts and decrypts data.

D

Data
Programs, files, and other information stored in, communicated, or processed by a computer.

Database
A set of related information, created, stored, or manipulated by a computerized management system.

Data Integrity
A condition in which data has not been modified or destroyed in an unauthorized manner.

Digital Identification
Name given to a certificate.

Digital Signature
The transformation of a message through an asymmetric encryption system such that a person with the initial message and the signer's public key can accurately determine if the transformation was created using the private key corresponding with the signer's public key and if the message has been altered since the transformation.

Directory
See Reference Archives

Distinguished Name
Distinctive name.

Distinguished Name (DN)
A set of data that identifies a real entity, such as a person in a computer-based environment (CN = Common Name) (C = Country) (S = State) (O = Organization) (OU = Organization Unit).

E / F

Electronic certificate
A certificate is an electronic file that represents a digital identification document by establishing a link with the entity associated with it.

Electronic mail
Messages sent, received, or forwarded in digital form via a computer-based communications system (email).

Electronic Certification Service
Services provided by a certification (electronic) services provider. For example, issuance of electronic certificates, certification directory service, CRL provision, provision of time stamp token, archiving, etc.

Employee in Good Standing
A non-probationary employee that has not been terminated or suspended, and is not facing pending disciplinary action by his or her employer.

Encryption
Process by which intelligible information is made unintelligible in order to protect confidentiality.

End Entity
See person.

File Transfer Protocol (FTP)
An application protocol that offers a file transfer system in an Internet environment.

Free certificate
A certificate issued by a registration authority without charge.

G / H

Generate a Key Pair
To create, in a trustworthy environment, during certificate application, private keys whose corresponding public keys are submitted to the CA in a way that demonstrates the applicant's capacity to use the private key.

Hash (Hash Function)
A mathematical function such as:
▪ A message yields the same result each time that the algorithm is applied to the same message;
▪ It is mathematically impossible to deduct or reconstitute the message from the result produced by the algorithm;
It is mathematically impossible to find two different messages that produce the same hash result with the same algorithm

HSM
Hardware Security Module

I / J

Identification
The process of confirming the identity of a person. Identification is facilitated in public key cryptography by certificates.

Identity

A unique piece of information that marks or signifies a particular entity in a domain. This information is only unique within its domain.

Identity Naming
The use of an "Organization Unit" extended field (OU =) in an X.509 v3 certificate.

Integrity
See data integrity

K / L

Key Generation
Trustworthy process for creating a key pair (private / public).

KEYNECTIS Naming Authority
A naming authority that established and enforces controls over and has decision-making power regarding the issuance of relative distinguished names for all RAs.

Key Pair
A private key and its corresponding public key. The public key can authenticate a digital signature created by using the corresponding private key. In addition, depending on the type of algorithm used, key pair components can also encrypt and decrypt information for confidentiality purposes, in which case, only a private key allows you to read encrypted information through its corresponding public key.

M

Message
A digital representation of information; computer-based record.

N / O

Name
A set of identifying attributes used to describe a certain type of entity.

Naming
The assignment of descriptive identifiers to objects of a particular type. This is done by an authority that follows specific issuing procedures and maintains specific records in keeping with identified registration procedures.

Naming Authority
An entity that executes naming procedures and policies and has control over the registration and assignment of basic names to objects of a particular usage.

Non-KEYNECTIS RA
An RA that is not owned or operated by KEYNECTIS, and whose functions are limited to that of an RA, or machines.

Nonrepudiation
Provides proof of the origin or delivery of data in order to protect the issuer against a false declaration by the recipient that the information has not been received and to protect the recipient against a false declaration by the issuer that the data has not been issued. Provides proof in case of disagreement.

Notice
The result of notification in accordance with this CPS.

Notify
To share specific information with another person as required by this CPS and applicable law.

Organization
An entity with which a user is affiliated. The organization itself may be a user.

Originator
A person by whom (or on whose behalf) a data message is presumed to have been generated, store, or communicated. A person acting as an intermediary is not considered to be an originator.

P / Q

Parties
Entities whose rights and obligations must be governed by a CPS. These entities may be certificate subscribers, CAs, or trusting third parties.

Password
Confidential authentication information comprised of a string of characters used for access to a resource.

Person
A human being or organization (or a device under the control of a human or organization) capable of signing or confirming a message.

Personal Presence
The act of appearing (physically, rather than virtually or figuratively) before an RA or its designee and proving one's identity as a prerequisite to the issuance of a certificate under certain conditions.

PKI Hierarchy
All of the CAs whose functions are organized according to the principle of delegation of authority and related to each other as subordinate or superior.

Private Key
A mathematical key kept secret by its holder. It is used to sign information electronically and decrypt data encrypted by the corresponding public key.

Promise
Agreement or behavior whose purpose is to convey the general intention of a registration authority, supported by a good faith effort, to provide and maintain a specific service. A "Promise" does not necessarily involve a guarantee that the services shall be fully provided and satisfactory. Promises are separate from assurance and guarantees, unless expressly indicated.

Public Key
A mathematical key that can be made public used to verify the electronic signatures created by its corresponding private key. A public key may also be used to encrypt data that is decrypted by the corresponding private key.

Public Key Certificate
See certificate

Public Key Cryptography
A method of cryptography based on a pair of mathematically related keys. The public key can be made available to anyone who wishes to use it. It can encrypt information or verify a digital signature. The private key is kept secret by its holder and can decrypt information or generate a digital signature.

Public Key Infrastructure (PKI)
All the technical, human, document, and contract means made available to users to ensure, along with asymmetrical cryptographic systems, a secure environment for electronic communications.

Publish
To record and usageify information in the reference archives in order to disclose and make public certain information in compliance with this CPS and applicable law.

Qualifier
A data syntax facilitating the representation of a set of values that restrict the meaning of the CPS. The qualifier value increases the certificate policy extension in all certificates, according to the rules defined by X509.

R

Recipient (of a digital signature)
A person who receives a digital signature and who is in a position to trust it, regardless of whether such trust occurs.

Record
Information that is inscribed on a tangible medium (a document) or stored in an electronic medium or other, which can be retrieved in a perceptible form. The term "record" is the cumulative term for "document" and "message" (see document, message).

Reference archives
Certificate database that also contains other relative information.

Registration
Process by which an applicant requests a certificate.

Registration Authority Administrator
An employee of an RA responsible for performing the functions of an RA.

Registration Authority (RA)
An entity responsible for identifying and authenticating electronic certificate applicants on behalf of a CA, but is not in charge of issuing electronic certificates.

Registration Field Information
Country, zip code, age, and type of data included within a designated certificate, based on options selected by the applicant

Relative Distinguished Name (RDN)
A set of attributes including an entity's distinguished name that distinguishes this entity from others of the same type.

Relying party
An individual who uses an Adobe Acrobat product to validate a certified document.

Renewal
The process of obtaining a new certificate of the same usage and type as the previous certificate once it has expired.

Repudiation
The denial or attempted denial by an entity involved in communication of having participated in all or part of the communication.

Revoke a Certificate

The process of permanently ending the validity of a certificate from a specific time (for example, when a private key is compromised).

Root
The CA that issues the first certificate in a certification chain. The root's public key must be known in advance by the certificate user in order to validate a certification chain.

Root Certification Authority (RCA)
Highest level Certification Authority

RSA
A public key cryptographic system invented by Rivest, Shamir, and Adelman.

S

S/MIME
A specification for secure electronic mail using a cryptographic message syntax in an Internet environment.

Secret Share
A portion of an encrypted secret distributed among a number of physical tokens.

Secret Share Holder
An authorized holder of a physical token containing a secret share.

Secret Share Issuer
A person designated by a RA to create and distribute secret shares.

Secret Sharing
The practice of distributing secret shares of a private key to a certain number of secret share holders, based on the tolerance of key sharing.

Secure channel
A cryptographically-enhanced communications path that protects messages against perceived threats.

Security
The quality or state of being protected against unauthorized access or uncontrolled losses or events. Absolute security is impossible to achieve in practice and the security of any given system is relative.

Security Policy
A document articulating the needs and good practices in regards to the protection and security practices maintained by a trustworthy system in support of the CPS.

Security Services
Services provided by a set of security mechanisms. Among these services are access control, data confidentiality, and data integrity.

Self-Signed Public Key
A data structure that is constructed like a certificate, but signed by its own subject. Unlike a certificate, a self-signed public key may not be used to authenticate a public key to other parties.

Serial Number
(See certificate serial number).

Server

A computer system that responds to requests from client systems.

Sign
To create a digital signature for a message or to affix a signature to a document.

Signature
A method that is adopted or used by a document's originator to identify himself or herself. This method is either accepted by the recipient, or its use is routine under the circumstances.

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

Smart Card
A hardware security device that contains a user certificate and related private key.

Smart key
Physical cryptographic device enabling the secure manufacturing and storage of an electronic certificate. It can be used without a reader and connects to the computer's USB port.

Subject
Holder of a private key corresponding to a public key. The term "subject" can refer to both the equipment and device that holds the private key and to the individual person, if any, who controls that equipment or device. A subject is assigned an unambiguous name bound to a public key contained in the subject's certificate.

Subject Name
Unambiguous value contained in the subject name field bound to the public key.

Subscriber
A person who is the subject of, has been issued a certificate, and who is capable of using and authorized to use, the private key that corresponds to the public key listed in the certificate.

Subscriber agreement
An agreement executed between an applicant and a CA for the provision of designated electronic certificate services in accordance with this CPS.

T / U

Test Certificate
A certificate issued by a CA for technical testing only. Only authorized individuals may use test certificates.

Threat
A circumstance or event likely to cause harm to a system, including the destruction, unauthorized disclosure or modification of data, or denial of service.

Time Stamping
A service that indicates the correct date and time of an event in a reliable manner.

Token
A hardware device that is used to store either a certification authority's or a subscriber key pair and certificate chain and perform signing.

Transaction
Transfer of professional information by computer, which consists of special processes to facilitate communication over global networks.

TransNUM
Unique Electronique reference of a CDS Document signed by the Usage3 organization certificate and used in the Usage1 certificate issuance (refers to Kwebsign PGP document OID:1.3.6.1.4.1.22234.2.4.6.1.2).

Trust / To Trust
To accept a digital signature and act in a way that would be harmful if the digital signature should be proven ineffective.

Trusted Root
A trusted root is a public key that has been confirmed as bound to a CA by a user or a system administrator. Software and systems that perform authentication using public key cryptography and certificates assume that the key's value has been correctly obtained. Trust is confirmed by always accessing the root from a trusted archives base that can only be modified by identified, trusted administrators.

Trusted Role
A trusted role applies to person who have access to or control over cryptographic operations that may materially affect the CA's issuance, use, or revocation of certificates, including access to restricted operations of the KEYNECTIS reference archives, Additional security rules, defined by KEYNECTIS ' security department complete the definition of the role (Ie: Secret sharing holder)

Trusted Third Party
Independent and impartial third party that contributes to the final security and trustworthiness of computer-based information transfers.

Trusting Parties
Recipients who act in trust of a certificate or digital signature.

Trustworthy System
Computer hardware, software, and procedures that are protected against intrusion and misuse; provide a reasonable level of availability; suited to perform their intended functions; and strengthen the applicable security policy

Trustworthy Audit report
Electronic report electronically timestamped.
Type of Certificate
The defined properties of a certificate that limit its role to a usage of applications associated to that exact type.

UH
Unite d'Horodatage : French term to designate the Entity able to sign time stamping token with a certificate

Unambiguous Name
See Distinguished Name

Universal Resource Locator (URL)
A standard device for identifying and locating certain records and other resources located on the World Wide Web.

Unverified Information (UVI)
Information contained in a certificate and submitted by an applicant to a CA that has not been confirmed by the CA, and for which the CA provides no assurances other than that the information was submitted by the certificate applicant. Information such as titles, professional degrees, accreditations, and registration field information are considered UVI, unless otherwise indicated.

User
An authorized entity that uses a certificate as applicant, recipient, or trusted party. Does not include the CA who issues the certificate.

V

Validation of a Certificate
The process performed by a recipient or trusted party to confirm that a certificate is valid, and to confirm that it was valid at the date and time a digital signature was created.

Validation of a Certificate Application
The process performed by the CA, following the submission of a certification request, as a prerequisite for the approval of the application and issuance of a certificate.

Validation of a Certificate Chain
For each certificate in the chain, the process performed by the recipient or trusted party to:
- Authenticate the public key (of each certificate),
- Confirm that each certificate is valid
- Was issued during its validity period, and that all of the trusted parties acted in compliance with the CPS.

Validity Period
The period beginning on the date and time a certificate is issued (or later if specified in the certificate) and ending with the date and time on which the certificate expires or is revoked.

Verify (a digital signature)
To accurately determine that:
- The digital signature was created during the certificate's validity period by the private key corresponding to the public key contained in the certificate.
- The message has not been modified since the creation of the digital signature.

Violation
A violation (or suspected violation) of a security measure (i.e. confidential information was or possible was disclosed or control of this information was lost).

W / X / Y / Z

World Wide Web (WWW)
A hyper-text based, distributed information system in which users may create, edit, or browse hypertext documents. Graphic publication media and document viewing.

Writing
Information in a record that is accessible and useable for future reference

X.509
The ITU-T (International Telecommunications Union-T) standard for certificates. Designates certificates containing or capable of containing extensions.