

KEYNECTIS

Root CA Certification Policy

Date : 16/04/2009

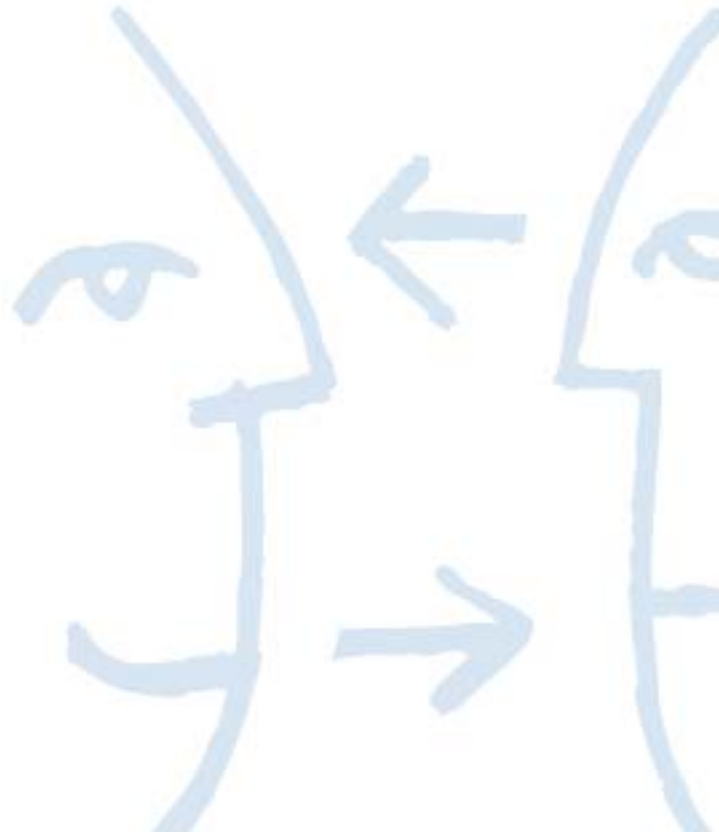
ROOT CA CERTIFICATION POLICY

Subject : Root CA certification policy

Version number :	0.6	Number of pages :	43
Status :	<input type="checkbox"/> Project	<input checked="" type="checkbox"/> Final version	
Writer :	Emmanuel MONTACUTELLI	KEYNECTIS	

Mailing list :	<input checked="" type="checkbox"/> External	<input checked="" type="checkbox"/> Internal KEYNECTIS
Certificate users		KEYNECTIS

Document history :				
Date	Version	Writer	Comments	Validated by
12/12/07	0.1	EM	Modification of the document	JYF
19/05/08	0.2	JYF	Revision	EM
06/06/08	0.3	EM	Integration of comments	JYF
19/11/08	0.4	EM	Integration of comments	JYF
20/11/08	0.5	EM	Integration of comments	JYF
16/04/09	0.6	JYF	Change KEYNECTIS Address	EM



SUMMARY

1	INTRODUCTION	8
1.1	Overview	8
1.2	Document name and Identification	9
1.3	PKI Participants	9
1.3.1	KEYNECTIS Management Authority (KMA)	9
1.3.2	Root Certificate Authority (RCA)	10
1.3.3	Certification Authorities (CA)	10
1.3.4	Registration Authorities (RA)	10
1.3.5	Publication Service (PS)	10
1.3.6	Other Participants	10
1.4	Certificate Usage	11
1.4.2	Prohibited Certificate Uses	11
1.5	Policy Administration	11
1.5.1	Organization Administering the Document	11
1.5.2	Contact Person	11
1.5.3	Person Determining CP Suitability for the Policy	12
1.5.4	CPS Approval Procedure	12
1.6	Definitions and Acronyms	12
1.6.1	Definitions	12
1.6.2	Acronyms	15
2	PUBLICATION AND REPOSITORY RESPONSIBILITIES	16
2.1	Repositories	16
2.2	Publication of Certificate Information	16
2.3	Time or Frequency of Publication	16
2.4	Access Controls on Repositories	16
3	IDENTIFICATION AND AUTHENTICATION	16
3.1	Naming	16
3.1.1	Type of Names	16
3.1.2	Need for Names to be Meaningful	17
3.1.3	Anonymity or pseudonym of Subscribers	17
3.1.4	Rules for Interpreting Various Name Forms	17
3.1.5	Uniqueness of Names	17
3.1.6	Recognition, Authentication, and Role of Trademarks	17
3.2	Initial Identity Validation	17
3.2.1	Method to Prove Possession of Private Key	17
3.2.2	Authentication of Organization identity	17
3.2.3	Authentication of Individual identity	18
3.2.4	Non-Verified Subscriber information	18
3.2.5	Validation of Authority	18
3.2.6	Criteria for Interoperation	18
3.3	Identification and Authentication for Re-key Requests	18
3.3.1	Identification and Authentication for Routine Re-key	18
3.3.2	Identification and Authentication for Re-key After Revocation	18
3.4	Identification and Authentication for Revocation Request	19
4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	19
4.1	Certificate Application	19
4.1.1	Origin of a certificate request	19
4.1.2	Enrolment Process and Responsibilities	19
4.2	Certificate Application Processing	19
4.2.1	Performing Identification and Authentication Functions	19
4.2.2	Approval or Rejection of Certificate Applications	20
4.2.3	Time to Process Certificate Applications	20

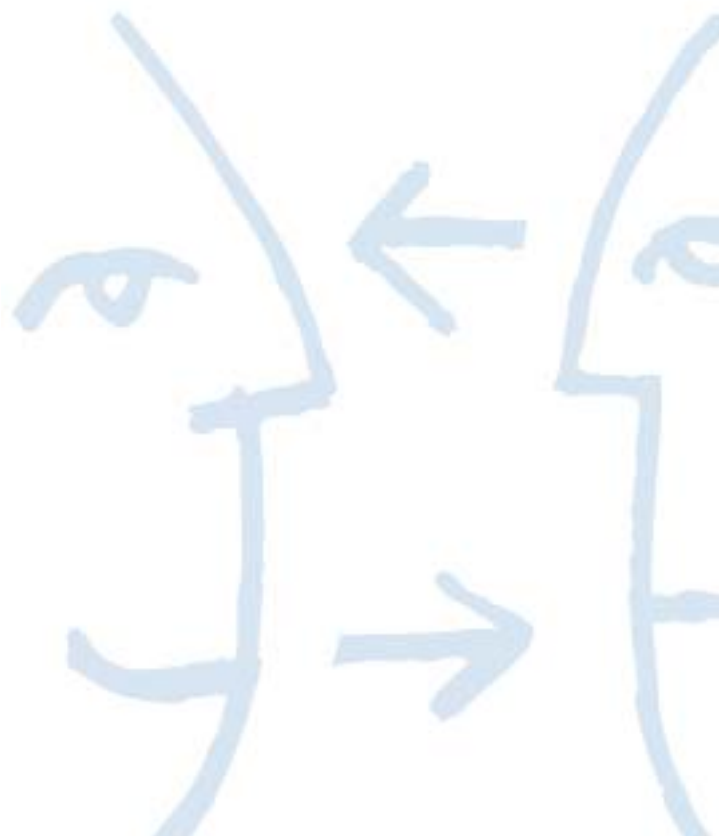
4.3	Certificate Issuance	20
4.3.1	CA Actions during Certificate Issuance	20
4.3.2	Notifications to Subscriber by the CA of Issuance of Certificate	20
4.4	Certificate Acceptance	20
4.4.1	Conduct Constituting Certificate Acceptance	20
4.4.2	Publication of the Certificate by the CA	20
4.4.3	Notification of Certificate Issuance by the CA to Other Entities.....	21
4.5	Key Pair and Certificate Usage	21
4.5.1	CA Private Key and Certificate Usage	21
4.5.2	Relying Party Public Key and Certificate Usage	21
4.6	Certificate Renewal	21
4.7	Certificate Re-Key	21
4.8	Certificate Modification	21
4.9	Certificate Revocation and Suspension	21
4.9.1	Circumstances for Revocation	21
4.9.2	Origin of Revocation Request	22
4.9.3	Procedure for Revocation Request.....	22
4.9.4	Revocation Request Grace Period	23
4.9.5	Time within Which CA Must Process the Revocation Request	23
4.9.6	Revocation Checking Requirements for Relying Parties	23
4.9.7	ARL Issuance Frequency.....	23
4.9.8	Maximum Latency for ARLs.....	23
4.9.9	On-Line Revocation/Status Checking Availability.....	23
4.9.10	On-Line Revocation Checking Requirements.....	23
4.9.11	Other Forms of Revocation Advertisements Available	23
4.9.12	Special Requirements regarding Key Compromise.....	24
4.9.13	Circumstances for Suspension	24
4.9.14	Who Can Request Suspension.....	24
4.9.15	Procedure for Suspension Request.....	24
4.9.16	Limits on Suspension Period	24
4.10	Certificate Status Services	24
4.10.1	Operational Characteristics.....	24
4.10.2	Service Availability	24
4.10.3	Optional Features	24
4.11	End of Subscription	24
4.12	Key Escrow and Recovery	24
5	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	24
5.1	Physical Controls	24
5.1.1	Site Location and Construction	25
5.1.2	Physical Access	25
5.1.3	Power and Air Conditioning	25
5.1.4	Water Exposures	25
5.1.5	Fire Prevention and Protection	25
5.1.6	Media Storage.....	25
5.1.7	Waste Disposal	25
5.1.8	Off-Site Backup.....	25
5.2	Procedural Controls	26
5.2.1	Trusted Roles.....	26
5.2.2	Number of Persons Required per Task	26
5.2.3	Identification and Authentication for Each Role	26
5.2.4	Roles Requiring Separation of Duties.....	26
5.3	Personnel Controls	27
5.3.1	Qualifications, Experience, and Clearance Requirements	27
5.3.2	Background Check Procedures	27
5.3.3	Training Requirements.....	27
5.3.4	Retraining Frequency and Requirements	27
5.3.5	Job Rotation Frequency and Sequence	27
5.3.6	Sanctions for Unauthorized Actions.....	28
5.3.7	Independent Contractor Requirements.....	28
5.3.8	Documentation Supplied to Personnel	28

5.4	Audit Logging Procedures	28
5.4.1	Types of Events Recorded	28
5.4.2	CA	28
5.4.3	Frequency of Processing Log	28
5.4.4	Retention Period for Audit Log	29
5.4.5	Protection of Audit Log	29
5.4.6	Audit Log Backup Procedures	29
5.4.7	Audit Collection System	29
5.4.8	Notification to Event-Causing Subject	29
5.4.9	Vulnerability Assessments	29
5.5	Records Archival	29
5.5.1	Types of Records Archived	29
5.5.2	Retention Period for Archive	30
5.5.3	Protection of Archive	30
5.5.4	Archive Backup Procedures	30
5.5.5	Requirements for Time-Stamping of Records	30
5.5.6	Archive Collection System (Internal or External)	30
5.5.7	Procedures to Obtain and Verify Archive Information	30
5.6	Key Changeover	30
5.6.1	RCA	30
5.6.2	CA	30
5.7	Compromise and Disaster Recovery	31
5.7.1	Incident and Compromise Handling Procedures	31
5.7.2	Computing resources, software, and/or data are corrupted	31
5.7.3	Entity private key compromise procedures	31
5.7.4	Business continuity capabilities after a Disaster	32
5.8	RCA component termination	32
6	TECHNICAL SECURITY CONTROLS	32
6.1	Key Pair Generation and Installation	32
6.1.1	Key Pair Generation	32
6.1.2	Private Key Delivery to CA	32
6.1.3	Public Key Delivery to Certificate Issuer	32
6.1.4	CA Public Key Delivery to Relying Parties	32
6.1.5	Key Sizes	32
6.1.6	Public Key Parameters Generation and Quality Checking	33
6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field)	33
6.2	Private Key Protection and Cryptographic Module Engineering	33
6.2.1	Cryptographic Module Standards and Controls	33
6.2.2	Private Key (m out of n) Multi-Person Control	33
6.2.3	Private Key Escrow	33
6.2.4	Private Key Backup	33
6.2.5	Private Key Archival	33
6.2.6	Private Key Transfer Into or From a Cryptographic Module	33
6.2.7	Private Key Storage on Cryptographic Module	33
6.2.8	Method of Activating Private Key	33
6.2.9	Method of Deactivating Private Key	34
6.2.10	Method of Destroying Private Key	34
6.2.11	Cryptographic Module Rating	34
6.3	Other Aspects of Key Pair Management	34
6.3.1	Public Key Archival	34
6.3.2	Certificate Operational Periods and Key Pair Usage Periods	34
6.4	Activation Data	34
6.4.1	Activation Data Generation and Installation	34
6.4.2	Activation Data Protection	34
6.4.3	Other Aspects of Activation Data	35
6.5	Computer Security Controls	35
6.5.1	Specific Computer Security Technical Requirements	35
6.5.2	Computer Security Rating	35
6.6	Life Cycle Technical Controls	35
6.6.1	System Development Controls	35

6.6.2	Security Management Controls.....	36
6.6.3	Life Cycle Security Controls.....	36
6.7	Network Security Controls	36
6.7.1	RCA.....	36
6.7.2	CA	36
6.8	Time-Stamping.....	36
7	CERTIFICATE, ARL, AND OCSP PROFILES	36
7.1	Certificate Profile.....	36
7.1.1	Certificate Extensions	36
7.1.2	Algorithm Object Identifiers.....	36
7.1.3	Name Forms	37
7.1.4	Certificate Policy Object Identifier.....	37
7.1.5	Usage of Policy Constraints Extension.....	37
7.1.6	7.1.8 Policy Qualifiers Syntax and Semantics	37
7.1.7	Processing Semantics for the Critical Certificate Policies Extension	37
7.2	ARL Profile.....	37
7.2.1	ARL and ARL Entry Extensions	37
7.3	OCSP Profile	37
7.3.1	Version Number(s).....	37
7.3.2	OCSP Extensions	37
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	37
8.1	Frequency and Circumstances of Assessment	37
8.2	Identity/Qualifications of Assessor	38
8.3	Assessor's Relationship to Assessed Entity	38
8.4	Topics Covered by Assessment.....	38
8.5	Actions Taken as a Result of Deficiency	38
8.6	Communications of Results.....	38
9	OTHER BUSINESS AND LEGAL MATTERS	38
9.1	Fees.....	38
9.1.1	Certificate Issuance or Renewal Fees	38
9.1.2	Certificate Access Fees	38
9.1.3	Revocation or Status Information Access Fees.....	38
9.1.4	Fees for Other Services	39
9.1.5	Refund Policy.....	39
9.2	Financial Responsibility	39
9.2.1	Insurance Coverage.....	39
9.2.2	Other Assets	39
9.2.3	Insurance or Warranty Coverage for End-Entities	39
9.3	Confidentiality of Business Information	39
9.3.1	Scope of Confidential Information.....	39
9.3.2	Information Not Within the Scope of Confidential Information.....	39
9.3.3	Responsibility to Protect Confidential Information	39
9.4	Privacy of Personal Information	39
9.4.1	Privacy Plan	39
9.4.2	Information Treated as Private.....	40
9.4.3	Information Not Deemed Private.....	40
9.4.4	Responsibility to Protect Private Information	40
9.4.5	Notice and Consent to Use Private Information.....	40
9.4.6	Disclosure Pursuant to Judicial or Administrative Process.....	40
9.4.7	Other Information Disclosure Circumstances	40
9.5	Intellectual Property rights.....	40
9.6	Representations and Warranties	40
9.6.1	RCA Representations and Warranties.....	40
9.6.2	CA Representations and Warranties	41
9.6.3	KMA Representations and Warranties	41
9.6.4	Representations and Warranties of Other Participants	41
9.7	Disclaimers of Warranties	41



9.8	Liability limitation	41
9.9	Indemnities	41
9.10	Term and Termination	42
9.10.1	Term	42
9.10.2	Termination	42
9.10.3	Effect of Termination and Survival	42
9.11	Individual Notices and Communications with Participants	42
9.12	Amendments	42
9.12.1	Procedure for Amendment	42
9.12.2	Notification Mechanism and Period	42
9.12.3	Circumstances under Which OID Must be Changed	42
9.13	Dispute Resolution Provisions	42
9.14	Governing Law	42
9.15	Compliance with Applicable Law	43
9.16	Miscellaneous Provisions	43
9.16.1	Entire Agreement	43
9.16.2	Assignment	43
9.16.3	Severability	43
9.16.4	Waiver of Rights	43
9.16.5	Act of god	43
9.17	Other Provisions	43



1 INTRODUCTION

1.1 Overview

KEYNECTIS is the leading certification services provider in France. KEYNECTIS Company was born from the merging of 2 trust services operators: Certplus and PK7. Created in 1998 on the initiative of Gemplus, VeriSign, France Telecom and Matra Hautes Technologies (later EADS), Certplus was the first French trust services manufacturer to become also a trust services operator. Created in February 2000 by La Poste and Sagem in the form of a simplified joint stock company, PK7 specialized in the technical trade of Certification Services Operator, while retaining and developing a technical and legal expertise in the field of electronic signatures.

The birth of KEYNECTIS, in 2004, is due to 2 requirements:

- Create a technological infrastructure meeting the needs of major projects
- Establish a hub of expertise acknowledged at the European level and able to address the concentration of market players

In order to provide its trust services, KEYNECTIS benefits from a dedicated operation center. Like any other industrial site, the KEYNECTIS production site is being carefully monitored and continuously improved. Dedicated to the trust operator trade, it must take all developments into account, whether in the technical field or in that of applicable legislation (labour law, provisions for new technologies, etc.).

To this end, KEYNECTIS has, since its creation, performed and updated the required risk analyses concerning the certification operator's trade. It selected the EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) methodology, which was initially developed by DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) to cater for the French government's needs in this field.

Today, KEYNECTIS Center is ETSI 101 456 TS certified regarding the European directive on electronic signature. This certification was established by an accredited company, under the COFRAC (French Accreditation Comity) authority, auditing KEYNECTIS Trust Center regarding the Certificate Policy (CP) to manage and deliver qualified certificate for electronic signature purpose.

KEYNECTIS manages PKI (Public Key Infrastructures) services to issue different types of X. 509 digital certificates as an answer to various customers needs (intranet, extranet, business applications ...).

To that way, KEYNECTIS operates a Root Certification Authority (RCA) that certifies CA able to deliver certificates according to trusted services security standards (KEYNECTIS SSL CP, EV SSL CP, ETSI 101456 and 101 042 certificate policy requirements, PRIS ...) defined and/or recognised by KEYNECTIS.

This certificate policy (CP), also called RCA CP, presents the requirements, principles and procedures the KEYNECTIS RCA implements to certify Certification Authority (CA). A CA that is certified by the KEYNECTIS RCA (named RCA in this document) has to enforce the present CP. Prior to certify a CA, the KEYNECTIS RCA verifies that the CA that request certification supports a CP defined and/or recognised by KEYNECTIS. Both represent the common shared requirements that a CA has to respect to be signed by the RCA. The present CP defines objectives and requirements for the practise (business, legal, and technical) employed by the RCA to provide certification services that covers X.509 digital certificate life cycle, including enrolment, issuance, renewal and revocation of digital certificates. The present CP defines also objectives and requirements for the practise (legal, organisational and technical) employed by the CA to create and protect the CA private key.

By this way, the RCA creates the root of common trust shared identities community between organisation and their Internet customers. The KEYNECTIS RCA owns a self-signed certificate and represents the common anchor of all trusted link (certification path) created by the CA that were certified by the RCA and the certificates they deliver. The trusted links are built as follow:

- RCA trust common anchor: self-signed RCA certificate generated and managed by KEYNECTIS according to the RCA CP;
- CA certificate: certificate delivered by the RCA according to the RCA CP;
- End users certificate: certificates delivered by CAs according to their CPs.



The RCA certificate is available in all browsers and all messaging software to simplify recognition of all issued CA certificates. Be signed by the RCA means that the CA will be recognized everywhere, at anytime, in the Internet relationships with the same level of trust.

Each CA has to develop its own CP/CPS (Certificate Practise Statement). All CA certificates, managed by the RCA according this CP, will represent only one level of trust shared by all the partners and trusted by Internet customers.

The present CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practise Statement Framework.

1.2 Document name and Identification

This CP is the KEYNECTIS property. This CP has a registered policy object identifier (OID) that is: 1.3.6.1.4.1.22234.2.5.1.1.2.

1.3 PKI Participants

KEYNECTIS operates the RCA in his dedicated trust center. For this purpose KEYNECTIS has established a KMA to manage the RCA and the CA candidates. To host, operate the RCA and certify and host (when relevant) the CA, KEYNECTIS deploys a PKI. For the CA certificate issuance activity delivered by the RCA, this PKI is composed of the components described below and supports the following services:

- Generation of RCA key: KEYNECTIS operates the RCA and generates the RCA keys in its trust center during an operation called "Key ceremony";
- Generation of RCA certificate: KEYNECTIS operates the RCA and generates the RCA certificate in its trust center during an operation called "Key ceremony";
- Authentication of CA: KEYNECTIS collects and verifies each CA identity and information that will be included in the public key certificate to be delivered. This service is supported by an authority called RA that is hosted and managed by KEYNECTIS in its trust center;
- Establishing CA compliance: prior to the generation of a CA certificate by the RCA, KEYNECTIS determines the mapping between the CA CP/CPS and the RCA CP. This task is performed by the KMA in the KEYNECTIS trust center;
- Generation of CA certificate: when the CA CP/CPS enforces the RCA CP requirements and is compliant with an recognized CP, the RA owns all the necessary information and had successfully proceeded to all required checks, the RCA certifies the CA and generates a CA digital certificate according to the RCA CP. This operation is performed by the RCA in the KEYNECTIS trust center;
- Revocation of CA certificate: when the link between the CA and CA public key defined within the certificate delivered by the RCA is considered no longer valid, then the RCA revokes the CA certificate. This operation is performed by the RCA in the KEYNECTIS Trust Center;
- Renewal and Re-key of CA certificate: action of delivering a new certificate to the CA, renewing a CA certificate means creating a new certificate for the CA with the same or different information (key, name ...) as the previous one, Re-keying a certificate means creating a new certificate for the CA with a new public key. This operation is performed by the RCA in the KEYNECTIS trust center;
- Publication services: the RCA certificate, all the CA certificates and corresponding ARL are published by the KEYNECTIS Publication Service (PS). In the meantime, the RCA certificate is provided to main browsers and messaging software developers (Microsoft, Mozilla foundation...) by KEYNECTIS to be published in these software.

The RCA CP gives the security requirements for all the described services, the RCA CPS will give more details on the practices enforced by each entity participating to the RCA activities.

1.3.1 KEYNECTIS Management Authority (KMA)

The KMA defines and approves the RCA CP. The KMA proceeds to the mapping of:

- The RCA CPS with the present CP: the result of the mapping guarantees that the RCA operates in compliance with its CP. The result of the compliance review is validated by the KMA;
- The candidate CA CP/CPS with the present CP: the result of the mapping guarantees that the CA operates in compliance with the present CP. The result of the compliance review is validated by the KMA;
- The CA CP/CPS with a KEYNECTIS recognized trusted service security standard: the result of the mapping guarantees that the CA operates in compliance with the trusted service security standard. The result of the compliance review is validated by the KMA.

KEYNECTIS benefits from a specific audit framework to audit the RCA and the CA. If the CA has a positive audit result (i.e. its CP/CPS perimeter covers the same perimeter than the RCA CP, then the audit result will be acceptable by the KMA).

All the KMA decisions and approvals made by the KMA have to be approved by the KEYNECTIS' board. For example the certification of a new CA by the RCA will have to be prior approved by the KEYNECTIS board.

1.3.2 Root Certificate Authority (RCA)

The RCA is a public root CA operated by KEYNECTIS. The RCA signs and revokes certificates for CA. In this CP, when the term 'RCA' is used without reference to any component (RA, Publication Service...) it covers the overall deployed PKI, dealing with legal and business matters. The RCA supports the PKI services as described above. The RCA uses the service of the RA to authenticate and identify the CA for certificates request, revocation request and certificate renewal and re-key request. The RCA uses the publication service to publish the certificates and the ARL that it generates. The RCA operates its services according to the Root CA CP and the corresponding CPS. The RCA cannot start operation without prior approval of the KMA.

1.3.3 Certification Authorities (CA)

In the present document, a CA is a Certification Authority that generates certificates for its own customers (users belonging to the organisation, partners, suppliers) and allows its own customers to have trust communications in a trusted community using certificates signed by the same RCA. If the KMA approves the CA certificate request, the CA is signed by the RCA.

KEYNECTIS may host and operate the CA, on the opposite the CA may be operated by another trusted service provider. In any cases the CA have to provide its CP/CPS to the KMA for mapping, thought the RA, to comply with the process. The CA implements its own CPS for its PKI operations and provides a CPS that is compliant with the RCA CP and the CA CP.

If the CA is not a self-signed CA, means that belongs to a PKI hierarchy, the CA has only to provide a CP/CPS of the CA that request a certificate to the RCA. The KMA will determine the acceptance of the mapping review regarding the perimeter and the commitment of the CA.

In any case, the CA has to declare to the RCA the type of certificate it delivers. The RCA deliver a CA certificate to the CA that has to be used only the type of certificate declared in the CP the KMA had reviewed.

1.3.4 Registration Authorities (RA)

A RA is an entity that delivers CA authentication services for the RCA according to the RCA CP. The RA identifies and checks the identity of the CA that request a certificate and prepares all the necessary forms for the KMA approval process.

1.3.5 Publication Service (PS)

The PS is an entity that makes available information such as RCA CP and ARL.

1.3.6 Other Participants

1.3.6.1 Relying Party (RP)

A Relying Party is an entity that relies on the validity of the binding of the CA's name to a public key. A Relying Party is responsible for deciding how to check the validity of a CA Certificate, at least by checking the appropriate certificate status information. A Relying Party may use information in the Certificate (such as Certificate Policy identifiers) to determine the suitability of the Certificate for a particular use.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

1.4.1.1 CA certificate

The CA certificate is used to sign X.509 certificates, CRL and/or ARL according to the CP of the CA. The CA certificate is used to authenticate the certificate, CRL and/or ARL delivered by the CA.

1.4.1.2 Root CA certificate

The Root CA is used to sign its X.509 RCA CA self signed certificate, X.509 CA certificate and ARL according the present CP.

The Root CA certificate is used by relying party to check and verify the identity of a CA.

1.4.2 Prohibited Certificate Uses

No other application (means different certificate format or different CA function) than the one stated in § 1.4.1.1 and § 1.4.1.2 above are covered by the RCA CP.

A CA, which owns a CA certificate issued by the RCA, is not authorized to use this certificate to:

- Deliver certificates that are not X.509 compliant,
- To deliver functions that are not covered by the RCA CP,
- To provide services that are not declared to the RCA at the time the RCA was provided the CA CP/CPS, unless it has provided with an additional request (including an updated CP/CPS) and that this additional request has been approved by the KMA.

KEYNECTIS is not responsible for any other use that these stated in the RCA CP

Certificates shall only be used in line with the applicable law, and in particular shall only be used to the extent permitted by applicable export or import laws. CA Certificates shall not be used for any functions except CA functions.

KEYNECTIS is not responsible for the use of CA function in delivering end users certificates to customers.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The KMA is responsible for all aspects of this CP.

1.5.2 Contact Person

The Certificate Policy Manager is responsible for the KMA

KEYNECTIS

Contact: Security and Quality Director

11-13 rue René Jacques – 92131 Issy les Moulineaux Cedex FRANCE

Phone : +33 (0)1 55 64 22 00

Fax : +33 (0)1 53 64 22 01

info@keynectis.com

1.5.3 Person Determining CP Suitability for the Policy

The KMA approves the RCA CPS and determines compliance of CA CP/CPS. Entities will be required to attest to such compliance periodically as established by the KMA. Further, the KMA reserves the right to audit entity compliance as set in section 8 of the RCA CP and in the contract between KEYNECTIS and the CA.

In each case, the determination of suitability shall be based on an independent compliance audit report and recommendations and/or by the KMA expert. See section 8 for definition of independent compliance auditor.

1.5.4 CPS Approval Procedure

The term CPS is defined in the Internet RFC 3647, X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework as: "A statement of the practices, which a Certification Authority employs in issuing certificates". It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management. It shall be more detailed than the corresponding CP described above.

The KMA approves and maintains the RCA CPS. The CA Entity is responsible for the elaboration, approval and maintenance of the CA CP/CPS.

The RCA CPS and CA CP/CPS, which are separate documents, are published where necessary by the KMA for the RCA CPS and by the CA Entity for the CA CP/CPS. The KMA approves the results of the review made by KMA experts or independent auditors on the CA CPS compliance with the RCA CP based on the CA CP/CPS.

Amendments shall either be in the form of a new CP/CPS (with a sum up of the modifications). The new version of CP/CPS replaces automatically the previous one and becomes operational as soon as the KMA has established its agreement on the mapping result. A new version of CP/CPS has to be still compliant with the present CP to permit the RCA and CA to refer to this CP/CPS and deliver certificates.

1.6 Definitions and Acronyms

1.6.1 Definitions

Activation data: Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a pass phrase, or a manually-held key share).

Administrative contact: the CA Entity representative that is authorized to act on behalf of the CA Entity for all interaction with the RCA (transmission of requests to the RA...).

Audit: Independent review and examination of system records and activities to assess the adequacy and effectiveness of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [ISO/IEC POSIX Security]

Authority Revocation List (ARL): A list digitally signed by a CA, and contains certificates identities that are no longer valid. The list contains the issuing CA identity, the date of issue and the revoked certificates serial numbers.

Availability: The property of being accessible and upon demand by an authorized entity [ISO/IEC 13335-1:2004].

Certificate: The public key of a customer, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it [ISO/IEC 9594-8; ITU-T X.509]. In this context, the certificates for the customers are certificates used by server to establish SSL connexion with a certified DN. The certificate contains the Fully Qualified Domain Name (FQDN) that belongs to the customer.

CA-certificate: A certificate for one CA issued by another CA. [ISO/IEC 9594-8; ITU-T X.509]. In this context, the CA-certificates are RCA-certificate (self-signed certificate) and CA-certificate (sign by the RCA).

CA activation data: a set of m (fixed integer that is determine in the CPS) activation data (portion of key, secret PIN ...) that are used to activate the CA private key. The CPS define the number of n ($n > 1$) necessary activation data that are sufficient to activate the CA private key. Actually a single activation data can't be use to activate the



CA private key pair. All the m activation data are given to m authorized person that have to protect it in confidentiality and integrity.

CA Entity: A trusted third Entity that owns a CA certificate signed by the RCA and which is in a contractual relationship with KEYNECTIS.

CA Entity representative: a legally authorized representative of the CA Entity, that has rights to nominate the administrative contact..

Certificate Policies (CP): A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. [ISO/IEC 9594-8; ITU-T X.509]. The present document is the Root CA CP and is applicable to all CA that are signed by the RCA.

Certificate Request: A message transmitted by the RA to the RCA to have a CA-certificate delivered by the RCA.

Certification Authority (CA): An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users. Keys [ISO/IEC 9594-8; ITU-T X.509]. In this CP, the term CA is used to deal with the CA belongs to an Entity which wants to be signed by the RCA.

Certification Practice Statement (CPS)

A statement of the practices that KEYNECTIS (acting as a Certification Authority) employs in approving or rejecting Certificate Applications (issuance, management, renewal and revocation of certificates). [RFC 3647]

Certificate validity period: The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. [RFC 3280].

Certification Path: A chain of multiple certificates needed to validate a certificate containing the required public key. A certificate chain consists of a RCA-certificate, CA-certificate and the end user certificates signed by the CA.

Compromise: A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO/IEC 13335-1:2004].

CRL distribution point: A directory entry or other distribution source for CRLs (ARL); a CRL or ARL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs. [ISO/IEC 9594-8; ITU-T X.509].

Cryptographic modules: a set of software and hardware components that are used to operate private cryptographic key to enable cryptographic operations (signature, encryption, authentication, key generation ...). When a cryptographic module stores private key it needs an activation data to activate the private key stored inside. For a CA, a cryptographic module is a Hardware Secure Module evaluated (FIPS or EAL) that is used to store and operate the CA private key.

Customer: An organization requiring a end user certificate signed by the CA. A customer is able to use and is authorized to use, the private key that corresponds to the public key listed in the Certificate.

Disaster Recovery Plan: A plan defined by a CA to recover its all or part of PKI services, after they've been destroyed following a disaster, in a delay define in the CP/CPS.

Hash function: A function which maps string of bits to fixed-length strings of bits, satisfying the following two properties:

- It is computationally infeasible to find for a given output an input which maps to this output;
- It is computationally infeasible to find for a given input a second input which maps to the same output [ISO/IEC 10118-1].

Integrity: Refers to the correctness of information, of originator of the information, and the functioning of the system which processes it.

Interoperability: Implies that equipment and procedures in use by two or more entities are compatible, and hence that it is possible to undertake common or related activities.

KMA: Describes the authoritative body within KEYNECTIS with all of the following functions with respect to the implementation and management of a PKI:

- Establishing and administering the set of security policies (procedures, root CA CP and associated RCA CPS) supported by the RCA;
- Approving policy mapping between the CA Entity and KEYNECTIS requirements CP;
- Oversighting the operation of the RCA;
- Choose the trusted service security standard to be used as a basis for the review of the CA CP/CPS.

The KMA doesn't have final decision to enter in a contractual relationship with the Entity CA. This decision is submitted to the KEYNECTIS board which is composed of the KEYNECTIS directors.

Key Ceremony A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.

KEYNECTIS Trust Center: The initial purpose of the KEYNECTIS Trust Center and resources operated by KEYNECTIS is the management of digital certificates life cycle. In practice, they reach much further and also support on their own the comprehensive establishment of your areas of trust and the generation of the required elements of proof. These services include:

- Management of the certificate authorities life cycle;
- Management of the digital certificates life cycle;
- Publication of the elements associated to those life cycles' management;
- Production of time stamps;
- Customization of smart cards and other USB cryptographic tokens;
- Verification of digital certificate validity status
- Verification of electronic signatures validity ...

Mapping process: Process established by the KMA to determine if a CA is compliant with the RCA CP and the trusted service security standard. To realize the process, the KMA uses the present CP and documents from the trusted service security standard as the set of reference of KEYNECTIS requirements for CA certificates services. The KMA maps the CP/CPS provided by the Entity for its CA with the set of reference documentation. The KMA checks for any difference and decides whether there is or not differences with the set of reference documentation. The RCA and CA have to provide an audit result on the perimeter defined in the RCA CP. The audit result can come from the WebTrust CA audit process, ETSI TS 101 456 and 101 042 certification practice statements, CSP qualification process and/or other audit process defined by institution such as government (for example in France, KMA accepts the PRIS audit scheme and the TélÉTVA audit scheme). In particular, KMA defines a special training program and audit framework to audit if the CA respects the registration procedures of a certificate request in compliance with the generics defined by KEYNECTIS.

Online Certificate Status Protocol (OCSP): A protocol for providing Relying Parties with real-time Certificate status information.

PKCS #10 Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.

Policy qualifier: Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate. [RFC 3647]

Private key: That key of an entity's asymmetric key pair which should only be used by that entity [ISO/IEC 9798-1].

Public key: That key of an entity's asymmetric key pair which can be made public. [ISO/IEC 9798-1]

Public Key Infrastructure (PKI): The infrastructure needed to generate, distribute, manage and archive keys, certificates and certificate-revocation lists and the repository to which certificates and CRLs are to be posted. [2nd DIS ISO/IEC 11770-3 (08/1997)]



Publication Services: A service that disseminates information (such as CP) to customers and eventually to relying parties.

Registration Authority (RA): An entity acting for a RCA, the RA is in charge of identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Relying Party: An individual or organization that relies on a certificate and/or a digital signature. An user or agent that relies on the data in a certificate in making decisions. In the present context, a CA customers that trust the CA certificates, means he trusts the KEYNECTIS certification path, to have business relationship (access control on private network, trust server to transmit data ...) with end-users whose identities are included in the certificates delivered by the CA.

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

Root Certificate Authority (RCA): CA which has a self-signed CA certificate operated and managed by KEYNECTIS. The RCA manages CA certificate for Entities which own CA. The RCA-certificate is the common identity and public key trusted by all the internet customers to validate the certification path created according to the present CP.

Secure Socket Layer (SSL): The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.

Security policy: The set of rules laid down by the security authority governing the use and provision of security services and facilities [ISO/IEC 9594-8; ITU-T X.509]. In this context, the security policy will be set up by the Entity which host and operate CA.

Self-signed certificate: A certificate for one CA signed by that CA.

Token: The hardware device used to transport keys to an entity and which can protect those keys in operation [ISO/IEC 9798-1 (2nd edition): 1997].

Trustworthy System: Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.

Time stamping services: A service that provides a digitally signed assertion (a Digital Receipt) that a particular document or set of data existed at a particular point in time. Time Stamping Service: A service that provides a trusted association between a datum and a particular point in time, in order to establish reliable evidence indicating the time at which the datum existed.

1.6.2 Acronyms

ANSI: The American National Standards Institute;

ARL: Authority Revocation List;

CC: Common Criteria (ISO 15408 standard)

CP: Certificate Policy;

CPS: Certification Practice Statement;

CRL: Certificate Revocation List;

DN: Distinguished Name;

DNS: Domain Name Server;

EAL: Evaluation assurance level (pursuant to the Common Criteria);

FIPS: United State Federal Information Processing Standards;

HTTP: Hypertext Transport Protocol;

IP: Internet Protocol;

ISO: International Organisation for Standardization;

KMA: KEYNECTIS Management Authority;

KTS: KEYNECTIS Trust Center;
LDAP: Lightweight Directory Access Protocol;
OCSP: Online Certificate Status Protocol;
OID: Object Identifier;
PIN: Personal identification number;
PKCS: Public-Key Cryptography Standard;
PKI: Public Key Infrastructure;
PS: Publication Service;
RA: Registration Authority;
RCA: Root Certification Authority;
RFC: Request for comment;
RSA: Rivest, Shamir, Adleman (Public-Key Cryptosystem);
SHA: Secure Hash Algorithm (US Standard);
CA: Certificate Authority that delivers end user certificate to customer;
SSL: Secure Socket Layer;
URL: Uniform Resource Locator.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The RCA operates a repository (PS) to make available the information defined below to the CA, its customers and relying parties.

2.2 Publication of Certificate Information

The RCA and CA ensure that the terms and conditions of the CP, CPS as necessary (for instance on a need to know basis), and certificates are made available to customers and relying parties by their PS. RCA makes available the following information through its PS:

- Root CA CP;
- Root CA certificate;
- CA Certificate status (ARL).

These information are available through a durable means of communication and in readily understandable language at www.keynectis.com.

2.3 Time or Frequency of Publication

The information identified above at § 2.2 are available:

- Before service starts for initial RCA CP, no later than 48 hours after Root CA CP update is approved by the KMA for any RCA CP update;
- Before service starts for Root CA certificate;
- No later than 24 hours after generation for CA Certificate status (ARL).
- Before service starts for CA CP;
- Before service starts for initial CA certificates, no later than 48 hours after generation for CA certificate renewal or re-key ;
- No later than 24 hours after generation for Certificate status (CRL ...) of the certificates issued by CA.

2.4 Access Controls on Repositories

The PS ensures that the information is made available and protected in integrity and authenticity from unauthorised modification. Information is publicly and internationally available through the Internet. Any PKI Repository information not intended for public dissemination or modification is protected.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Type of Names

RCA and CA have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate subject name field and in accordance with RFC3280. For the CA, the organisation name (O of the DN) is the legal name of the Entity CA. The CPS gives all the details for the identity given to the RCA and for a CA.

If the CA Entity changes of identity, it has to inform RCA of its modification and the RCA has to verify the new identity according the section 3.2.2. Because of this modification, the CA Entity can be re-certified by the RCA or keep its hold identity and therefore the same certificate.

3.1.2 Need for Names to be Meaningful

The certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the person or object to which they are assigned in a meaningful way.

3.1.3 Anonymity or pseudonym of Subscribers

The identity used for the RCA and CA certificates is not a pseudonym or an anonymous name.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are self contained in the applicable certificate profile as defined in § 3.1.1 and 7.1.

3.1.5 Uniqueness of Names

The CA identity (refer to § 3.1.1) is unique for all certificates generated by the RCA. The RA ensures this uniqueness through its registration process (refer to § 3.2.2).

An CA Entity requesting a certificate from the RCA demonstrates its right to use a particular name for its identity. Where there is a dispute about a name for a certificate, the KMA is responsible for solving the name claim dispute resolution.

3.1.6 Recognition, Authentication, and Role of Trademarks

An CA Entity is not guaranteed that its name will contain a trademark if requested. The RCA is not obliged to research trademarks or resolve trademark disputes.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

RCA generates its key pair within the KEYNECTIS Trust Center and generates its self-signed certificates under trusted roles control. The KMA acknowledges the successful result of these operations.

CA generates its key pair in a manner that the CA Entity is ensured the CA owns the private key corresponding to the public key to be certified by the RCA. The RCA ensures that the CA owns the private key corresponding to the public key it request a certificate for using a PKCS#10 format file as certificate request.

3.2.2 Authentication of Organization identity

3.2.2.1 RCA

KEYNECTIS is the organization that owns the RCA.

3.2.2.2 CA Entity

A CA certificate request made on behalf of a CA Entity includes the organization name, address, and documents to prove existence of the Entity.

The RA checks the CA Entity ID information, authenticates the CA Entity representative that provides the certificate request and verifies his/her authorization to act on behalf of the Entity, using documents provided by authorized government bodies or relevant databases that has the ability to confirm the existence of the CA entity.

3.2.3 Authentication of Individual identity

3.2.3.1 RCA

Evidence of the Individual identity of the representative of the RCA is checked by the KMA against a physical person during a face to face meeting. Evidence of the individual is verified by RA using the national and legal identity card of the individual. Details on the authentication process are given in the RCA CPS.

3.2.3.2 CA

Evidence of the individual identity of the representative of the CA Entity is checked by the RA against a physical person during a face to face meeting. Evidence of the individual is verified by RA using the national and legal identity card of the individual. Details on the authentication process are given in the RCA CPS.

3.2.4 Non-Verified Subscriber information

Information that is not verified is not be included in Certificates.

3.2.5 Validation of Authority

3.2.5.1 RCA

The KMA authenticates the authorization and/or the authority of the RCA representative using the same procedure than the one described in sections 3.2.2 and 3.2.3. Details on the authentication process are given in the RCA CPS.

3.2.5.2 CA

The RA authenticates the authorization and/or the authority of the CA Entity representative with the same procedure than the one described in sections 3.2.2 and 3.2.3. Details on the authentication process are given in the RCA CPS.

3.2.6 Criteria for Interoperation

A CA which is certified by the RCA adheres to the following requirements:

- Having a CP/CPS determined by the KMA as compliant with the RCA CP;
- Operating a PKI that has undergone a successful compliance audit pursuant to section 8 of the RCA CP;
- Having a CP compliance with a trust service security standard recognized by KEYNECTIS;
- Issuing certificates and certificates status information available to the relying party, such as described in the CP of the CA that was reviewed by the KMA.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

A request for re-key may only be made by the organization in whose name the keys have been issued. The CA and RCA identify itself using the initial identity-proving process as described above. At each re-key request the identity of a CA, identified as required in § 3.2, is re-established through the initial registration process.

3.3.2 Identification and Authentication for Re-key After Revocation

After the RCA or a CA has been revoked other than during a renewal or update action, the CA and RCA is required to go through the initial registration process described in § 3.2 to obtain a new certificate.

If the RCA or CA has been revoked for key compromise, then the RCA or CA cannot use the revoked key to be certified again and needs the agreement of the organisation it belongs to generate a new key pair and be issued a new certificate.

3.4 Identification and Authentication for Revocation Request

RCA and CA revocation requests are respectively authenticated by the KMA for the RCA and the RA for the CA. The authentication procedure requires to go through the initial registration process (See § 3.2.2 and 3.2.3) to make sure the RCA or CA has effectively requested its RCA or CA certificate revocation.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Origin of a certificate request

KEYNECTIS KMA is in charge of requesting the RCA creation.
Only the authorized responsible of the CA Entity can make a certificate request to the KMA.

4.1.2 Enrolment Process and Responsibilities

4.1.2.1 Root CA

The RCA naming document, which is the application for a Root CA certificate is drafted by the KMA.

4.1.2.2 CA

The CA certificate request form for a CA certificate is composed of the following information:

- CA Entity identification data, i.e. full name and legal status of the associated legal person or other organizational entity and any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity;
- CA Entity representative personal identification, i.e. full name, including surname and given names, a nationally recognized identity number, or other attributes of the subject which may be used to, as far as possible, distinguish the person from others with the same name;
- Evidence that the CA Entity representative is associated with the legal person or other organizational entity;
- Name of the CA representative who will act as the Administrative contact for the RCA;
- Physical and electronic addresses, or other attributes, which describe how the PKI contact may be contacted.
- CA identification (Refer to § 3.1.1);
- Public key in PKCS#10 format;
- Content of the requested CA certificate;
- CP/CPS of the CA;
- Type of certificate to be delivered by the CA.

If the CA representative is different from the CA Entity representative (i.e. belongs to a separate entity) then evidence shall be provided that the representative is authorized to act on behalf of the CA Entity.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

4.2.1.1 Root CA

The KMA submit the RCA certificate creation request to the KEYNECTIS board of directors for approval. The RCA certificate creation or renewal request (composed of the RCA naming document) is signed by the KEYNECTIS Chief Executive Officer (CEO) that approves the creation a the RCA certificate.

The RA records all the given information to verify naming document and the naming document.

4.2.1.2 CA

The CA Entity representative (administrative contact) submits the CA certificate request form to the RA (refer to § 4.1.2) during a face to face meeting. The RA verifies that the information included in the CA certificate application is accurate and authenticates the CA Entity and its representative.

The RA records all the given information to verify the CA Entity identity and, if applicable, any specific attributes, including any reference number on the documentation used for verification, and any limitations on its validity.

4.2.2 Approval or Rejection of Certificate Applications

4.2.2.1 Root CA

Once the KEYNECTIS board of directors approves the RCA certificate request, the KEYNECTIS CEO signs the naming document. The RCA certificate creation or renewal is approved.

4.2.2.2 CA

If the certificate request form is complete and accurate had the RA successfully authenticated the requestor, then the RA transmits the CA certificate request form to the KMA for approval.

KMA maps the document with the present CP requirements (refer to § 1.5.3) and checks the audit result provided by the CA. The CPS provides details on the mapping process.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

RCA checks that the certificate to be signed contains all fields and extensions properly populated. RCA generates the RCA or CA certificate activating its private key using activation data.

All the operations are protected in a manner to guarantee the integrity, confidentiality (when it is necessary) and origin of transmitted data and secure link between operation and component.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

KMA notifies the KEYNECTIS board of directors of the RCA certificate issuance.

RCA notifies the CA and CA Entity of certificate issuance.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Notification of RCA issuance to the KEYNECTIS board of directors means acceptance of the RCA certificate by KEYNECTIS.

CA certificate acceptance is a paper or electronic document signed by the administrative contact of the CA Entity. This document is transmitted during a face-to-face meeting with a KMA representative or using secure communication. Once the CA certificate acceptance has been received by the KMA, the CA may start delivery of certificates to its customers.

4.4.2 Publication of the Certificate by the CA

The RCA uses KEYNECTIS PS for the publication of its certificate (refer to § 2.2)

The RCA transmits the CA certificate to the CA for publication (refer to § 2.2).

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 CA Private Key and Certificate Usage

The Root CA key pair is used to sign CA certificates, ARL and its own self-signed certificate.

The CA key pair is used to sign certificates and corresponding CRL for customer managed by the CA.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties use the trusted certification path and associated public keys for the purposes constrained in the certificates extensions (such as key usage, extended key usage, certificate policies, etc.) and to authenticate the trusted common identity of the services according to the present CP and the CP supported by the CA.

4.6 Certificate Renewal

This section addresses CA certificate generation without changing the public key or any other information in the certificate. Only the validity period and the serial number of the certificate are changed.

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised and the CA name and attributes are unchanged. This operation is possible only if the key re-used in the certificate is still compliant with cryptographic security recommendation for key size length issued by national bodies or international standard institutes.

The validity period of the new certificate cannot exceed the remaining lifetime of the private key, as specified in § 5.6. The RA proceeds to the check of the existence and validity status of the certificate to be renewed and authenticates organizations and individuals using the process described in § 3.2.2 and 3.2.3.

The procedures that apply are the same than the ones for initial certificate generation.

4.7 Certificate Re-Key

This section addresses RCA or CA certificate generation changing the RCA or CA key pair.

The procedures that apply are the same than the ones for initial certificate generation keeping the same identity for the CA as defined and used in the previous CA certificate delivered by the RCA.

4.8 Certificate Modification

This section addresses CA certificate generation of a new certificate keeping the same key pair. This operation is possible only if the key re-used in the certificate is still compliant with cryptographic security recommendation for key size length issued by national bodies or international standard institutes and has not been compromised.

Changing a CA Entity name is a possible circumstance for certificate modification.

The procedures that apply are the same than the ones for the initial certificate generation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 RCA

A RCA certificate is revoked when the binding between the certificate and the public key it contains is considered no longer valid. Examples of circumstances that invalidate this binding are:

- The private key is suspected of compromise;
- The private is compromised;
- The RCA can be shown to have violated the stipulations of the present CP;
- End of the RCA services;
- Privilege attributes asserted in the RCA certificate are reduced;
- Change in the key length size recommendation coming from national agencies or international standard institute;

Whenever any of the above circumstances occurs, the associated certificate shall be revoked and placed in the ARL.

4.9.1.2 CA

A CA certificate is revoked when the binding between the certificate and the public key it contains is considered no longer valid. Examples of circumstances that invalidate the binding are:

- The RCA is revoked.
- The private key is suspected of compromise or is compromised;
- The CA can be shown to have violated the stipulations of the present CP;
- The CA can be shown to have violated the stipulations of the CA CP;
- The CA can be shown to have violated the stipulations of its agreement with KEYNECTIS;
- End of the CA services;
- Privilege attributes asserted in the CA's certificate are reduced;
- Change in the key length size recommendation coming from national agencies or international standard institute;

Whenever any of the above circumstances occurs, the associated certificate shall be revoked and placed in the ARL.

4.9.2 Origin of Revocation Request

4.9.2.1 RCA

It is the responsibility of the KMA to propose the revocation of a RCA to the KEYNECTIS board of directors.

4.9.2.2 CA

It is the responsibility of the CA Entity administrative contact to request the revocation of a CA Entity certificate to the RA.

4.9.3 Procedure for Revocation Request

4.9.3.1 RCA

Once the KEYNECTIS board of directors receives the RCA certificate revocation request from the KMA, it reviews the request.

Once the RCA certificate revocation request is approved by the KEYNECTIS board of directors, the RCA revokes all the CA certificate.

4.9.3.2 CA

The authorized requestor transmits a revocation request which contains at minimum the following information:

- CA Entity identification data, i.e. full name;
- CA identification (Refer to § 3.1.1);
- Serial number of the CA certificate to be revoked;
- CA administrative contact identification, i.e. full name, including surname and given names;
- Physical and electronic address, or other attributes, which describe how the administrative contact may be reached;
- Optionally: revocation reason.

The RA authenticates the revocation request.

The RA transmits the revocation request to the RCA.

The RCA authenticates the RA and revokes the certificate using its key pair.

All the operations are protected in a manner to guarantee the integrity, confidentiality (when it is necessary) and origin of transmitted data and secure link between operation and component.

The CA of a revoked certificate is informed of the change of status of its certificate. Once a certificate is definitively revoked it is not re-certified. The corresponding CA private key has to be destroyed by the CA.

4.9.4 Revocation Request Grace Period

There is no revocation grace period. Responsible parties must request revocation as soon as they identify the need for revocation.

4.9.5 Time within Which CA Must Process the Revocation Request

Upon system failure, service or other factors which are not under the control of the RCA, the RCA makes best endeavours to ensure that this service is not unavailable for longer than a maximum period of time as denoted in the contract with the Entity CA. The RCA shall process a revocation request as soon as practical after receiving the revocation request and preferably immediately.

4.9.6 Revocation Checking Requirements for Relying Parties

Use of revoked certificates could have damaging or catastrophic consequences in certain applications for Internet customer acting as a relying party. The matter of how often new revocation data should be obtained is a determination to be made by relying parties. If it is temporarily infeasible to obtain revocation information, then the relying parties either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a certificate, i.e. certification path provided according to the present CP, whose authenticity cannot be guaranteed to the standards of this CP.

4.9.7 ARL Issuance Frequency

ARLs are issuance where necessary (i.e after being issued).

RCA ensures that superseded ARLs are removed from the repository upon posting of the latest ARL.

4.9.8 Maximum Latency for ARLs

The maximum delay between the time a CA certificate is revoked by the RCA and the time when revocation information is available to relying parties is no longer than 24 hours.

4.9.9 On-Line Revocation/Status Checking Availability

No stipulation.

4.9.10 On-Line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements regarding Key Compromise

There are no more specific requirements than those specified in section 4.9.3.

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The information status is available through the PS as described in section 2.

4.10.2 Service Availability

The PS availability is described in section 2.3.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

CA certificates that have expired prior to or upon end of subscription are not required to be revoked. Where the CA ends its relationship with KEYNECTIS, then the entire guarantee provided under the present CP on the CA certificate is not applicable.

It is the responsibility of the CA to keep the level of trust provided to the relying party by its own CP/CPS and CA certificate.

4.12 Key Escrow and Recovery

Under no circumstances the RCA or a CA key is escrowed by a third-party or any else other entity.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

All requirements and procedures applying to CA under the present section are identified in the applicable CP/CPS, unless specified in the present section.

5.1 Physical Controls

The RCA physical and environmental security policy for systems concerned with certificate generation, RCA cryptographic module operation and revocation management services address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure

collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery, etc. Controls are implemented to avoid loss, damage or compromise of assets and interruption to business activities and theft of information and information processing facilities.

5.1.1 Site Location and Construction

RCA critical and sensitive information processing facilities are housed in secure areas, protected by defined security perimeter, 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 RCA risk analysis.

RCA is located in the KEYNECTIS Trust Center in France.

5.1.2 Physical Access

5.1.2.1 RCA

The facilities concerned with certificate generation, RCA cryptographic module operation and revocation management are operated in an environment which physically protects the services from compromise through unauthorized access to systems or data. Any persons entering this physically secure area shall not be left for any significant period without oversight by an authorized person. Physical protections are achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate generation, RCA cryptographic module operation and revocation management services. Any parts of the premises shared with other organizations shall be outside this perimeter.

5.1.2.2 CA

The facilities concerned with certificate generation and use CA cryptographic module operation are operated in an environment which physically protects the CA's key from compromise through unauthorized access to systems or data. Any persons entering this physically secure area shall not be left for any significant period without oversight by an authorized person. Physical protections are achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the use CA cryptographic module operation. Any parts of the premises shared with other organizations shall be outside this perimeter.

5.1.3 Power and Air Conditioning

RCA ensures that the power and air conditioning facilities are sufficient to support the operation of the RCA system.

5.1.4 Water Exposures

RCA ensures that the RCA system is protected from water exposure.

5.1.5 Fire Prevention and Protection

RCA ensures that the RCA system is protected with a fire suppression system.

5.1.6 Media Storage

Media used within the RCA and CA are securely handled to protect media from damage, theft and unauthorized access. Media management procedures are protected against obsolescence and deterioration of media within the period of time that records are required to be retained. All media are handled securely and media containing sensitive data are securely destroyed when no longer required.

5.1.7 Waste Disposal

All media used for the storage of information such as keys, activation data or RCA files shall be destroyed before released for disposal.

5.1.8 Off-Site Backup

Full system backups of the RCA, sufficient to recover from system failure, are made periodically as described in the respective CPS. Back-up copies of essential business information and software are taken 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. Backup arrangements for individual systems are regularly tested to ensure that they meet the requirements of business continuity plans. At least one full backup copy is stored at an offsite location (at a location separate from the RCA equipment). The backup is stored at a site with physical and procedural controls commensurate to that of the operational RCA.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The functions performed in these roles form the basis of trust for all uses of the RCA.

Trusted roles include roles that involve the following responsibilities:

- Security Officer: Overalls responsibility for administering the implementation of the security practices;
- Administrator: Approves the generation/revocation/suspension of certificates;
- System Engineer: Authorized to install, configure and maintain the RCA trustworthy systems for registration, certificate generation, cryptographic module operation and revocation management;
- Operator: Responsible for operating the RCA trustworthy systems on a day to day basis. Authorized to perform system backup and recovery;
- Auditor: Authorized to view archives and audit logs of the RCA trustworthy systems;
- RCA activation data holder: Authorized person to have a RCA activation data that is necessary for cryptographic module operation.

5.2.2 Number of Persons Required per Task

5.2.2.1 RCA

The number of persons to provide the RCA services are describe in the CPS to guarantee the trust for all services of the RCA (key generation, certificate generation, revocation ...) so that any malicious activity would require collusion. Where multiparty control is required, at least one of the participants shall be an Administrator. All participants shall serve in a trusted role as defined in section 5.2.1.

5.2.2.2 CA

The number of person to provide key pair CA operation (generation, activation and destruction) services are at list under dual control.

5.2.3 Identification and Authentication for Each Role

5.2.3.1 RCA

Before to have a role in the RCA, the person has to be checked to verify and confirm that he is authorized and well authenticated.

Each person that has a role, as describe in the present CP, is identified and authenticated in a manner to guarantee that it is the right role supported by the right known person to perform the RCA services supported by a component. The CPS describes the mechanisms that are used to identify and authenticate role.

5.2.3.2 CA

Each person that has a role is identified and authenticated in a manner to guarantee that it is the right role supported by the right known person to perform the key pair CA operation services supported by a component dedicated to the generation, activation and destruction of CA key pair. The CA's CPS describes the mechanisms that are used to identify and authenticate role.

5.2.4 Roles Requiring Separation of Duties



Role separation may be enforced either by the RCA equipment, or procedurally, or by both means. Individual RCA personnel are specifically designated to the four roles defined in section 5.2.1 above. It is forbidden to have, at the same time, the following roles:

- Security officer and System Engineer or Operator;
- Auditor and Security Officer or Operator or Administrator or System Engineer;
- System Engineer and Operator;

No individual shall be assigned more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

RCA employs a sufficient number of personnel which possess the expert knowledge, experience and qualifications necessary for the offered services and appropriate for the job function. RCA personnel fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, actual experience, or a combination of the two. Trusted roles and responsibilities, as specified in the RCA CPS, are documented in job descriptions and clearly identified. RCA personnel (both temporary and permanent) have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. RCA personnel shall be formally appointed to trusted roles by senior management responsible for security.

The job descriptions include skills and experience requirements. Managerial personnel who are employed possess experience or training in electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

5.3.2 Background Check Procedures

All RCA personnel in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the RCA operations. The RCA shall not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position. Personnel shall not have access to the trusted functions until any necessary checks are completed. RCA asks the candidate to provide past convictions and turn down an application in case of refusal. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation.

5.3.3 Training Requirements

RCA ensures that all personnel performing duties with respect to the operation of a RCA receive comprehensive training in:

- CA/RA security principles and mechanisms;
- Software versions in use in the PKI CA system;
- Duties they are expected to perform;
- Disaster recovery and business continuity procedures.

RCA and RA personnel shall be retrained when changes occur in RCA or RA systems. Refresher training shall be conducted as required, and the RCA shall review refresher training requirements at least once a year.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for trusted roles shall be aware of changes in the RCA or RA operations, as applicable. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented.

5.3.5 Job Rotation Frequency and Sequence

RCA ensures that any change in the staff will not affect the operational effectiveness of the service or security of the system.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary sanctions are applied to personnel violating CP or CPS.

5.3.7 Independent Contractor Requirements

Contractor personnel employed have to perform RCA functions operations according to the same requirements as defined in section 3.

5.3.8 Documentation Supplied to Personnel

The RCA makes available to its personnel the present CP and the corresponding CPS, and any relevant statutes, policies or contracts. Other technical, operations, and administrative documents (e.g., Administrator Manual, User Manual, etc.) are provided in order for the trusted personnel to perform their duties.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

5.4.1.1 RCA

Audit log files are generated for all events relating to the security and services of the RCA components (Cf. 6.5). Where possible, the security audit logs shall be automatically collected. When this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

RCA ensures all events related to the life cycle of certificates are logged in a manner to ensure their imputability to a person acting in a given role on behalf of the RCA. The CPS gives details on what is logged. At a minimum, each audit record includes the following (either recorded automatically or manually for each auditable event):

- Type of the event,
- Date and time the event occurred,
- Success or failure (where appropriate),
- Identity of the entity and/or person that caused the event,
- Identity for which the event is addressed ;
- Cause of the event.

5.4.2 CA

CA ensures all events related to the life cycle of CA's key are logged in a manner to ensure their imputability to a person acting in a given role on behalf of the CA. The CA's CPS gives details on what is logged. At a minimum, each audit record includes the following (either recorded automatically or manually for each auditable event):

- Type of the event,
- Date and time the event occurred,
- Success or failure (where appropriate),
- Identity of the entity and/or person that caused the event,
- Identity for which the event is addressed ;
- Cause of the event.

5.4.3 Frequency of Processing Log

Audit logs are reviewed periodically for a reasonable search for any evidence of malicious activity and following each important operation.

5.4.4 Retention Period for Audit Log

Records concerning RCA and CA certificates are held for a period of time appropriate for providing necessary legal evidence in accordance with applicable legislation. The records could be needed at least as long as a transaction relying on a valid certificate can be questioned.

5.4.5 Protection of Audit Log

The events are logged in a way that they cannot be deleted or destroyed (except for transfer to long term media) within the period of time that they are required to be held.

The events are logged in a manner to ensure that only authorized trusted access can make operation regarding their profile role without modifying integrity, authenticity and confidentiality of the data.

The events are protected in a manner to keep them still readable in the time of their storage.

The events are dated in a secure manner that guarantees, from the date of creation of the record to the end of the archive period, the trusted link between the event and the time of its realisation.

5.4.6 Audit Log Backup Procedures

Audit logs and audit summaries are backed-up in a secure location (safe ...), under the control of authorized trusted role, separated from their component source generation. Audit logs backup are protected with the same level of trust defined for the original logs.

5.4.7 Audit Collection System

Audit processes are invoked at system start up and end only at system shutdown. The audit collection system has to keep the integrity and the availability of the data collected. If necessary, the audit collection system protects the data in confidentiality. If a problem appears during the process of the audit collection system then the RCA determines whether to suspend RCA operation until the problem is solved and inform the impacted component.

5.4.8 Notification to Event-Causing Subject

No stipulation.

5.4.9 Vulnerability Assessments

The Auditor explains all significant events in an audit log summary. Such reviews involves verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews are documented.

5.5 Records Archival

5.5.1 Types of Records Archived

RCA and RA archive records shall be detailed enough to establish the validity of a signature and of the proper operation of the PKI. At a minimum, the following data shall be archived:

- RCA events records;
- RCA audit documentation;
- RCA CP document;
- RCA CPS document;
- CA CP/CPS (at CA level);
- Any contractual agreements between KEYNECTIS and CA Entity;
- System equipment configuration;
- Certificates and ARLs (or other revocation information);
- Other data or applications sufficient to verify archive contents;
- All work related to or from the KMA, CA and compliance auditors.

5.5.2 Retention Period for Archive

The minimum retention period for archive data is 10 years after the event occurred.

5.5.3 Protection of Archive

The archives are created in a way that they cannot be deleted or destroyed (except for transfer to long term media) within the period of time that they are required to be held. Archive protections ensure that only authorized trusted access can make operation regarding their profile role without modifying integrity, authenticity and confidentiality of the data. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site.

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time-Stamping of Records

No stipulation.

5.5.6 Archive Collection System (Internal or External)

The archive collection system respects the security requirements defined in § 5.4.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorised RCA equipment, trusted role and other authorized person (legal person ...) are allowed to access the archive. Access to archive information is requested to the KMA.

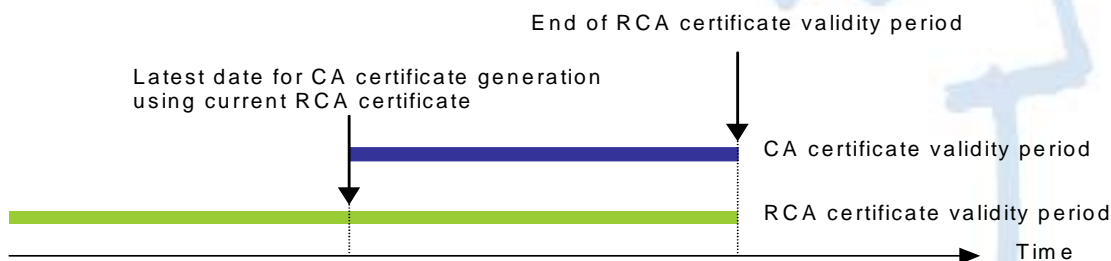
5.6 Key Changeover

5.6.1 RCA

The RCA maintains its private key operational period compliant with the cryptographic recommendation for key size length issued by national bodies or international standard institutes.

The KMA reserves its right to take decision to change the RCA key pair at any time. In this case the CA Entities will be informed.

As the RCA cannot generate CA certificates whose validity period would be superior to the RCA certificate validity period, the RCA is re-keyed at the latest the duration period of CA certificates before the end of the RCA certificate validity period, such as illustrated on the following diagram:



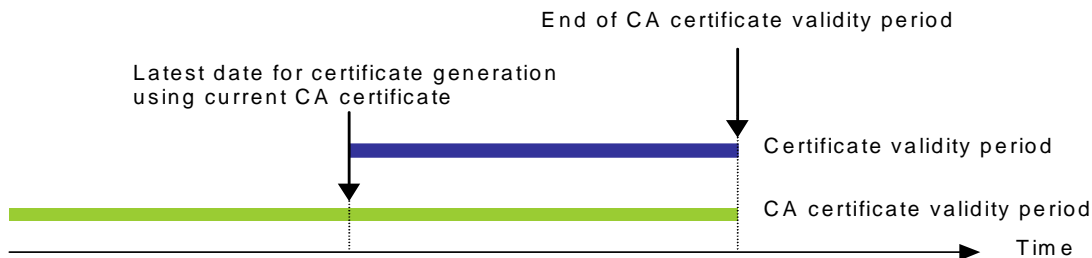
As soon as a new RCA key pair is generated, only this new key can be used to sign CA certificate and associated ARL.

The previous RCA certificate stay valid for validation process of certification path until all CA certificates signed using the previous RCA key pair are expired.

5.6.2 CA

The CA maintains its private key operational period compliant with the cryptographic recommendation for key size length issued by national bodies or international standard institutes.

As the CA cannot generate certificates whose validity period would be superior to the CA certificate validity period, the CA is re-keyed at the latest the duration period of the certificates it issues before the end of its certificate validity period, such as illustrated on the following diagram:



As soon as a new CA key pair is generated, only this new key can be used to sign certificate and associated CRL. The previous CA certificate stay valid for validation process of certification path until all issued certificates signed using the previous CA key pair are expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

KEYNECTIS has established business continuity procedures for the RCA PKI that outlines the steps to be taken in the event of the corruption or loss of computing resources, software and/or data that could disturb or compromise the RCA services. KMA carries out a risk assessment to evaluate business risks and determines the necessary security requirements and operational procedures and elaborates in consequences its disaster recovery plan. This risk analysis is regularly reviewed and revised if necessary (threat evolution, vulnerability evolution ...).

KEYNECTIS personnel that have trusted role and/or operation role are specially trained to operate according to procedure defined in the KEYNECTIS disaster recovery plan for the most sensitive activities.

If a RCA detects a potential hacking attempt or other form of compromise, it performs an investigation in order to determine the nature and the degree of damage. Otherwise, the scope of potential damage is assessed by the KMA in order to determine if the RCA needs to be rebuilt, only some certificates need to be revoked, and/or the RCA needs to be declared compromised, and which services has to be maintained (revocation and certificate status information) and how according to the KEYNECTIS disaster recovery plan.

The CA certified by the RCA are notified if suspected or detected compromise (logical, physical, electric ...) of a RCA system could compromise or will compromise or disturb the CA services. This will allow CA to activate their own disaster recovery plan to protect their interests and the relying parties' ones.

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

In case a RCA equipment is damaged or rendered inoperative, but the signature keys are not destroyed, the operation is re-established as quickly as possible, giving priority to the ability to generate certificate status information according to the KEYNECTIS disaster recovery plan.

5.7.3 Entity private key compromise procedures

If a RCA signature key is compromised, lost, destroyed or suspected to be compromised:

- KMA, after investigation on the "key-problem" decides that the RCA certificate is revoked;
- All Entity CAs, signed by the compromised RCA, are securely notified at the earliest feasible time so that Entity CA, according to the result of the investigation on the RCA compromised key, may decide to revoke or not their certificates;
- A new RCA key pair is generated and a new RCA certificate created;

- CA Entity decides to re-generate or not a new CA certificates.

5.7.4 Business continuity capabilities after a Disaster

The disaster recovery plan addresses the business continuity as described in § 5.7.1.

5.8 RCA component termination

In the event of termination of a RCA component, the RCA requests all certificates issued to this component to be revoked.

In the event of RCA termination, the KMA provides notice to all CAs prior to the termination, and:

- RCA archives all audit logs and other records prior to termination;
- RCA destroys all its private keys upon termination;
- Archive records are transferred to an appropriate authority such as the KMA;
- RCA uses secure means to notify the customers to delete all trust anchors representing the RCA.

CA could still deliver end user certificate according to the CA's CP. In this case, the certification path, used for validation process, will no longer use the RCA certificate and the CA certificate issued by the RCA. Relying parties have to use the CA certification path defined in the CA CP.

6 TECHNICAL SECURITY CONTROLS

All requirements and procedures applying to CA under the present section are identified in the applicable CP/CPS, unless specified in the present section.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 RCA

RCA key generations are undertaken in a physically secure environment by personnel in trusted roles under dual control. RCA key generation is carried out within a hardware security module which either is FIPS 140-1 level 2 compliant or EAL 4+ certified.

6.1.1.2 CA

CA key generations are undertaken in a physically secure environment by personnel in trusted roles under dual control. CA key generation is carried out within a hardware security module which either is FIPS 140-1 level 2 or EAL 4+ certified.

6.1.2 Private Key Delivery to CA

CA generates itself its private key, as described in its CP.

6.1.3 Public Key Delivery to Certificate Issuer

CA public keys are delivered securely to the RCA for certificates issuance through the RA. The delivery mechanism binds CA checked identities to the public keys to be certified.

6.1.4 CA Public Key Delivery to Relying Parties

KEYNECTIS makes RCA certificate available to relying parties by publishing them in the PS and in the major browsers software. RCA certificate is also delivered to the CA representative during the CA certificate generation ceremony (Cf. § 4.3).

CA makes their CA certificates available to relying parties by publishing them according to their CP/CPS.

6.1.5 Key Sizes

If the KMA determines that the security of a particular algorithm may be compromised, it may require the RCA and CAs to revoke the affected certificates.

RCA and CA keys for the RSA algorithm are at least 2048 bits length using at minimum the SHA-1 hash function.

6.1.6 Public Key Parameters Generation and Quality Checking

RSA keys and CA keys are generated in accordance with the cryptography tools of hardware security modules (see section 6.2.11).

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Private key usage of RCA and CA are defined in the certificate profiles (refer to § 7.1). The key usage is set to allow private keys to only sign certificates and ARL or CRL. This restriction is implemented in the certificate using the extension "Key usage".

6.2 Private Key Protection and Cryptographic Module Engineering

6.2.1 Cryptographic Module Standards and Controls

RCA and CA hardware security module is either approved FIPS 140-1 level 2 or EAL 4+ certified, or higher.

6.2.2 Private Key (m out of n) Multi-Person Control

RCA activates its private key with multi-person control, performing duties associated with their trusted roles. Trusted roles permitted to participate to this private key multi-person controls are strongly authenticated.

CA activates its private key with multi-person control, performing duties associated with their trusted roles. Trusted roles permitted to participate to this private key multi-person controls are strongly authenticated.

6.2.3 Private Key Escrow

The RCA and CA private keys are never escrowed, for any reason.

6.2.4 Private Key Backup

The RCA private signature keys are backed up for disaster recovery purposes.

The CA private signature key could be backed up for disaster recovery purposes.

6.2.5 Private Key Archival

Private RCA and CA keys never archived.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

RCA private keys are generated, activated and stored in hardware security modules. When private key is transferred between the hardware security modules, it is encrypted using AES or Triple DES. An encrypted private key can only be decrypted using a hardware security module under multi person control with trusted role.

CA private keys are generated, activated and stored in hardware security modules. Any transfer of the CA private key between hardware security modules has to be protected in confidentiality and in integrity in a manner that nobody can deduced the value of the CA private key.

6.2.7 Private Key Storage on Cryptographic Module

RCA private keys are stored in hardware security modules or in an encrypted form (using AES or Triple DES).

CA private keys are stored in hardware security modules or in an encrypted form (using AES or Triple DES).

6.2.8 Method of Activating Private Key

RCA private key is activated under multi person control with trusted roles that have owns CA activation data. The people who have a trusted role have to be strongly authenticated by the cryptographic module.

CA private key is activated under multi person control with trusted roles that have owns CA activation data. The people who have a trusted role have to be strongly authenticated by the cryptographic module.

6.2.9 Method of Deactivating Private Key

The RCA cryptographic modules that have been activated are not left unattended or otherwise available to unauthorized access. After use, the cryptographic module is deactivated. Hardware cryptographic modules are removed and stored in secure locations.

The CA cryptographic modules that have been activated are not left unattended or otherwise available to unauthorized access. After use, the cryptographic module is deactivated. Hardware cryptographic modules are removed and stored in secure locations.

6.2.10 Method of Destroying Private Key

RCA private keys are destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. Destroying private key requires destroying of the software and hardware, and all associated CA activation data in a manner that no information can be kept and used to deduce any part of the private key.

CA private keys are destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. Destroying private key requires destroying of the software and hardware, and all associated CA activation data in a manner that no information can be kept and used to deduce any part of the private key.

6.2.11 Cryptographic Module Rating

RCA and CA hardware security module are either approved at FIPS 140-1 level 2 or EAL 4+ certified.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival as described in § 5.5.2.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The RCA certificate is valid until 07 July 2019. The RCA private key validity period is determined in accordance with § 5.6.1.

CA private key validity period is determined in accordance with § 5.6.2.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

For RCA, the generation and use of CA activation data used to activate RCA private keys is made during the key ceremony (See section 6.1.1). CA activation data are either chosen by the holder or by a trusted role in a manner to keep the confidentiality and the integrity to the sole holder.

For CA, the generation and use of CA activation data used to activate CA private keys is made during the key ceremony (See section 6.1.1). CA activation data are either chosen by the holder or by a trusted role in a manner to keep the confidentiality and the integrity to the sole holder.

6.4.2 Activation Data Protection

RCA and CA activation data are protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should either be biometric in nature or memorized, not written down.

6.4.3 Other Aspects of Activation Data

Activation data are destroyed:

- When RCA hardware security module is entering a maintenance period;
- When RCA hardware security module is withdrawn from operational service;
- When RCA hardware security module is out of order.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards. The RCA and CA component, dedicated to the creation, destruction, and activation of RCA and CA private key, includes the following functionalities:

- Require authenticated logins for trusted role;
- Provide Discretionary Access Control;
- Provide a security audit capability (protected in integrity);
- Prohibit object re-use;
- Require use of cryptography for session communication and database security;
- Require a trusted path for identification and authentication;
- Provide domain isolation for process;
- Provide self-protection for the operating system.

When RCA PKI equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system), when possible, operates in an evaluated configuration. At a minimum, such platforms use the same version of the computer operating system as that which received the evaluation rating. The computer systems are configured with minimum of the required accounts, network services, and no remote login.

6.5.2 Computer Security Rating

All the RCA PKI components software of the KEYNECTIS center have been developed following the requirements of the protection profile from the French NSA (PP_IGC, PP_AC and PP_AE available on www.ssi.gouv.fr).

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The System Development Controls for the RCA are as follows:

- Use software that has been designed and developed under a formal, documented development methodology;
- Hardware and software procured are purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase);
- Hardware and software developed are developed in a controlled environment, and the development processes are defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software;
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location;
- The hardware and software are dedicated to performing the PKI activities. There is no other applications; hardware devices, network connections, or component software installed which are not part of the PKI operation;
- Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the PKI operations are obtained from sources authorized by local policy. RCA hardware and software are scanned for malicious code on first use and periodically thereafter;

- Hardware and software updates are purchased or developed in the same manner as original equipment; and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

Configuration of the RCA system as well as any modifications and upgrades are documented and controlled by KEYNECTIS management. There is a mechanism for detecting unauthorized modification to the RCA software or configuration. A formal configuration management methodology is used for installation and ongoing maintenance of the RCA system. The RCA software, when first loaded, is verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Controls

For the software and hardware that are evaluated, KMA keeps watching on the maintenance scheme requirements to keep the level of trust.

6.7 Network Security Controls

6.7.1 RCA

The RCA is off-line. Network accessible PKI PS is connected to the Internet via boundary protections and provides continuous service (except, when necessary, for brief periods of maintenance or backup). Information is transported from the Internal PKI PS to the Border PKI PS using manual mechanisms.

6.7.2 CA

CA PKI components, dedicated to the creation, destruction, and activation of CA private key, employ appropriate security measures to ensure they are guarded against attacks.

6.8 Time-Stamping

All RCA components are regularly synchronize with a time service such as Atomic Clock or Network Time Protocol (NTP) Service. A dedicated authority (Time stamping authority) can provide this trusted time. Time derived from the time service shall be used to establish the time of:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates.

Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events as listed in section 5.4.1.

7 CERTIFICATE, ARL, AND OCSP PROFILES

7.1 Certificate Profile

The RCA and CA certificate are X.509 v3 certificates (populate version field with integer "2"). The certificate fields are those defined in the RFC 5280.

7.1.1 Certificate Extensions

At a minimum, the following extensions are included in RCA and CA certificates:

- Authority Key Identifier or/and Subject Key Identifier;
- Key usage (non critical);
- CRL Distribution Points;
- Basic Constraints;
- Certificate policy.

CPS will give details on certificate content.

7.1.2 Algorithm Object Identifiers

They are defined in the RCA CPS.

7.1.3 Name Forms

The name forms follow the requirements described in the section 3.1.

7.1.4 Certificate Policy Object Identifier

The CA certificate delivered by Root CA certificate contained an OID to identify a CP according the rules given in the CPS.

7.1.5 Usage of Policy Constraints Extension

No stipulation.

7.1.6 7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.7 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 ARL Profile

RCA shall issue X.509 version two (v2) ARLs (populate version field with integer "1"). The ARL fields are those defined in the RFC 3280.

7.2.1 ARL and ARL Entry Extensions

CPS will give details on ARL extension fields.

7.3 OCSP Profile

No stipulation.

7.3.1 Version Number(s)

No stipulation.

7.3.2 OCSP Extensions

If an OCSP is used, then the CPS will give details.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency and Circumstances of Assessment

The RCA PKI is subject to periodic compliance audits, to allow KMA to authorize or not (regarding the audit result) RCA to operate under the RCA CP.

Further, the KMA has the right to require a periodic compliance audit of CA that operate under the RCA CP. The KMA states the reason for any periodic compliance audit.

All CA that are certified by RCA according to the RCA CP, have to provide an audit result to demonstrate the compliance of their CP/CPS to the present CP and to the applicable trusted service security standard.

8.2 Identity/Qualifications of Assessor

The compliance auditor shall demonstrate competence in the field of compliance audits, and shall be thoroughly familiar with requirements of this CP. The KMA looks carefully, regarding its own audit requirements basis, to the methods employed to audit RCA and CA PKI.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor is either a private firm, which is independent from the entity being audited, or sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation.

The KMA determines whether a compliance auditor meets this requirement.

8.4 Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a component operates in accordance with the RCA CP and the component CA CP/CPS.

8.5 Actions Taken as a Result of Deficiency

The KMA may determine that the RCA and CA are not complying with its obligations set forth in the RCA CP. When such a determination is made, the KMA may suspend or direct to stop relation with the affected CA (e.g., by revoking the certificate that the RCA has issued), or may request that corrective actions be taken which allow to continue operation of the operation of the noncompliant CA. When the compliance auditor finds a discrepancy between how the CA is designed or is operated or maintained, and the requirements of the RCA CP, the following actions shall be performed:

- The compliance auditor notes the discrepancy;
- The compliance auditor notifies the Entity of the discrepancy. The Entity notifies the KMA promptly;
- The party responsible for correcting the discrepancy determines what further notifications or actions are necessary pursuant to the requirements of the RCA CP, and then proceed to make such notifications and take such actions without delay in relation with the approval of KMA.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the KMA may decide to stop temporarily operation of a CA, to revoke a certificate issued by the RCA, or take other actions it deems appropriate.

8.6 Communications of Results

An Audit Compliance Report, including identification of corrective measures taken or being taken by the component, is provided to the KMA as set forth in § 8.1. The report identifies the versions of the CP and CPS used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in § 8.5 above. The Audit Compliance Report is not available on Internet for relying parties.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

CPS will give details.

9.1.2 Certificate Access Fees

The RCA PS is free access on the internet for relying parties.

9.1.3 Revocation or Status Information Access Fees

The RCA PS is free access on the internet for relying parties.

This publication is not intended to be used by OCSP services or other else similar services but only for relying parties to verify whether a certificate is valid or not.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

This topic is addressed in contractual arrangements between KEYNECTIS and CA Entity.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

KEYNECTIS maintains reasonable levels of insurance coverage.

9.2.2 Other Assets

KEYNECTIS maintains sufficient financial resources to maintain operations and fulfil RCA duties.

9.2.3 Insurance or Warranty Coverage for End-Entities

If there is damage for a CA customer due to KEYNECTIS fault, KEYNECTIS will activate its insurance to cover part of the customer damage in the limits stated in contractual arrangements between KEYNECTIS and CA Entity.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

RCA guarantees a special treatment for the confidential following:

- Records and archive;
- Personal identity data;
- RCA PKI private keys;
- CA Audit result and reports;
- RCA Disaster recovery plans;
- Contractual arrangements with CA Entity;
- Internal KEYNECTIS trust center security policy;
- Part of the RCA CPS defined as confidential.

9.3.2 Information Not Within the Scope of Confidential Information

All information that is published in the PS is not considered confidential, but can be covered by the law on intellectual property right.

9.3.3 Responsibility to Protect Confidential Information

KEYNECTIS enforces French law for the protection of data (confidential and personal data).

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

KMA collects, stores, processes and discloses personally identifiable information in accordance with the European law on privacy data protection.

KEYNECTIS is fully compliant with the French law on the management and protection of personal data and has a special permanent KMA correspondent with the CNIL (National Commission for data privacy) to ensure that KEYNECTIS trust center respects all applicable laws. KEYNECTIS has been audited for this section in the scope of European electronic directive requirements.

9.4.2 Information Treated as Private

KMA considers that information considered as private for RCA and CA are:

- Certificate request form;
- Revocation request form;
- Revocation reason.

9.4.3 Information Not Deemed Private

No stipulation.

9.4.4 Responsibility to Protect Private Information

RCA PKI component treat and protect all the private information in a manner that only authorize access to trusted role (internal or legal entity) according to the KEYNECTIS trust center requirements on the privacy data protection.

9.4.5 Notice and Consent to Use Private Information

All the private information coming from the CA Entity cannot be used, for the purpose of RCA services, without any explicit consent from the CA Entity. This consent is obtained with submitting the certificates request and accepting the CA certificate delivered by the RCA (means that the applicability of the present CP is recognized).

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

KEYNECTIS is compliant with the national law and use secure procedures to allow access to the private data for any legal entity with authentication and secured controlled access to those data.

9.4.7 Other Information Disclosure Circumstances

RCA obtains consent from CA Entity to transfer its private data in case of transfer of activity, as described in the § 5.8.

9.5 Intellectual Property rights

KEYNECTIS retains all intellectual property rights, and is proprietary of the RCA CP and associated CPS, RCA certificate, CA certificate and revocation information that are issued by the RCA.

The CA Entity retains all intellectual rights it owns on information contained in the CA certificate delivered by the RCA (CA distinguished name, public key, policy OID, CRL DP ...) and for which it is the proprietary.

9.6 Representations and Warranties

9.6.1 RCA Representations and Warranties

The RCA ensures that all requirements on RCA PKI, as detailed in the RCA CP and in the corresponding CPS, are implemented as applicable to deliver and manage CA certificate.

The RCA has the responsibility for compliance with the procedures prescribed in the present CP, even when the RCA functionality is undertaken by sub-contractors. The RCA provides all its certification services consistent with its certification practice statement.

Common obligations for RCA PKI components and CA are:

- Protect and guarantee integrity and confidentiality of their secret data and/or private key;

- Only use their cryptographic key and certificate, with associated tools specified in CPS, for what purpose they have been generated for;
- Respect and operate CPS part that deals with their duty (this part of CPS has to be transmitted to the corresponding component);
- Let auditor team audit and communicate every useful information to them, according to the KMA intention, control and check the compliance with the present CP and with the components CP/CPS;
- Respect total or part of agreements that binds it to the CA;
- Document their internal procedures to complete global CPS;
- Use every means (technical and humans) necessary to achieve the realization of the CP/CPS it has to implement and they are responsible for.

9.6.2 CA Representations and Warranties

The RCA obliges through agreement the CA Entity to address, in accordance with the present CP, all the following obligations:

- Submit accurate and complete information to the RCA (CP, CPS, identity for registration, ...);
- Make a compliance audit to provide to KMA;
- Respect the RCA CP and the CP/CPS that has been approved by the KMA as compliant with the present CP;
- Exercise reasonable care to avoid unauthorized use of the CA private key and maintain private key under the CA unique control.
- Notify the RCA without any reasonable delay, if any of the following event as described in section 4.9.1.2 occur up to the end of the validity period indicated in the certificate;
- In case of compromise, immediately and permanently stop the use of the CA private key.

9.6.3 KMA Representations and Warranties

The KMA establishes that external CA signed by the RCA complies with the present CP. The processes and procedures and audit framework used to determine compliance are documented within the certification agreement which is approved by the KMA and the CA Entity.

9.6.4 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

The RCA services only guarantees the identification and authentication of the RCA, with RCA self-signed certificate, and of CA that own a certificate issued by the RCA, and the management of the corresponding certificate and certificate status information regarding the present CP. Not any more guarantees can be pinpointed by CA, relying parties and/or by CA customers in their contractual relationship (if there is any).

9.8 Liability limitation

KEYNECTIS is only responsible for the present CP requirements and principles, for the compliance audit between the present CP and the CA Entity CP/CPS.

CA are responsible for any damage caused to one of its customer or a relying parties because of improperly operating of the CA CP/CPS.

KEYNECTIS assumes no liability whatsoever in relation to the use of RCA certificate and CA certificates or associated public/private key pairs for any use other than the one stated in the present CP.

9.9 Indemnities

In a damage proved to be under KEYNECTIS responsibility, the indemnities are limited to maximum sum of money that is given in the RCA CPS.

9.10 Term and Termination

9.10.1 Term

The RCA CP becomes effective, and after its amendments, upon ratification by the KMA, adoption by the KEYNECTIS board of directors and publication in the PS.

9.10.2 Termination

A new version of the RCA CP accepted by KMA and made available by the PS may oblige CA to change their own CP to stay compliant with the new version of the CP. According to the importance of the change done in the CP, the KMA will decide either to re-mapped CA CP/CPS or to give instruction to the CA Entity to take action to be compliant in a due delay. KMA has the same procedure of action for RCA. Depending on the importance of the CP modification, the CA certificate doesn't have to be re-certified by anticipation.

9.10.3 Effect of Termination and Survival

The end of the validity of the present CP ends all the obligation and liability for the RCA. Depending on the reason of the end of the CP (close services or upgrade services), it could also stop the CA Entity to be bound with KMA to deliver certificates and CA Entity cannot keep on delivering certificates referring to the RCA CP.

9.11 Individual Notices and Communications with Participants

KMA provides participants with new version of CP as soon as it is validated by KEYNECTIS board of directors, via the PS. CA Entity are informed of a new version of the CP in advance, in a manner that allow them to be compliant before the new CP is applicable.

9.12 Amendments

9.12.1 Procedure for Amendment

The KMA reviews the CP and CPS at least once a year. Additional reviews may be enacted at any time at the discretion of the KMA. Spelling errors or typographical corrections which do not change the meaning of the CP are allowed without notification. Prior to approving any changes to the RCA CP, the KMA notifies the CA Entities. The KMA may request CA to notify their customers of consequences of the proposed changes. If the KMA or CA wishes to recommend amendments or corrections to the CP, such modifications shall be circulated to appropriate parties identified by the KMA. The KMA collects, sums up and proposes modifications on the CP following KEYNECTIS approval procedures.

9.12.2 Notification Mechanism and Period

KMA notifies RCA and CA on its intention to modify CP/CPS no less than 30 days before entering the modification process.

9.12.3 Circumstances under Which OID Must be Changed

Present CP OIDs are changed if the KMA determines that a change in the CP modify the level of trust provided by the CP requirements or CPS material.

9.13 Dispute Resolution Provisions

KEYNECTIS proposes to solve dispute on identity to set in the certificate and in the case that parties in conflict cannot find an arrangement; the problem will be solved in a French court. The contractual arrangements between KEYNECTIS and CA Entity contains a dispute resolution clause.

9.14 Governing Law

The applicable laws that govern the RCA CP/CPS applicability are the laws of the State of France, according to the entire relevant European directive that could apply to the present CP/CPS. This choice of law is made to ensure uniform procedures and interpretation for all CA Entity with no matter at where they are located.

9.15 Compliance with Applicable Law

This CP is subject to applicable national, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing cryptographic software, hardware, or technical information.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

If there is any, the KMA has to approve it according to the KEYNECTIS approval procedures.

9.16.2 Assignment

Except where specified by other contracts, only the KMA may assign and delegate this CP to any party of its choice.

9.16.3 Severability

If any part of the CPS is unenforceable by a court of law, it doesn't make the other part of the CPS invalid.

9.16.4 Waiver of Rights

The requirements defined in the CP/CPS are to be implemented as described in CP and corresponding to the CPS without possible waiver of right in the intention of changing any defined rights or obligation.

9.16.5 Act of god

KEYNECTIS is not responsible for indirect damage and interruption of services due to act of god that direct caused direct damage to customer and relying party.

9.17 Other Provisions

If there is any, CPS will give details.

