



KEYNECTIS

■ CERTIFICATE POLICY KEYNECTIS SSL CA

Date: 05/02/2009



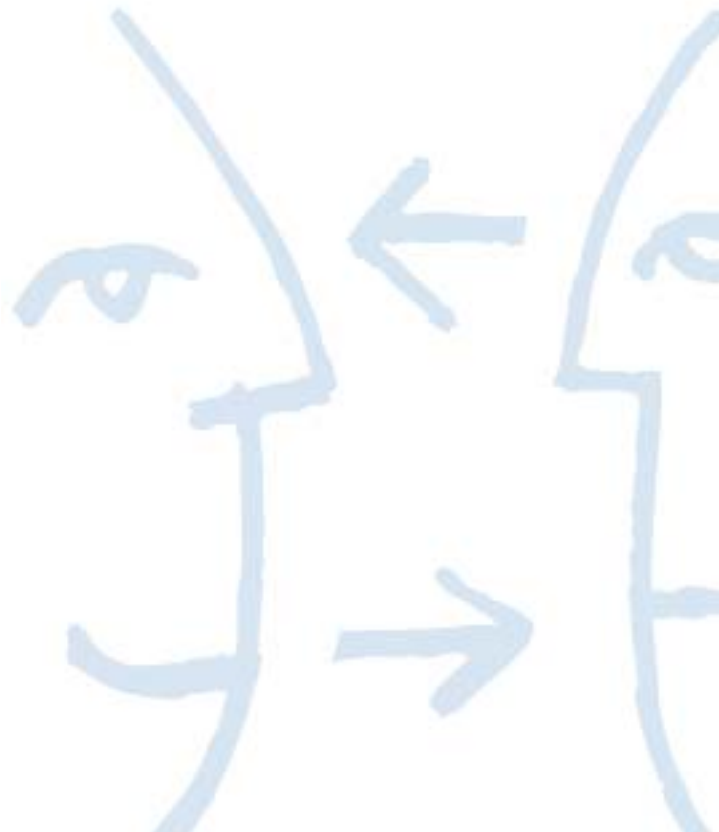
KEYNECTIS SSL CA CERTIFICATE POLICY

Subject: KEYNECTIS SSL CA Certificate Policy

Version number:	1.1	Number of pages:	49
Status of the document:	<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	
			KEYNECTIS

Document history:				
Date	Version	Writer	Comments	Validated by
12/12/07	0.1	EM	Creation of the document	JYF
03/01/08	0.2	EM	Answer to comments	JYF
08/01/08	0.3	CDR	Review	JYF
23/01/08	0.4	CDR	Review	JYF
18/02/08	1.0	CDR	Version to publish	JYF
05/02/09	1.1	JYF	Update of Silver SSL offer	BG -TdV



SUMMARY

1	INTRODUCTION	8
1.1	Overview	8
1.2	Document Name and Identification	9
1.3	PKI Participants	9
1.3.1	KEYNECTIS SSL Certificate Authority (KEYNECTIS SSL CA)	10
1.3.2	Registration Authorities (RA)	10
1.3.3	Publication Service (PS)	10
1.3.4	Owner of Domain Name (ODN)	10
1.3.5	Technical contact (TC)	10
1.3.6	SSL administrator	10
1.3.7	Other Participants	11
1.4	Certificate Usage	11
1.4.1	Appropriate Certificate Use	11
1.4.2	Prohibited Certificate Use	11
1.5	Policy Administration	12
1.5.1	Organization Administering the Document	12
1.5.2	Contact Person	12
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	Definition	12
1.6.2	Acronyms	15
2	PUBLICATION AND REPOSITORY RESPONSIBILITIES	17
2.1	Repositories	17
2.2	Publication of Certificate Information	17
2.3	Time or Frequency of Publication	17
2.4	Access Controls on Repositories	17
3	IDENTIFICATION AND AUTHENTICATION	18
3.1	Naming	18
3.1.1	Type of Names	18
3.1.2	Need for Names to be Meaningful	18
3.1.3	Anonymity or pseudonym of Customers	18
3.1.4	Rules for Interpreting Various Name Forms	18
3.1.5	Unicity of Names	18
3.1.6	Recognition, Authentication, and Role of Trademarks	18
3.2	Initial Identity Validation	18
3.2.1	Method to Prove Possession of Private Key	19
3.2.2	Authentication of an organization identity	19
3.2.3	Authentication of Individual identity	19
3.2.4	Non-Verified information	19
3.2.5	Validation of Authority	19
3.2.6	Criteria for Interoperation	19
3.3	Identification and Authentication for Re-key Requests	20
3.3.1	Identification and Authentication for Routine Re-key	20
3.3.2	Identification and Authentication for Re-key After Revocation	20
3.4	Identification and Authentication for Revocation Request	20
4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	21
4.1	Certificate Application	21
4.1.1	Origin of a certificate request	21
4.1.2	Enrolment Process and Responsibilities	21
4.2	Certificate Application Processing	22



KEYNECTIS

4.2.1	Performing Identification and Authentication Functions	22
4.2.2	Approval or Rejection of Certificate Applications.....	23
4.2.3	Time to Process Certificate Applications	23
4.3	Certificate Issuance.....	24
4.3.1	CA Actions during Certificate Issuance (K.SSL Gold and Silver offers, Club SSL and ISP SSL offers)	24
4.3.2	Notifications to Customer by the CA of Issuance of Certificate	24
4.4	Certificate Acceptance.....	24
4.4.1	Conduct Constituting Certificate Acceptance	24
4.4.2	Publication of the Certificate by the CA	24
4.4.3	Notification of Certificate Issuance by the CA to Other Entities.....	24
4.5	Key Pair and Certificate Usage	24
4.5.1	SSL Private Key and Certificate Usage	24
4.5.2	Relying Party Public Key and Certificate Usage.....	25
4.6	Certificate Renewal	25
4.6.1	Circumstances for Certificate Renewal.....	25
4.7	Certificate Re-Key.....	25
4.8	Certificate Modification.....	25
4.9	Certificate Revocation and Suspension.....	25
4.9.1	Circumstances for Revocation	25
4.9.2	Procedure for Revocation Request.....	26
4.9.3	Revocation Request Grace Period	27
4.9.4	Time within Which CA Must Process the Revocation Request	27
4.9.5	Revocation Checking Requirements for Relying Parties	27
4.9.6	CRL Issuance Frequency	27
4.9.7	Maximum Latency for CRL	27
4.9.8	On-Line Revocation/Status Checking Availability.....	27
4.9.9	On-Line Revocation Checking Requirements.....	27
4.9.10	Other Forms of Revocation Advertisements Available	27
4.9.11	Special Requirements regarding Key Compromise.....	27
4.9.12	Circumstances for Suspension	27
4.9.13	Who Can Request Suspension.....	27
4.9.14	Procedure for Suspension Request.....	28
4.9.15	Limits on Suspension Period	28
4.10	Certificate Status Services	28
4.10.1	Operational Characteristics.....	28
4.10.2	Service Availability	28
4.10.3	Optional Features	28
4.11	End of Subscription	28
4.12	Key Escrow and Recovery	28
5	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	29
5.1	Physical Controls	29
5.1.1	Site Location and Construction	29
5.1.2	Physical Access	29
5.1.3	Power and Air Conditioning	29
5.1.4	Water Exposures	29
5.1.5	Fire Prevention and Protection	29
5.1.6	Media Storage.....	29
5.1.7	Waste Disposal.....	29
5.1.8	Off-Site Backup.....	29
5.2	Procedural Controls.....	30
5.2.1	Trusted Roles.....	30
5.2.2	Number of Persons Required per Task	30
5.2.3	Identification and Authentication for Each Role.....	30
5.2.4	Roles Requiring Separation of Duties.....	30
5.3	Personnel Controls	30
5.3.1	Qualifications, Experience, and Clearance Requirements	30



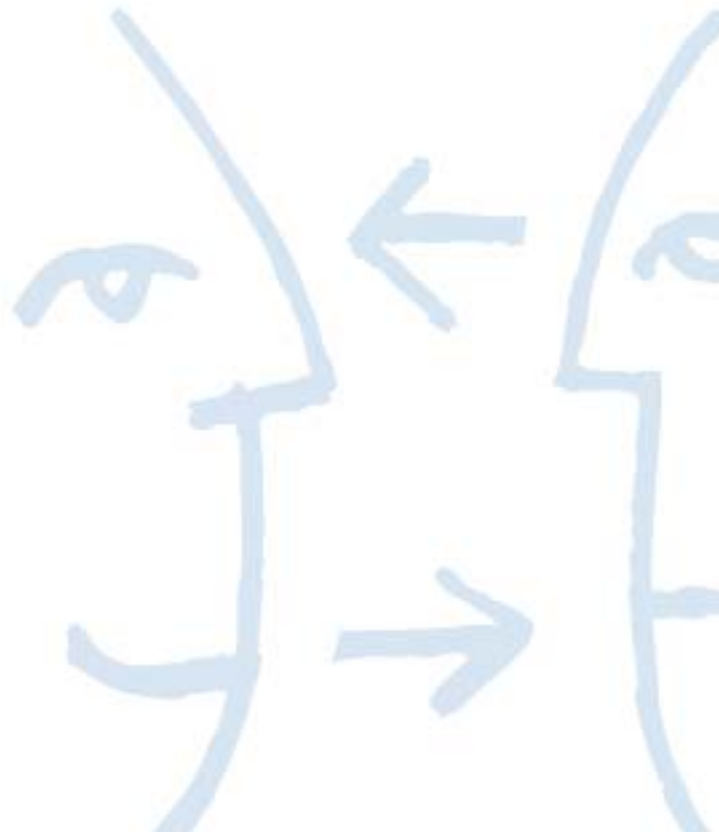
5.3.2	Background Check Procedures	31
5.3.3	Training Requirements.....	31
5.3.4	Retraining Frequency and Requirements	31
5.3.5	Job Rotation Frequency and Sequence	31
5.3.6	Sanctions for Unauthorized Actions.....	31
5.3.7	Independent Contractor Requirements.....	31
5.3.8	Documentation Supplied to Personnel	31
5.4	Audit Logging Procedures	32
5.4.1	Types of Events Recorded.....	32
5.4.2	Frequency of Processing Log	32
5.4.3	Retention Period for Audit Log.....	32
5.4.4	Protection of Audit Log.....	32
5.4.5	Audit Log Backup Procedures	32
5.4.6	Audit Collection System (Internal vs. External).....	32
5.4.7	Notification to Event-Causing Subject	33
5.4.8	Vulnerability Assessments	33
5.5	Records Archival	33
5.5.1	Types of Records Archived.....	33
5.5.2	Retention Period for Archive	33
5.5.3	Protection of Archive.....	33
5.5.4	Archive Backup Procedures.....	33
5.5.5	Requirements for Time-Stamping of Records	33
5.5.6	Archive Collection System (Internal or External)	33
5.5.7	Procedures to Obtain and Verify Archive Information	33
5.6	Key Changeover	34
5.6.1	SSL certificate.....	34
5.6.2	KEYNECTIS SSL CA certificate	34
5.7	Compromise and Disaster Recovery.....	34
5.7.1	Incident and Compromise Handling Procedures	34
5.7.2	Computing resources, software, and/or data are corrupted	35
5.7.3	Entity private key compromise procedures.....	35
5.7.4	Business continuity capabilities after a Disaster.....	35
5.8	SSL CA component termination	35
6	TECHNICAL SECURITY CONTROLS	36
6.1	Key Pair Generation and Installation.....	36
6.1.1	Key Pair Generation.....	36
6.1.2	Private Key Delivery to Customer	36
6.1.3	Public Key Delivery to Certificate Issuer	36
6.1.4	CA Public Key Delivery to Relying Parties.....	36
6.1.5	SSL certificate Key Size.....	36
6.1.6	Public Key Parameters Generation and Quality Checking	36
6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field)	36
6.2	Private Key Protection and Cryptographic Module Engineering	36
6.2.1	Cryptographic Module Standards and Controls.....	36
6.2.2	Private Key (m out of n) Multi-Person Control	37
6.2.3	Private Key Escrow	37
6.2.4	Private Key Backup.....	37
6.2.5	Private Key Archival	37
6.2.6	Private Key Transfer Into or From a Cryptographic Module	37
6.2.7	Private Key Storage on Cryptographic Module.....	37
6.2.8	Method of Activating Private Key	37
6.2.9	Method of Deactivating Private Key.....	37
6.2.10	Method of Destroying Private Key	37
6.2.11	Cryptographic Module Rating	37
6.3	Other Aspects of Key Pair Management.....	38
6.3.1	Public Key Archival	38
6.3.2	Certificate Operational Periods and Key Pair Usage Periods	38



6.4	Activation Data	38
6.4.1	Activation Data Generation and Installation.....	38
6.4.2	Activation Data Protection.....	38
6.4.3	Other Aspects of Activation Data.....	38
6.5	Computer Security Controls	38
6.5.1	Specific Computer Security Technical Requirements	38
6.5.2	Computer Security Rating.....	39
6.6	Life Cycle Technical Controls	39
6.6.1	System Development Controls	39
6.6.2	Security Management Controls.....	39
6.6.3	Life Cycle Security Controls.....	39
6.7	Network Security Controls	39
6.8	Time-Stamping	39
7	CERTIFICATE, CRL, AND OCSP PROFILES	41
7.1	Certificate Profile	41
7.1.1	Certificate Extensions	41
7.1.2	Algorithm Object Identifiers.....	41
7.1.3	Name Forms	41
7.1.4	Certificate Policy Object Identifier.....	41
7.1.5	Usage of Policy Constraints Extension.....	41
7.1.6	Processing Semantics for the Critical Certificate Policies Extension	41
7.2	CRL Profile	41
7.2.1	CRL and CRL Entry Extensions.....	41
7.3	OCSP Profile	41
7.3.1	Version Number(s).....	41
7.3.2	OCSP Extensions	42
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	43
8.1	Frequency and Circumstances of Assessment	43
8.2	Identity/Qualifications of Assessor	43
8.3	Assessor's Relationship to Assessed Entity	43
8.4	Topics Covered by Assessment	43
8.5	Actions Taken as a Result of Deficiency	43
8.6	Communications of Results	43
9	OTHER BUSINESS AND LEGAL MATTERS	44
9.1	Fees	44
9.1.1	Certificate Issuance or Renewal Fees	44
9.1.2	Certificate Access Fees	44
9.1.3	Revocation or Status Information Access Fees.....	44
9.1.4	Fees for Other Services.....	44
9.1.5	Refund Policy	44
9.2	Financial Responsibility	45
9.2.1	Insurance Coverage.....	45
9.2.2	Other Assets	45
9.2.3	Insurance or Warranty Coverage for End-Entities	45
9.3	Confidentiality of Business Information	45
9.3.1	Scope of Confidential Information.....	45
9.3.2	Information Not Within the Scope of Confidential Information.....	45
9.3.3	Responsibility to Protect Confidential Information	45
9.4	Privacy of Personal Information	45
9.4.1	Privacy Plan	45
9.4.2	Information Treated as Private.....	45
9.4.3	Information Not Deemed Private.....	46
9.4.4	Responsibility to Protect Private Information.....	46
9.4.5	Notice and Consent to Use Private Information.....	46
9.4.6	Disclosure Pursuant to Judicial or Administrative Process.....	46



9.4.7	Other Information Disclosure Circumstances	46
9.5	Intellectual Property rights	46
9.6	Representations and Warranties	46
9.6.1	KEYNECTIS SSL CA Representations and Warranties	46
9.6.2	Applicant Representations and Warranties	47
9.6.3	RA Representation and Warranties	47
9.6.4	TC Representation and Warranties	47
9.6.5	Representations and Warranties of Other Participants	47
9.7	Disclaimers of Warranties	47
9.8	Liability limitation	48
9.9	Indemnities	48
9.10	Term and Termination	48
9.10.1	Term	48
9.10.2	Termination	48
9.10.3	Effect of Termination and Survival	48
9.11	Individual Notices and Communications with Participants	48
9.12	Amendments	48
9.12.1	Procedure for Amendment	48
9.12.2	Notification Mechanism and Period	48
9.12.3	Circumstances under Which OID Must be Changed	49
9.13	Dispute Resolution Provisions	49
9.14	Governing Law	49
9.15	Compliance with Applicable Law	49
9.16	Miscellaneous Provisions	49
9.16.1	Entire Agreement	49
9.16.2	Assignment	49
9.16.3	Severability	49
9.16.4	Waiver of Rights	49
9.16.5	Act of god	49
9.17	Other Provisions	49



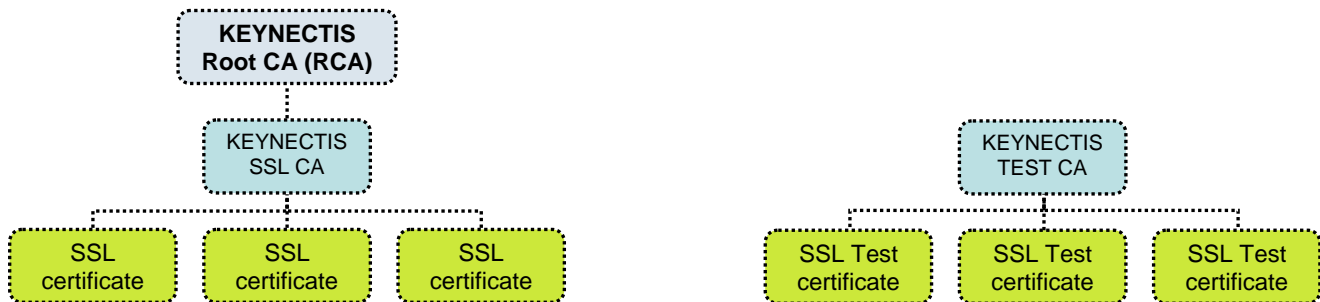
1 INTRODUCTION

1.1 Overview

Dematerialization, i.e. the conversion to an electronic format of traditional daily transactions (contracts, mail, invoices, administrative forms, etc.) is primarily a way of expediting business processes. The innovating and technical aspects of these applications require firms to call on specialized service providers that are in a position to play the role of trusted third party – in order to produce proof of the transaction as required.

At the core of the technologies are the electronic certificates. In order to provide their trust services , Trusted Third Parties (Certificate Authority, Time stamping Authority, Validation Authority), firms and organizations that use electronic certificates rely on KEYNECTIS' production unit and authorities (CAs, TSAs, VAs) for certificate and time stamp issuance, as well as validation services.

KEYNECTIS operates a Root Certification Authority (RCA) that certifies the KEYNECTIS SSL CA, which delivers SSL certificates in accordance with the present CP. An SSL certificate is a digital certificate allowing SSL connections between servers and websites.



An SSL certificate allows to:

- Establish binding between a web page hosted on a server and its owner;
- Authenticate the server hosting the web page;
- Initialize secure communication between the server hosting the web page and people or servers connecting to this web page.

The KEYNECTIS SSL CA delivers SSL certificates to customers through three distinct offers that are:

K.SSL Gold and Silver:

Gold and Silver K.SSL offers are provided to customers on a unitary basis. Each time a customer purchase an SSL certificate, he or she has to complete the overall registration toward the KEYNECTIS SSL registration authority. Gold SSL certificates verifications proceeded by the KEYNECTIS SSL registration authority are more stringent than Silver SSL certificates ones (refer to § 4 below);

Club SSL:

Club SSL offer proposes customers to purchase SSL certificates on a quantity basis (Club SSL 10 for 10 SSL certificates, Club SSL 100 for 100 SSL certificates) and have to be used within one year. Customers are small and large organizations that need quantity certificates to cover requirements of their domain names. The organization and its representative identities are checked by the KEYNECTIS SSL registration authority before the SSL registration desk is opened.

ISP SSL:

Gold certificates are purchased on a quantity basis by Internet Service Providers on behalf of their customers to cover the requirements of the hosted domain names. The ISP and its representative identities are checked by the KEYNECTIS SSL registration authority before the registration desk is opened.

K.SSL test certificates:



These SSL certificates are delivered for test purposes only by a single self-signed CA dedicated for SSL test certificates issuance. KEYNECTIS, as issuer of SSL test certificates, will not be deemed responsible for any use of SSL test certificates. These certificates are delivered by KEYNECTIS automatically to the requestor during online transaction without any verification. K.SSL test certificate validity period is 14 days. KEYNECTIS SSL CA does not manage the K.SSL test certificate status.

The trust and the quality provided by an SSL certificate depend on the SSL CA requirements and means defined in its CP/CPS. The present CP defines the objectives and requirements for the practises (business, legal, and technical) employed by RCA and KEYNECTIS SSL CA to provide certification services that include enrolment, issuance, renewal and revocation of SSL certificates.

KEYNECTIS RCA certificate and KEYNECTIS SSL CA certificate are available in all the browsers and messaging tools to simplify the recognition of all SSL certificates issued by KEYNECTIS.

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:

1.3.6.1.4.1.22234.2.5.1.3 for SSL certificates signed by KEYNECTIS SSL CA

1.3.6.4.1.22234.2.7.1.1 for SSL test certificates signed by KEYNECTIS TEST CA

This OID will be set in the SSL certificates delivered by the KEYNECTIS SSL CA.

1.3 PKI Participants

To host and operate its CA, KEYNECTIS deployed a PKI (Public Key Infrastructure) in its trust center. This PKI is composed of the following components to support KEYNECTIS SSL CA services:

- Generation of SSL CA key: KEYNECTIS SSL CA generates its key pairs in KEYNECTIS trust center during a specific operation called “Key ceremony”;
- Generation of SSL CA certificates: KEYNECTIS SSL CA requests KEYNECTIS RCA for a certificate according to the RCA CP;
- Authentication of RA: KEYNECTIS SSL CA authenticates the Registration Authority in order to register SSL certificate requests;
- Generation of key pair for SSL certificates: the SSL certificate applicant generates its own cryptographic key pair(s);
- Authentication of the SSL certificate applicant : before delivering SSL certificates, the RA (Registration Authority) collects and checks information included in the requests;
- Generation of SSL certificates: If the applicant request is accurate and validated by the RA, then the KEYNECTIS SSL CA generates an SSL certificate;
- Revocation of SSL certificates: when the bending between the certificate applicant and the public key defined within the certificate delivered by KEYNECTIS SSL CA is considered no longer valid, then the SSL certificate has to be revoked either the applicant, either by the RA or KEYNECTIS SSL CA;
- Renewal of SSL certificates: renewing an SSL certificate means generating a new certificate with the same or different information (key, name ...) as the previous certificate. The certificate applicant is responsible of the renewal request;
- Publication services: RCA certificate, SSL CA certificate and associated CRLs are published by KEYNECTIS on its web site. Also, the RCA certificate and SSL CA certificates are provided to main browsers editors (Microsoft, Mozilla foundation...) by KEYNECTIS to be published in their software.

The following CP gives the security requirements for all the described services, the corresponding CPS will give more details on the practises supported by each entity.



1.3.1 KEYNECTIS SSL Certificate Authority (KEYNECTIS SSL CA)

KEYNECTIS SSL CA is a CA that generates SSL certificates for customers (companies, government agencies...) and allows them to set up trusted communications. KEYNECTIS SSL CA uses KEYNECTIS Publication Service to publish its certificates and the CRL it issues.

KEYNECTIS SSL CA operates its own PKI in accordance with its CP/CPS.

1.3.2 Registration Authorities (RA)

An RA is an entity that realizes the authentication and verification of SSL certificate applicants. An SSL applicant transmits SSL certificate request(s) according to the present CP. An RA is authenticated and recognized by KEYNECTIS SSL CA.

KEYNECTIS SSL CA customer service acts as an RA for the K.SSL Gold and Silver offers.

SSL Administrators act as RA for the Club SSL and the ISP SSL offers, (refer to § 1.3.6 below).

1.3.3 Publication Service (PS)

A PS is an entity that makes available certificates, CRLs and any CA relevant information on the Internet.

1.3.4 Owner of Domain Name (ODN)

The ODN is the legal entity that holds the domain name to include in an SSL certificate delivered by KEYNECTIS SSL CA. The domain name is managed by a domain name administrator. An "Authentication" step enables KEYNECTIS SSL CA to ascertain that:

- The organization mentioned in the Certificate Signing Request (CSR) exists and is legally entitled to the exclusive use of its name;
- The domain name featured in the request belongs to that organization, which is therefore entitled to use it;
- There is either an SSL administrator (refer to § 1.3.6 below) acting as the SSL certificate Applicant or a technical contact (refer to § 1.3.5 below), acting as the SSL certificate Applicant, who is entitled to submit the request since he belongs to the ODN organization, or a company appointed by the ODN organization, and which authorized him to send the request.

1.3.5 Technical contact (TC)

A Technical Contact is a person appointed by the ODN organization and which is authorized to:

- Act as an SSL applicant for the generation of SSL Certificate Signing Requests (CSR)
- Fulfil SSL certificate requests forms
- Retrieve SSL certificates.

1.3.6 SSL administrator

An SSL administrator is a person authorized by the SSL customer to act as an SSL certificate applicant for Club SSL and ISP SSL offers. The SSL administrator may also revoke certificates on behalf of the SSL customer.

- In case of a Club SSL offer, the SSL administrator is acting as an applicant for the organization that owns the domain names.
- In case of the ISP SSL offer, the SSL administrator is acting as an applicant for the ISP which himself is acting on behalf of organizations owning the domain names.

For the Club SSL offer, the SSL administrator acts as an RA and manages RA services for the KEYNECTIS SSL CA. In this perspective, the SSL administrator is in charge of:

- Filling the SSL certificate requests on behalf of the SSL customer
- Transmitting the SSL certificate retrieval codes to the appropriate technical contact
- Revoking the SSL certificate
- Authenticate to the KEYNECTIS SSL CA as necessary.

For the ISP SSL offer, the SSL administrator acts as an RA and manages RA services for the KEYNECTIS SSL CA. In this perspective, the SSL administrator is in charge of:

- Filling the SSL certificate requests on behalf of the (ODN) hosted organizations
- Transmitting the SSL certificate retrieval codes to the appropriate technical contact



- Revoking the SSL certificate
- Authenticate to the KEYNECTIS SSL CA as necessary.

When a KEYNECTIS SSL CA customer owns its RA services it has to first contract with the KEYNECTIS SSL CA. The contract mentions that:

- The organization is responsible for internal authentication and all checks necessary to validate SSL certificates in accordance with the present CP
- The organization, acting as an RA, implements parts of the CP/CPS that apply
- The organization has to inform the KEYNECTIS SSL CA, in a reasonable and safe delay, of any changes related to the identity and the position of its representatives toward KEYNECTIS SSL CA
- Its SSL administrator uses electronic certificates on smartcards to authenticate with the KEYNECTIS SSL CA website when proceeding to SSL certificate application and validation
- Its RA services are subject to KEYNECTIS SSL CA audits.

1.3.7 Other Participants

1.3.7.1 KEYNECTIS Management Authority (KMA)

The KMA establish the present CP that KEYNECTIS SSL CA implements, in accordance with the RCA CP. The KMA defines the compliance process for KEYNECTIS SSL CA.

KEYNECTIS benefits from her own audit framework to audit KEYNECTIS SSL CA.

All KMA decisions related to the set up of a CA under KEYNECTIS root CA, such as the set up of KEYNECTIS SSL CA, are approved by the KEYNECTIS board of shareholders.

1.3.7.2 Root Certificate Authority (RCA)

The RCA is operated by KEYNECTIS. The RCA signs and revokes KEYNECTIS SSL CA certificates. In the present CP, when the 'RCA term' is used without any details components (RA, PS...), it covers all the aspects of the deployed PKI dealing with legal and business matters of the root CA. The RCA supports the PKI services as described above (refer to § 1.3). The RCA uses the service of its RA to authenticate and identify KEYNECTIS SSL CA for certificates request, revocation request and renewal request. The RCA uses the Publication Service to publish the certificates and the ARL that it generates. RCA operates its services according to the RCA CP and the corresponding CPS. The RCA can't operate without the approval of the KMA.

1.3.7.3 Relying party

A relying party is an individual or an organization that relies on certificates and/or a digital signature. In this context, an internet customer that trusts the SSL certificates, means trusts the KEYNECTIS SSL CA certification path, to have business relationship (access control on private network, trust server to transmit data ...) with the organization whose domain name is included in the SSL certificate.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Use

1.4.1.1 SSL CA certificate

The KEYNECTIS SSL CA certificate is used by an internet customer to check the identity of an SSL certificate delivered according to the KEYNECTIS SSL CA CP.

1.4.1.2 SSL certificate

An SSL certificate delivered by the KEYNECTIS SSL CA is used by (internet or intranet) relying parties to check the identity of a domain name hosted by a server.

1.4.2 Prohibited Certificate Use

Other applications than SSL certificate issuance, means different certificate profile and/or different function, are not covered by the present CP.



CA Certificates shall not be used for any functions except CA functions.

KEYNECTIS SSL CA will not be deemed responsible for any other perimeter or use than the one defined in the present CP.

Certificates shall be used only with applicable law, and in particular, only to the extent permitted by applicable export or import laws.

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

30, rue du Château des Rentiers, 75647 Paris Cedex 13 - FRANCE

Phone: +33 (0)1 53 94 22 00

Fax: +33 (0)1 53 94 22 01

info@keynectis.com

1.5.3 Person Determining CP Suitability for the Policy

KEYNECTIS SSL CA is responsible for the implementation and maintenance of the present CP. KEYNECTIS SSL CA is responsible for the definition, operation and maintenance of the associated CPS.

The KMA maps KEYNECTIS SSL CA CP/CPS in order to allow KEYNECTIS SSL CA to be signed by the RCA as described in the RCA CP.

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.

KEYNECTIS SSL CA CPS is not published. KEYNECTIS SSL CA submits its CPS to KMA for approval.

The KMA review and approves the mapping results made by KMA experts as a result of KEYNECTIS SSL CA CPS compliancy analysis.

Amendments to CPS are issued as a new CPS version. The new version of CPS replaces automatically the previous version and becomes operational as soon as the KMA has established his agreement on the mapping result. A new version of CPS is still compliant with the present CP to permit KEYNECTIS SSL CA to refer to this CP to deliver SSL certificates.

1.6 Definitions and Acronyms

1.6.1 Definition

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).

Applicant: a person authorized by the ODN or the SSL customer to proceeds to SSL Certificate Signing Requests (CSR).



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]

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 customer are certificates used by server to establish SSL connection 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 (signed by the RCA).

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

Certificate Policy (CP): A named set of rules that indicates the applicability of a certificate to a particular community and/or a class of applications with common security requirements. [ISO/IEC 9594-8; ITU-T X.509]. The present document is the KEYNECTIS SSL CA CP.

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

Certificate Request: A message transmitted by the RA to the CA to have an SSL certificate delivered by the KEYNECTIS SSL CA.

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 KEYNECTIS SSL CA is used to deal with a CA which requests 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 2527]

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, a CA-certificate and the SSL certificates signed by a KEYNECTIS SSL 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; a CRL 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].



CRL Usage Agreement An agreement setting forth the terms and conditions under which a CRL or the within information can be used.

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 an SSL certificate to secure its website. 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 defined in the CP/SPC.

Domain name: Name that has been registered by the organization with legal agencies such as AFNIC or INTERNIC. It is composed of the name preceding the extension (such as .fr or .com) and completed by the extension itself. The domain name is always to be registered in the name of the organization that requests it. During the registration process, the domain name is "associated" to a technical contact that is legally entitled to use this domain name.

KEYNECTIS SSL CA: A KEYNECTIS owned Trusted Third Party (enterprise in telecom industry, internet enterprise ...) that set up its own CA, signed by the KEYNECTIS RCA, to deliver SSL certificates to customers according to the present CP. KEYNECTIS SSL CA has to be successfully mapped with the present CP by the KMA before starting delivery of SSL certificates.

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 inside KEYNECTIS. Refer to § 1.3.7.1 for more details.

Key Ceremony: A procedure whereby a CA or an RA key pair is generated using a cryptographic module and where the public key is certified.

KEYNECTIS Trust Center: The initial purpose of the KEYNECTIS Trust Center and resources operated by KEYNECTIS is the generation of electronic certificates. These services include:

- Management of the certificate authorities' life cycles
- Management of the digital certificates' life cycles
- Publishing of the elements associated to those life cycles' management
- Production of time stamping tokens
- Customization of chip cards and other USB keys
- Verification of electronic signatures or of the validity of certificates

Mapping process: Process established by the KMA to determine whether KEYNECTIS SSL CA operation is compliant or not with the present CP. To realize the process, the KMA uses the present CP, the "KEYNECTIS SSL CA CPS" and any other applicable procedure as the set of reference of KEYNECTIS requirements for SSL certificates issuance. The KMA has to check policy and practices and decide if there is a difference with regard to the defined security requirements.



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 2527]

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 CRL are to be posted. [2nd DIS ISO/IEC 11770-3 (08/1997)]

Publication Services (PS): A service that disseminates information to customers, and eventually to relying parties.

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

Relying Party: refer to § 1.3.7.3 above.

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

Root Certificate Authority (RCA): refer to § 1.3.7.2 above.

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.

SSL Administrator: refer to § 1.3.6 above.

Security policy: The set of rules lay 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 KEYNECTIS which host and operate KEYNECTIS SSL CA.

Self-signed certificate: A certificate for one CA signed using its private key.

Technical contact: refer to § 1.3.5 above.

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].

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

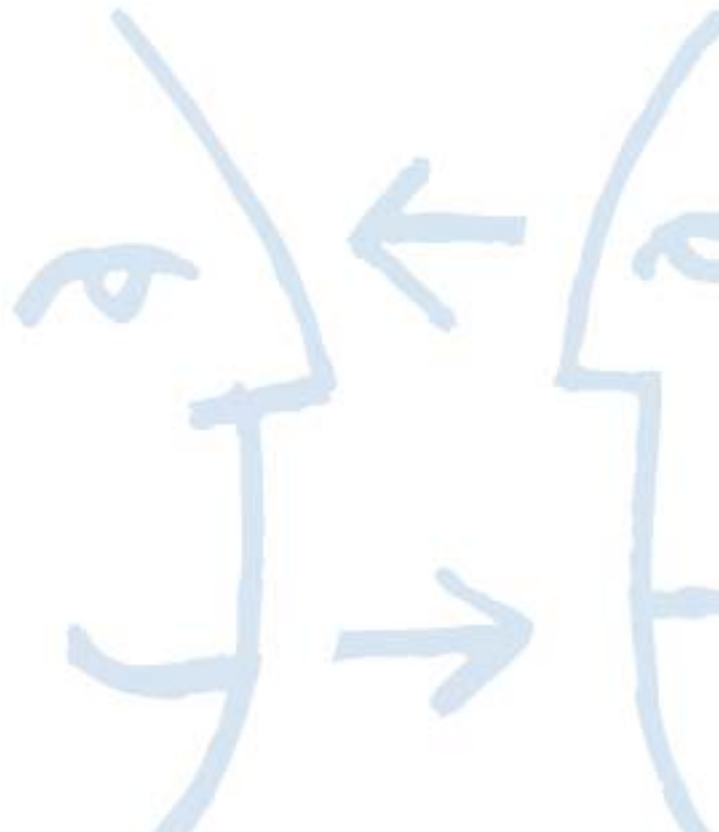
ANSI: The American National Standards Institute;

ARL: Authority Revocation List;

KEYNECTIS SSL CA: Certificate Authority that delivers SSL certificates to customer;



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 Organization for Standardization;
KMA: KEYNECTIS Management Authority;
KTS: KEYNECTIS Trust Center;
LDAP: Lightweight Directory Access Protocol;
OCSP: Online Certificate Status Protocol;
ODN: Owner of a Domain Name
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);
SSL: Secure Socket Layer;
URL: Uniform Resource Locator.





2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

KEYNECTIS SSL CA relies on the PS repository to make available the information defined below to customers and relying parties.

2.2 Publication of Certificate Information

KEYNECTIS SSL CA ensures that the terms and conditions of the CP and certificates are made available to customers and relying parties using KEYNECTIS PS. The following information is published:

- Root CA certificate
- KEYNECTIS RCA CP
- KEYNECTIS SSL CA certificate
- KEYNECTIS SSL CA CP
- Documentation related to certificates request, retrieval and revocation request
- SSL certificates status.

This information is published on the KEYNECTIS website at the following addresses:

- www.keynectis.com/PC for the certificate policies
- www.keynectis.com/PC for the CA certificates
- <http://trustcenter-crl.certificat2.com/keynectis/crl/class2keynectisca.crl> for the SSL certificates status (CRLs)
- <http://trustcenter-crl.certificat2.com/keynectis/crl/testkeynectisca.crl> for the SSL test certificates status (CRLs)
- <http://ssl.keynectis.com> for the documentation related to certificates request, retrieval and revocation request.

KEYNECTIS SSL CA does not publish any information related to the K.SSL test certificates.

2.3 Time or Frequency of Publication

CP and documentation related to certificates are published no longer than 2 (two) days after approval of the applicable version.

The CA certificates are published at the latest 24 (twenty four) hours after generation.

The SSL certificate status is made available through CRLs.

CRLs are published at least every 24 (twenty four) hours.

2.4 Access Controls on Repositories

The KEYNECTIS 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

KEYNECTIS SSL CA does not proceed to any identification and authentication related to any K.SSL test certificates requests.

3.1 Naming

3.1.1 Type of Names

SSL certificate have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate subject name field, in accordance with RFC3280. The distinguished name is composed with the following elements:

Organization	The entity for which the SSL certificate is issued. The term 'Organization' is a generic name covering the various types of entities requesting SSL certificates (business, administration, local community, association ...). The name of the Organization must be the same than that which is associated to the DUNS number featured in the request.
Common Name	The Common Name is the Fully Qualified Domain Name (FQDN). It is the name of the website to be secured. Therefore, the Common Name is all that follows http://, including the extension. The Common Name can never be an IP address.
Locality	The customer must fulfil this data field with the name of the city where his organization's head office is located.
State	The customer fills in here the state, region, or the 'department' where his organization is located.
Country	The customer must enter here the 2-letters country code (ISO standard)

If the customer changes any information contained in the DN, he has to inform the RA of the modification. The new identity is then checked according to § 3.2.2 below. In case the verification succeeds, the customer can be re-certified by KEYNECTIS SSL CA.

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 domain in a meaningful way.

3.1.3 Anonymity or pseudonym of Customers

The identity used for the SSL 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 the chapters 3.1.1 and 7.1.

3.1.5 Unicity of Names

The SSL certificate identities (refer to § 3.1.1 above) are unique for all SSL certificates generated by the KEYNECTIS SSL CA. The RA ensures this unicity by its registration process (Cf. section 3.2.2).

A technical contact requesting for an SSL certificate from KEYNECTIS SSL CA demonstrates its right to use a particular name for his identity. Where there is a dispute about a name for a certificate, KEYNECTIS SSL CA is responsible to solve the name claim dispute resolution.

3.1.6 Recognition, Authentication, and Role of Trademarks

A customer is not guaranteed that its name will contain a trademark if requested. KEYNECTIS SSL CA is not obligated to research trademarks or resolve trademark disputes.

3.2 Initial Identity Validation



3.2.1 Method to Prove Possession of Private Key

The TC proceeds to the generation of the key pairs and SSL CSR on behalf of the KEYNECTIS SSL CA customer.

KEYNECTIS SSL CA ensures that the customer requesting an SSL certificate owns the private key corresponding to the public key to be certified, using CSR on PKCSs#10 format.

3.2.2 Authentication of an organization identity

Authentication of an organization identity is based on the verification of information provided by the organization. This information includes the organization name, the address of the organization and documentation or references of the existence of the organization, the domain name it owns.

The entity that proceeded to the verification checks that the organization is legally entitled to the exclusive use of its name, by mapping the information provided in the SSL certificate application, Club SSL or ISP SSL contract with information retrieved from official database documentation (database issued from government agencies or competent authorities), that confirms the existence of the organization. That database documentation contains trusted information that is filled by the trusted source that registers the legal company.

Information that is subject to verification during the authentication of the organization identity includes the SIREN number, VAT declaration number, DUNS...

For the purpose of SSL certificate delivery, the verification also requires to check that the domain name featured in the request belongs to that organization, which is therefore entitled to use it. In this way, verifications are made against domain name database.

3.2.3 Authentication of Individual identity

Individual identities are authenticated using means and procedures adapted to the role the individual is assigned to.

A TC identity is checked during the validation step of the SSL certificate request, through a question & answer process realized by the RA.

An SSL administrator identity is checked by KEYNECTIS SSL CA during the registration process of the electronic certificate he is requesting for SSL administration purposes. The verification of an SSL administrator identity is based on the presentation of a government issued national ID that includes a picture of the individual that allows recognizing him.

3.2.4 Non-Verified information

Information that is not verified shall not be included in the certificates.

3.2.5 Validation of Authority

An applicant authority is checked during the registration and validation process of SSL certificates requests he proceeds to. The authentication of an applicant is based on a request sent to the ODN, whether he or she authorize or not the applicant to act as an applicant for the domain name he or she made the SSL certificate request for.

A TC authorization is verified during the retrieval of the SSL certificate by presentation of a retrieval code that was transmitted to the RA during the registration process. The retrieval code is only known from the applicant who transmits it to the TC prior to the retrieval of the SSL certificate.

AN SSL administrator authorization is also based on a document provided by the organization that gives evidence that the SSL administrator is appointed by the organization to this position.

In case an authentication of the organization or the individual is necessary, principles explained in § 3.2.2 and § 3.2.3 apply.

3.2.6 Criteria for Interoperation

A customer that obtains an SSL certificate is ensured to be certified by the KEYNECTIS SSL CA which adhered to the following requirements:



- Have a CPS mapped to, and determined by the KMA to be in conformance with the present CP
- Operate a PKI that has undergone a successful compliance audit pursuant to section 8 of this CP
- Issue SSL certificates and certificate status information compliant with the profiles described in § 7.2 below and available to the relying parties.

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 customer in the domain name whose keys have been issued. The customer identifies itself using the initial identity-proofing process as described in § 3.2 above.

3.3.2 Identification and Authentication for Re-key After Revocation

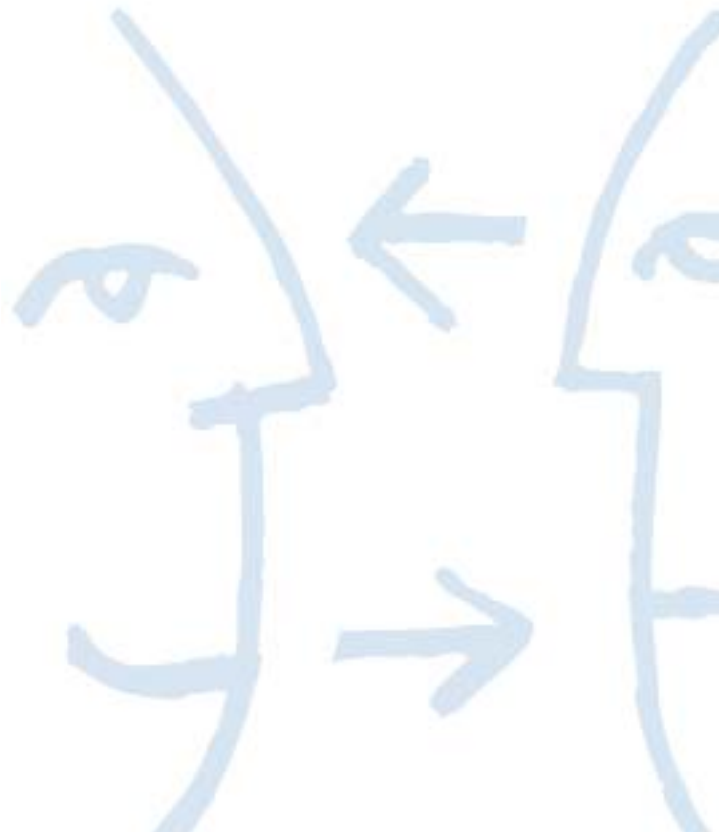
After an SSL certificate has been revoked other than during a renewal or update action, the SSL customer go through the initial registration process, such as described in § 3.2 above to obtain a new SSL certificate.

If the SSL certificate has been revoked for reason of key compromise, then the customer generates a new key pair prior to proceed to an SSL certificate application.

3.4 Identification and Authentication for Revocation Request

Revocation requests are authenticated by the RA.

Authentication procedure requires the same level of trust as defined for initial registration (refer to § 3.2.2 and § 3.2.3 above) to be sure that the certified customer has effectively requested for the revocation.



4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Origin of a certificate request

4.1.1.1 K.SSL Gold and Silver offers

Only applicants (ODN or TC) can fill SSL certificate requests.

4.1.1.2 Club SSL and ISP SSL offers

Only authorized SSL administrators can fill SSL certificate requests.

4.1.1.3 K.SSL test certificates

Anybody wishing to familiarize with SSL certificates has the opportunity to request a K.SSL test certificate from the KEYNECTIS SSL CA.

4.1.2 Enrolment Process and Responsibilities

4.1.2.1 K.SSL Gold and Silver offers

The K.SSL Gold offer enrolment process consists of two steps.

First the applicant fills in a form on KEYNECTIS SSL CA website at ssl.keynectis.com. The form includes the following fields:

- Identification of the TC, i.e. full name, including surname and given names, e-mail address, function, complete postal address, phone numbers (standard and direct numbers)
- Identification data of the organization for which an SSL certificate is requested, i.e. full name and legal status of the associated legal person and any relevant existing registration information (e.g. company registration)
- Public key in PKCS#10 format
- Domain name identification
- Duration of the SSL certificate (1 or 2 year(s))
- Secret information for KEYNECTIS SSL CA registration authority to proceed to verification of the request
- Secret code for SSL certificate retrieval by the TC.

The connection is protected (confidentiality and integrity of information,) using https protocol.

In a second step, the applicant transmits a purchase order to the KEYNECTIS SSL CA accompanied with the payment at the following address:

KEYNECTIS,
SSL Customer Service
30, Rue du Château des Rentiers,
75647 Paris Cedex 13 - FRANCE

Before entering into a contractual relationship with a customer, the KEYNECTIS SSL CA informs the customer of the terms and conditions regarding the use of the SSL certificates. These terms are included in the present CP.

4.1.2.2 Club SSL and ISP SSL offers

The organization owning a Club SSL or an ISP SSL account benefits from a dedicated interface as registration desk. To connect to this registration desk, the SSL administrator (named by the customer to act on its behalf) is authenticating using an individual electronic certificate.

Then, he accesses to a comprehensive form on the registration desk that allows

- Generation of a CSR,
- Filling of all necessary administrative information (last name, first name and e-mail address) of the applicant.



Application for SSL certificates requires entering into a contractual agreement with the KEYNECTIS SSL CA prior to the registration desk to be available.

4.1.2.3 K.SSL test certificates

The K.SSL Test certificate enrolment process consist in filling a request form on KEYNECTIS SSL CA website at: <http://ssl.keynectis.com>

The form includes the following fields:

- Identification of the TC, i.e. full name, including surname and given names, e-mail address, function, complete postal address, phone numbers (standard and direct numbers);
- Identification data of the organization for which an SSL certificate is requested, i.e. full name and legal status of the associated legal person and any relevant existing registration information (e.g. company registration);
- Public key in PKCS#10 format;
- Domain name identification;
- Secret code for SSL certificate retrieval by the TC.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

4.2.1.1 K.SSL Gold and Silver offers

Once the KEYNECTIS SSL CA has received the purchase order and the corresponding payment, the identification and authentication process starts.

The KEYNECTIS SSL CA customer service proceeds to the following operations:

- The SSL customer service checks that both the purchase order and the payment are complete and correct;
- The SSL customer service authenticates the customer organization according to § 3.2.2 above
- The SSL customer service checks customer organization owns the domain name
- The SSL customer service checks that the TC is acting on behalf of the SSL customer according to § 3.2.3 above
- The SSL customer service checks that the ODN organization accepts the SSL customer request SSL certificates for the domain names he or she owns.

The SSL customer service records all information used to check the customer's identity and, if applicable, any specific attributes, including any reference number on the documentation used for check, and any limitations on its validity.

4.2.1.2 Club SSL offer

Once the KEYNECTIS SSL CA has received the purchase order, the identification and authentication process starts.

The KEYNECTIS SSL CA customer service proceeds to the following operations:

For the delivery of SSL administrator electronic certificate:

- The SSL customer service checks the identity of the named Club SSL administrator(s)
- The SSL customer service checks the administrator has clearly been appointed by the ODN organization to act on its behalf

For the opening of the Club SSL registration desk:

- The SSL customer service authenticates the Club SSL customer organization according to § 3.2.2 above;
- The SSL customer service checks Club SSL customer organization owns the domain names it declared;
- The SSL customer service checks that the appointed SSL administrator is acting on behalf of the Club SSL customer according to § 3.2.3 above;

The SSL customer service records all the information used to check the customer's identity and, if applicable, any specific attributes, including any reference number on the documentation used for check, and any limitations on its validity.

4.2.1.3 ISP SSL offer

The identification and authentication of the ISP SSL customers is proceeded during the contractual step with the KEYNECTIS SSL CA, before the ISP SSL Customers starts SSL certificates enrolment.

The KEYNECTIS SSL CA customer service proceeds to the following operations:

- The SSL customer service authenticates the ISP SSL customer organization according to § 3.2.2 above;
- The SSL customer service checks ISP SSL customer organization is authorized to request SSL certificates for the domain names it declares;
- The SSL customer service checks that the appointed SSL administrator is acting on behalf of the ISP SSL customer according to § 3.2.3 above;
- The SSL customer service delivers an SSL administrator electronic certificate to the ISP SSL administrator;

The SSL customer service records all the information used to check the customer's identity and, if applicable, any specific attributes, including any reference number on the documentation used for check, and any limitations on its validity.

4.2.1.4 K.SSL test certificates

There is no operation realized as part of the K.SSL certificate application process.

4.2.2 Approval or Rejection of Certificate Applications

4.2.2.1 K.SSL Gold and Silver offers

Approval or rejection of SSL certificates applications are proceeded by the SSL customer service, based on the results of the actions described at § **Erreur ! Source du renvoi introuvable.** above.

When all authentication and checking operation are successful, SSL certificate requests are approved and transmitted to the KEYNECTIS SSL CA for generation.

In the meantime, an email is transmitted to the TC to notify that he or she has the possibility to proceed to the certificate retrieval.

4.2.2.2 Club SSL and ISP SSL offers

The approval of the certificate request is done by the SSL administrator.

After the SSL administrator approves an SSL certificate request, the SSL certificate request is transmitted to the KEYNECTIS SSL CA for generation.

In the meantime, an email is transmitted to the TC to notify that he or she has the possibility to proceed to the certificate retrieval.

4.2.2.3 K.SSL test certificates

K.SSL test certificates requests are automatically approved as far as the request form is completely and correctly filled in.

4.2.3 Time to Process Certificate Applications

4.2.3.1 K.SSL Gold and Silver offers

The time to process the identification and authentication process of an SSL certificate request is equal to 48 hours business time provided that the customer service was able to proceed to all required verifications and validations.

4.2.3.2 Club SSL and ISP SSL offer

SSL administrators are in charge of the approval of the certificate requests on behalf of the organization that appointed them. The time to process certificate application is given by the customer himself since he is in charge of the validation.

4.2.3.3 K.SSL test certificates

As far as the K.SSL application form is approved (automatically), the applicant receives an e-mail that notifies the URL where to retrieve the K.SSL test certificate.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance (K.SSL Gold and Silver offers, Club SSL and ISP SSL offers)

Before generating the SSL certificate, the KEYNECTIS SSL CA checks that the certificate to be signed has all fields and extensions properly populated.

The TC that proceeds to the retrieval authenticates himself to download the certificate, using the retrieval code that was transmitted to the KEYNECTIS SSL CA during the application process.

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 components.

4.3.1.1 K.SSL test certificates

The TC that proceeds to the retrieval authenticates himself to download the certificate, using the retrieval code that was transmitted to the KEYNECTIS SSL CA during the application process.

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 components.

4.3.2 Notifications to Customer by the CA of Issuance of Certificate

When an SSL certificate has been generated and retrieved, the TC and the SSL administrator (in case of a Club SSL and ISP SSL offer) is / are notified of the SSL certificate retrieval.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

As soon as the TC has downloaded its SSL certificate, then KEYNECTIS SSL CA considers that the certificate has been accepted.

4.4.2 Publication of the Certificate by the CA

SSL certificates issued by the KEYNECTIS SSL CA are not published by the KEYNECTIS publication service.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The applicant, the TC and the SSL administrator (in case of a Club SSL or an ISP SSL offer) are notified that an SSL certificate has been issued for the domain name(s) they are in charge of.

The KEYNECTIS SSL CA customer service is also informed that an SSL certificate was issued.

4.5 Key Pair and Certificate Usage

4.5.1 SSL Private Key and Certificate Usage

The SSL key pair is used to set SSL protocol.



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 by the SSL certificate extensions (such as key usage, extended key usage, certificate policies, etc.) and to authenticate the trusted common identity of the “SSL services” according to the present CP.

4.6 Certificate Renewal

This section describes SSL certificate renewal, without changing public keys or any other information included in certificates. Only the validity period and the serial number are change.

4.6.1 Circumstances for Certificate Renewal

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 revoked or compromised and the domain name and attributes are unchanged. In addition, the validity period of the certificate must not exceed the remaining lifetime of the private key, as specified in section 5.6. The RA shall check the existence and validity of the certificate to be renewed and that the information used to check the identity and attributes of the subject is still valid according to the same procedure as defined in sections 3.2.2 and 3.2.3 or with the procedures that have the same level of trust.

This operation is possible only if the key re-used in the certificate is still compliant with applicable cryptographic security recommendation for key size length.

The KEYNECTIS SSL CA sends warning messages to the customer to inform him on the incoming expiration of its SSL certificate (cf. section 4.1.1).

4.7 Certificate Re-Key

This section deals with the generation of a new certificate with changing of the public key contained in the certificate.

More often a key is used the more susceptible it is to loss or discovery. That is the reason why the key has to be periodically changed. Re-keying a certificate means that a new certificate is created according to the present CP. The KEYNECTIS SSL CA sends a warning message to the TC to alert him/her on the incoming expiration of its SSL certificate.

4.8 Certificate Modification

This section deals with the generation of a new certificate keeping the same key. This operation is possible only if the public key re-used in the certificate is still compliant with the applicable cryptographic security recommendations for key size length.

Changes in the identity contained in the SSL certificate are possible circumstances for certificate modifications.

4.9 Certificate Revocation and Suspension

Certificate revocation and suspension services are not proposed for K.SSL test certificates.

4.9.1 Circumstances for Revocation

An SSL certificate is revoked when the binding between it and the public key it includes is considered no longer valid. Examples of circumstances that invalidate the binding are:

- End of the KEYNECTIS SSL CA services;
- KEYNECTIS SSL CA can be shown to have violated the stipulations of its agreement with KEYNECTIS;
- Change in the key length size coming from regulatory body or international standard institute;
- KEYNECTIS SSL CA is revoked;
- The domain name registration or the organization's name changed and the applicant is no longer authorized to use the domain name;



- DN information filled incorrectly;
- The SSL certificate corresponding to the private key has been lost or compromised;
- The applicant has used a wrong DN in his initial request;
- The ODN organization wants to revoke the SSL certificate.

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

4.9.1.1 Origin of Revocation Request (K.SSL Gold and Silver offers, Club SSL and ISP SSL offers)

The TC and the SSL administrator (in case of a Club SSL or an ISP SSL offer) have authority to make revocation requests for the following reasons:

- The domain name registration or the organization's name changed and the applicant is no longer authorized to use the domain name;
- DN information filled incorrectly;
- The SSL certificate corresponding to the private key has been lost or compromised;
- The applicant has used a wrong DN in his initial request;
- The ODN organization wants to revoke the SSL certificate.

KEYNECTIS SSL CA has authority to make revocation requests for the following reasons:

- End of the KEYNECTIS SSL CA services;
- The KEYNECTIS SSL CA can be shown to have violated the stipulations of its agreement with KEYNECTIS;
- The KEYNECTIS SSL CA is revoked.

4.9.2 Procedure for Revocation Request

4.9.2.1 K.SSL Gold and Silver offers

The TC transmits a revocation request form to the SSL customer service that contains at a minimum:

- His or her personal identification;
- The secret information that was previously used to proceed to TC identity verification during registration process.

The revocation request is transmitted either online at support_ssl@keynectis.com, either by fax at the SSL customer services fax number +33(0)1 53 94 22 98.

The SSL customer service authenticates and authorizes revocation requests. In case the authentication is successful, the SSL customer service transmits the revocation request to KEYNECTIS SSL CA that authenticates the SSL customer service and revokes the SSL certificate (using the CA private key).

All the operation 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 components.

Once the SSL certificate is revoked, the KEYNECTIS SSL CA notifies the TC of the change of the SSL certificate status. Once a certificate is revoked it is not re-certified.

4.9.2.2 Club SSL and ISP SSL offers

TC or the SSL administrator transmits a revocation request form to the KEYNECTIS SSL CA that contains at a minimum:

- His or her personal identification;
- The secret information that was previously used to proceed to TC identity verification during registration process.

The revocation request is transmitted either online at support_ssl@keynectis.com, either by fax at the SSL customer services fax number +33(0)1 53 94 22 98.

The SSL customer service authenticates and authorizes revocation requests. In case the authentication is successful, the SSL customer service transmits the revocation request to KEYNECTIS SSL CA that authenticates the SSL customer service and revokes the SSL certificate (using the CA private key).All the operation 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 components.

Once the SSL certificate is revoked, the KEYNECTIS SSL CA notifies the TC and the SSL administrator of the change of the SSL certificate status. Once a certificate is revoked it is not re-certified.

4.9.3 Revocation Request Grace Period

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

4.9.4 Time within Which CA Must Process the Revocation Request

Online revocation management services are available 24 hours a day, 7 days a week.

SSL customer services for revocation are available during from 9:00 am to 06:00 pm Monday to Friday, except during bank holiday

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

4.9.5 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 the relying party. If it is temporarily infeasible to obtain revocation information, then the relying party either rejects use of the certificate, or makes an informed decision to accept the risk, responsibility, and consequences for using a certificate, i.e. certification path provided according the present CP, whose authenticity cannot be guaranteed to the standards of this CP. Such use may occasionally be necessary to meet urgent operational requirements.

4.9.6 CRL Issuance Frequency

CRL are issued every 24 hours. They are rendered available 24 hours per day, 7 days a week, by the KEYNECTIS PS. Even if there are no changes or updates to be made to ensure timeliness of information. KEYNECTIS SSL CA ensures that superseded CRL are removed from the repository upon posting of the latest CRL. Upon system failure, service or other factors which is not under the control of KEYNECTIS SSL CA, KEYNECTIS SSL CA makes best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the certification practice statement.

4.9.7 Maximum Latency for CRL

The maximum delay between the time an SSL certificate is revoked by the KEYNECTIS SSL CA and the time that this revocation information is available to relying parties is no longer than 24 hours.

4.9.8 On-Line Revocation/Status Checking Availability

No stipulation.

4.9.9 On-Line Revocation Checking Requirements

No stipulation.

4.9.10 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.11 Special Requirements regarding Key Compromise

There is no specific requirement more than those specified in section 4.9.3.

4.9.12 Circumstances for Suspension

Not applicable.

4.9.13 Who Can Request Suspension

Not applicable.

4.9.14 Procedure for Suspension Request

Not applicable.

4.9.15 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 § 2.

4.10.2 Service Availability

The certificate information status is available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the KEYNECTIS SSL CA, the KEYNECTIS SSL CA shall make best endeavours to ensure that this information service is not unavailable for longer than 4 (four) hours.

4.10.3 Optional Features

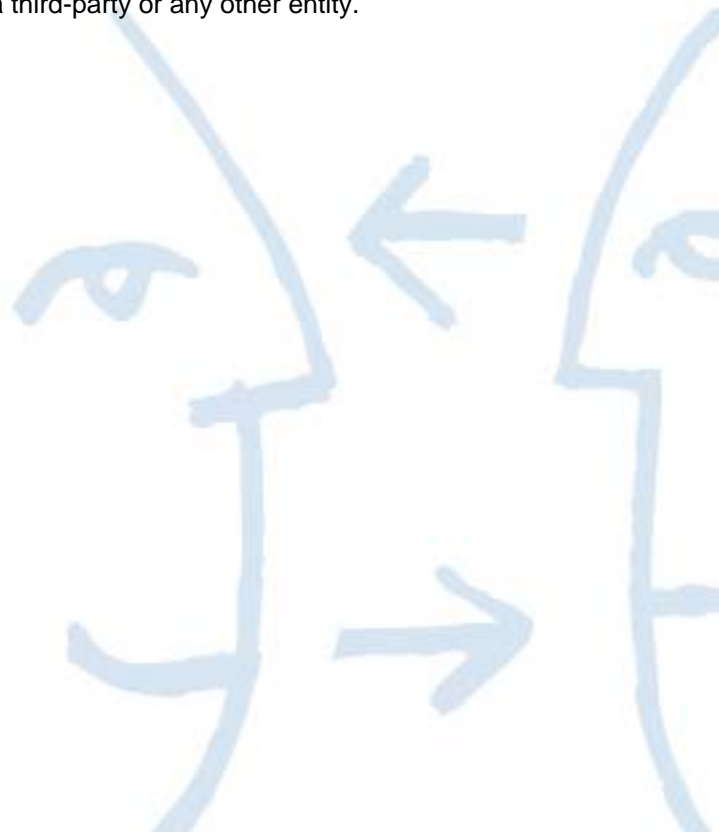
No stipulation.

4.11 End of Subscription

SSL certificates that have expired prior to or upon end of subscription are revoked. When the customer ends his relationship with the KEYNECTIS SSL CA, then the entire guarantee provided under the present CP on the SSL certificate is no longer applicable and all certificates are revoked.

4.12 Key Escrow and Recovery

Under no circumstances an SSL certificate key is escrowed by a third-party or any other entity.





5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

KEYNECTIS SSL CA physical and environmental security policy for systems used for SSL certificate life cycle management addresses 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

EYNECTIS SSL CA critical and sensitive information processing facilities are housed in secure areas with appropriate security barriers and entry controls. They are physically protected from unauthorized access, damage and interference. The protections provided are commensurate with the identified risks in the KEYNECTIS SSL CA risk analysis.

5.1.2 Physical Access

The facilities used for SSL certificate life cycle management are operated in an environment which physically protects the services from compromise through unauthorized access to systems or data. Any unauthorized persons entering this physically secured area are always accompanied by an authorized KEYNECTIS SSL employee. Physical protections are achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the systems hosting the operation. No parts of the KEYNECTIS SSL CA premises are shared with other organizations within this perimeter.

5.1.3 Power and Air Conditioning

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

5.1.4 Water Exposures

KEYNECTIS SSL CA ensures that the KEYNECTIS SSL CA system is protected from water exposure.

5.1.5 Fire Prevention and Protection

KEYNECTIS SSL CA ensures that the KEYNECTIS SSL CA system is protected with a fire suppression system.

5.1.6 Media Storage

Media used within the KEYNECTIS SSL CA are securely handled to protect them 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 in accordance with requirements of the information classification scheme and media containing sensitive are securely disposed of when no longer required.

5.1.7 Waste Disposal

All media used for the storage of information such as keys, activation data or KEYNECTIS SSL CA files are de-classified or destroyed before released for disposal.

5.1.8 Off-Site Backup

Full system backups of KEYNECTIS SSL CA, sufficient to recover from system failure, are made periodically as described in corresponding 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. Back-up 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 KEYNECTIS SSL CA equipment). The backup are stored at a site with physical and procedural controls commensurate to that of the operational KEYNECTIS SSL CA.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted roles involved on the KEYNECTIS SSL CA operation include are:

- 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 KEYNECTIS SSL CA systems used for SSL certificate life cycle management;
- Operator: Responsible for operating the KEYNECTIS SSL CA systems on a day to day basis. Authorized to perform system backup and recovery;
- Auditor: Authorized to view archives and audit logs of the KEYNECTIS SSL CA trustworthy systems;
- KEYNECTIS SSL CA activation data holder: authorized person that hold KEYNECTIS SSL CA activation data that are necessary for CA hardware security module operation.

5.2.2 Number of Persons Required per Task

The number of persons to provide the KEYNECTIS SSL CA services is detailed in the CPS. The goal is to guarantee the trust for all services of KEYNECTIS SSL CA (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 above.

5.2.3 Identification and Authentication for Each Role

Before appointing a person to a trusted role, KEYNECTIS SSL CA runs a background check.

Each person that has a role, as describe in the present CP, is identified and authenticated in a manner to guarantee that the right person has the right role to support the KEYNECTIS SSL CA. The CPS describes the mechanisms that are used to identify and authenticate people appointed to trusted roles.

5.2.4 Roles Requiring Separation of Duties

Roles separation may be enforced either by the KEYNECTIS SSL CA equipment, or procedurally or by both means.

Individual KEYNECTIS SSL CA personnel are specifically designated to the five roles defined in section 5.2.1 above. It is forbidden to own 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 or Administrator.

No individual shall be assigned more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

KEYNECTIS SSL CA employs a sufficient number of personnel which possess the expert knowledge, experience and qualifications necessary for the offered services, as appropriate to the job function. KEYNECTIS SSL CA 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 KEYNECTIS SSL CA CPS, are documented in job descriptions and clearly identified. KEYNECTIS SSL CA



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. KEYNECTIS SSL CA personnel shall be formally appointed to trusted roles by senior management responsible for security.

The job descriptions include skills and experience requirements. Managerial personnel are employed who 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 KEYNECTIS SSL CA personnel in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the CA operations. KEYNECTIS SSL CA 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. KEYNECTIS SSL CA 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

KEYNECTIS SSL CA ensures that all personnel performing duties with respect to the operation of KEYNECTIS SSL CA receive comprehensive training in:

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

KEYNECTIS SSL CA and RA personnel shall be retrained when changes occur in KEYNECTIS SSL CA or RA systems. Refresher training shall be conducted as required and KEYNECTIS SSL CA 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 KEYNECTIS SSL CA 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

KEYNECTIS SSL CA ensures that any change in the staff will not affect the operational effectiveness of the service or the 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 for KEYNECTIS SSL CA operation, have to perform KEYNECTIS SSL CA functions operations according to the same requirements than KEYNECTIS personnel.

5.3.8 Documentation Supplied to Personnel

KEYNECTIS SSL CA makes available to its personnel the present CP, 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 is 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

Audit log files are generated for all events relating to the security and services of the KEYNECTIS SSL CA components. Where possible, the security audit logs shall be automatically collected. Where 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.

KEYNECTIS SSL CA ensures all events relating to the life cycle of certificates are logged in a manner to ensure the imputability to a person in a trusted role of an action required for KEYNECTIS SSL CA services. The CPS gives details on what is logged. At a minimum, each audit record includes the following (either recorded automatically or manually) elements:

- The type of event,
- The date and time the event occurred,
- Success or failure where appropriate,
- The identity of the entity and/or operator that caused the event,
- The identity for which the event is addressee ;
- The cause of the event.

5.4.2 Frequency of Processing Log

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

5.4.3 Retention Period for Audit Log

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

5.4.4 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 date 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.

5.4.5 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 log backup are protected with the same level of trust than the one defined for the original log.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system is internal to KEYNECTIS SSL CA components. Audit processes are invoked at system start up and end only at system shutdown. The audit collection system ensures integrity and availability of the data collected. If necessary, the audit collection system protects the data in confidentiality. In case a problem occurs during the process of the audit collection system then KEYNECTIS SSL CA determines whether to suspend KEYNECTIS SSL CA operation until the problem is solved and inform the impacted components.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

The Auditor explains all significant events in an audit log summary. Such reviews involve 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

CA 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:

- KEYNECTIS SSL CA events records;
- KEYNECTIS SSL CA audit documentation;
- KEYNECTIS SSL CA CP document;
- KEYNECTIS SSL CA CPS documents;
- Any contractual agreements between an SSL certificate customer and KEYNECTIS SSL CA (Club and ISP SSL offers);
- System equipment configuration;
- Certificates and CRLs (or other revocation information);
- Other data or applications sufficient to verify archive contents;
- All work related communications to or from KEYNECTIS SSL CA and compliance auditors.

5.5.2 Retention Period for Archive

The minimum retention period for archive data is 10 years.

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

If a time stamping service is used to date the records, then it has to respect the requirements defined in section 6.8.

5.5.6 Archive Collection System (Internal or External)

The archive collection system respects the security requirements defined in section 5.3.

5.5.7 Procedures to Obtain and Verify Archive Information

Media storing of KEYNECTIS SSL CA archive information are checked upon creation. Periodically, statistical samples of archived information are tested to check the continued integrity and readability of the information.



Only authorised KEYNECTIS SSL CA equipment, trusted role and other authorized person (legal person ...) are allowed to access the archive.

5.6 Key Changeover

5.6.1 SSL certificate

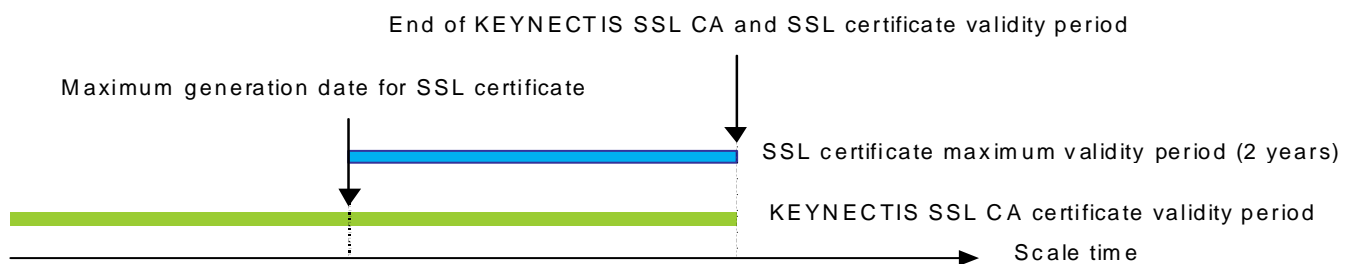
The validity period of an K.SSL test certificate is 14 days.

The validity period of an SSL certificate is 1 or 2 year(s).

It is recommended that SSL certificates issued with a 2 year(s) validity period are generated using a key which is 2048 bits long for the RSA algorithm.

5.6.2 KEYNECTIS SSL CA certificate

KEYNECTIS SSL CA cannot generate SSL certificates with an expiration date that exceeds the SSL CA certificate expiration date. As a consequence, KEYNECTIS SSL CA key pair are renewed at the latest 2 (two) years before the current SSL CA certificate expires.



As soon as a new KEYNECTIS SSL CA key pair is generated, only the new SSL CA private key is used to sign SSL certificates and CRL.

The previous SSL CA certificate stay valid for validation process of certification path until the SSL certificates are all expired.

KEYNECTIS SSL CA key changes are compliant with applicable cryptographic security recommendations for key size length or if it is compromised.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

KEYNECTIS SSL CA established business continuity procedures for the KEYNECTIS SSL CA 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 KEYNECTIS SSL CA services. KEYNECTIS SSL CA 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 ...). This business continuity is in the scope of the audit process as described in section 8 to validate what are the operations that are first maintained after a disaster and the recovery plan.

KEYNECTIS SSL CA person that owns a trusted role and operational role are specially trained to operate according to the procedures defined in the SSL CA disaster recovery plan for the most sensitive activities.

If a KEYNECTIS SSL CA 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 KEYNECTIS SSL CA in order to determine if the KEYNECTIS SSL CA needs to be rebuilt, only



some certificates need to be revoked, and/or the SSL CA needs to be declared compromised, and which services has to be maintained (revocation and certificate status information) and how according to the KEYNECTIS SSL CA disaster recovery plan.

The KEYNECTIS SSL CA is notified if suspected or detected compromise (logical, physical, electric ...) of a KEYNECTIS SSL CA system that would have compromised or will compromise or disturb the KEYNECTIS SSL CA services. This will allow KEYNECTIS SSL CA to activate their own disaster recovery plan to protect their interests and those of the relying parties.

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

If KEYNECTIS SSL CA 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 certificates status information according to the KEYNECTIS SSL CA disaster recovery plan.

5.7.3 Entity private key compromise procedures

In case a KEYNECTIS SSL CA signature key is compromised, lost, destroyed or suspected to be compromised:

- KEYNECTIS SSL CA, after investigation on the "key-problem" decides that the KEYNECTIS SSL CA certificate is revoked;
- All the SSL certificates issued by the compromised KEYNECTIS SSL CA are notified at the earliest feasible time that they may decide to revoke or not their SSL certificates and how to use in consequence their SSL certificates according to their business application;
- A new KEYNECTIS SSL CA key pair is generated;
- In case a new KEYNECTIS SSL CA certificate is generated, KEYNECTIS SSL CA proposes its SSL certificate customers to decide to re-generate or not new SSL certificates.

5.7.4 Business continuity capabilities after a Disaster

The disaster recovery plan deals with the business continuity as described in section 5.7.1. The PS containing certificates and certificate status information is deployed so as to provide 24 hours per day, 365 days per year availability (with rate of 99.95% availability excluding planned maintenance operation).

5.8 SSL CA component termination

In the event of termination of a KEYNECTIS SSL CA, the KEYNECTIS SSL CA requests to the KEYNECTIS RCA that issued its certificate to revoke it

In the event of a KEYNECTIS SSL CA termination, the KEYNECTIS SSL CA provides notice to all customers prior to the termination and:

- Stops delivering SSL certificates according to and referring to the present CP
- Archives all audit logs and other records prior to termination;
- Destroys all its private keys upon termination;
- Ensures archive records are transferred to an appropriate authority such as a CA that delivers identical services;
- Uses secure means to notify the customers to delete all trust anchors representing the SSL CA and takes care about their application.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

KEYNECTIS SSL CA key generation is undertaken in a physically secured environment by personnel in trusted roles under, at least, dual control, holder of CA secret data activation and witness. KEYNECTIS SSL CA key generation is carried out within a device which either: at least certified ISO 15408 Common Criteria at EAL 4+ level or above.

6.1.2 Private Key Delivery to Customer

SSL certificate customers generate cryptographic key whose the corresponding public key is contained in the certificate request provided to the KEYNECTIS SSL CA.

6.1.3 Public Key Delivery to Certificate Issuer

SSL certificate customers public keys are delivered securely (protected in integrity proof of origin) to the KEYNECTIS SSL CA for certificate issuance by the RA. The delivery mechanism binds the TC checked identity to its public key to be certified.

6.1.4 CA Public Key Delivery to Relying Parties

SSL CA certificates are available to relying parties by including them in the PS.

6.1.5 SSL certificate Key Size

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

SSL certificate customers generate RSA key pairs which are at a minimum 1024 bits long (recommended key length is 2048 bits for the RSA algorithm). KEYNECTIS SSL CA cannot approve SSL certificate key size which are less than 1024 bit long for the RSA algorithm.

It is recommended to use the RSA algorithm with SHA-1 hash function.

6.1.6 Public Key Parameters Generation and Quality Checking

SSL certificate customers generate key according to the technical requirements of the key generator they use and in a manner that it ensures there is no trace at all of any of information that it could be used to deduce the private key.

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

SSL certificates private key usage is defined in the certificate profile (See section 7.1 below). The key usage is set to only allow private key and corresponding SSL certificate to establish SSL connections.

This restriction is implemented in the certificate using the extension “Key usage”.

6.2 Private Key Protection and Cryptographic Module Engineering

SSL certificates keys are generated by the SSL customers using cryptographic service providers offered by the workstation or server on which they generate the key pair, in accordance with the conditions of use of the workstation or server.

6.2.1 Cryptographic Module Standards and Controls



KEYNECTIS SSL CA hardware security module is certified ISO 15408 Common Criteria at EAL 4+ level or above. SSL certificate customers are responsible for the choice of the security module (software, hardware ...) they use to generate, use and store their private keys.

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

KEYNECTIS SSL CA activates its private key for each cryptographic operation with multi-person control (using CA activation data) performing duties associated with their trusted roles. The trusted roles permitted to participate in this private key multi-person controls are strongly authenticated (i.e. token with PIN code).

The TC is responsible to protect and control the private keys of the SSL certificate customer he/she act on behalf of, in a manner to be sure that only authorized use of it is made.

6.2.3 Private Key Escrow

KEYNECTIS SSL CA private keys are never escrowed for any reason.

6.2.4 Private Key Backup

The KEYNECTIS SSL CA private keys are backed up under the same multi-person control as the original private key for disaster recovery plan purposes.

6.2.5 Private Key Archival

KEYNECTIS SSL CA private keys are not archived.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

KEYNECTIS SSL CA private keys are generated activated and stored in a hardware security module. When private keys are outside the hardware security module (either for storage or transfer), they are encrypted using the AES or the Triple DES algorithm. A ciphered private key can't be deciphered other else than in a cryptographic module under multiple control with trusted role.

6.2.7 Private Key Storage on Cryptographic Module

KEYNECTIS SSL CA private key are stored with same level of trust and operational mechanisms than the original cryptographic module.

6.2.8 Method of Activating Private Key

KEYNECTIS SSL CA private key is activated under the necessary minimum 4 persons in trusted roles, among them are activation data holders.

6.2.9 Method of Deactivating Private Key

KEYNECTIS SSL CA hardware security modules that have been activated are not left unattended or otherwise available to unauthorized access. During the time the KEYNECTIS SSL CA cryptographic module is on-line operational it is only used to sign SSL certificates and CRL from authenticated RA. When a KEYNECTIS SSL CA is no longer operational private key are removed from the hardware security module.

6.2.10 Method of Destroying Private Key

KEYNECTIS SSL CA private keys are destroyed when they are no longer needed or when the certificates to which they correspond expired or are revoked. Destroying private key requires destroying all associated CA secret activation data in a manner that not any information can be used to deduce any part of the private key.

6.2.11 Cryptographic Module Rating



KEYNECTIS SSL CA hardware security modules are certified ISO 15408 Common Criteria at EAL 4+ level or above.

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 process, as describe in section 5.5.2 above.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The KEYNECTIS SSL CA and SSL certificate have validity periods defined in the CP in accordance with section 5.6.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of KEYNECTIS SSL CA activation data used to activate KEYNECTIS SSL CA private keys are made during a key ceremony (Refer to section 6.1.1). Activation data are generated automatically and delivered to the holder who is a person in trusted role, in a manner to keep the confidentiality and the integrity of the activation data.

SSL certificate customers ensure that its key pairs are protected by appropriate means.

6.4.2 Activation Data Protection

KEYNECTIS SSL CA activation data are protected from disclosure by a combination of cryptographic and physical access control mechanisms. KEYNECTIS SSL CA activation data are stored in smart cards..

SSL certificate customers ensure that their activation data are protected in a manner that the private key is only activated by the sole authorized entity (person and/or machine).

6.4.3 Other Aspects of Activation Data

KEYNECTIS SSL CA activation data are only held by KEYNECTIS personnel in trusted roles. Any other specific requirement for activation data is detailed in the KEYNECTIS SSL CA CPS.

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 systems, software, and physical safeguards. The KEYNECTIS SSL CA PKI components includes the following functionalities:

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

When an KEYNECTIS SSL CA PKI equipment is hosted on an evaluated platform 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 KEYNECTIS SSL CA PKI component software has to be compliant with the requirements of the protection profile from the French infosec agency (PP_IGC, PP_AC and PP_AE available at www.ssi.gouv.fr).

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The System Development Controls for the KEYNECTIS SSL CA 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 process 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. KEYNECTIS SSL CA 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

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

6.6.3 Life Cycle Security Controls

KEYNECTIS SSL CA keeps watching on the maintenance scheme requirements to keep the level of trust of software and hardware that are evaluated and certified,

6.7 Network Security Controls

KEYNECTIS SSL CA PKI components implements appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of guards, firewalls and filtering routers. Unused network ports and services are turned off. Any boundary control devices used to protect the network on which PKI equipment are hosted deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 Time-Stamping

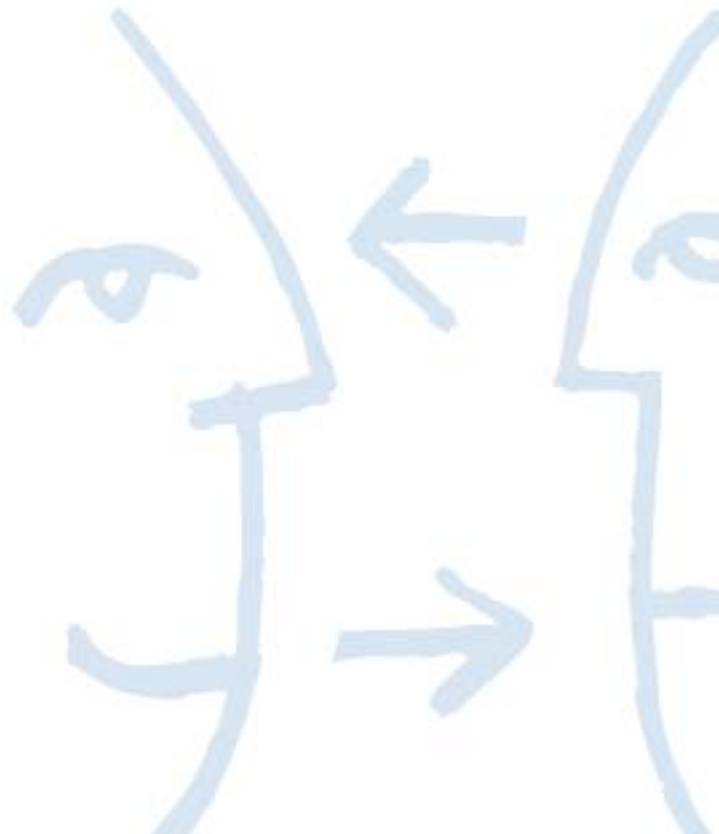
All KEYNECTIS SSL CA components are regularly synchronized with a time service such as an Atomic Clock or Network Time Protocol (NTP) Service. A dedicated authority (Time stamping authority) may be used to provide this trusted time. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a CA's Certificate;



- Revocation of a CA's Certificate;
- Posting of CRL updates.

Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events.



7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

The SSL certificates are X.509 v3 certificates (populate version field with integer "2").
The certificate fields are those defined in the RFC 3280.

7.1.1 Certificate Extensions

For an SSL certificate, at a minimum the following extensions are used:

- Authority Key Identifier;
- Key usage;
- Subject Key Identifier;
- CRL Distribution Points;
- Basic Constraints.

CPS will give details on the certificate for the other extensions.

7.1.2 Algorithm Object Identifiers

It is sha-1WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}.

7.1.3 Name Forms

The name form follows the requirements described in the section 3.1.

7.1.4 Certificate Policy Object Identifier

The SSL certificate contains the OID defined in the KEYNECTIS SSL CA CP.

7.1.5 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.6 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

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

7.2.1 CRL and CRL Entry Extensions

CPS will give details on CRL extension fields (CRL number and authority key identifier).

7.3 OCSP Profile

If an OCSP is used, then it is conformed to RFC2560.

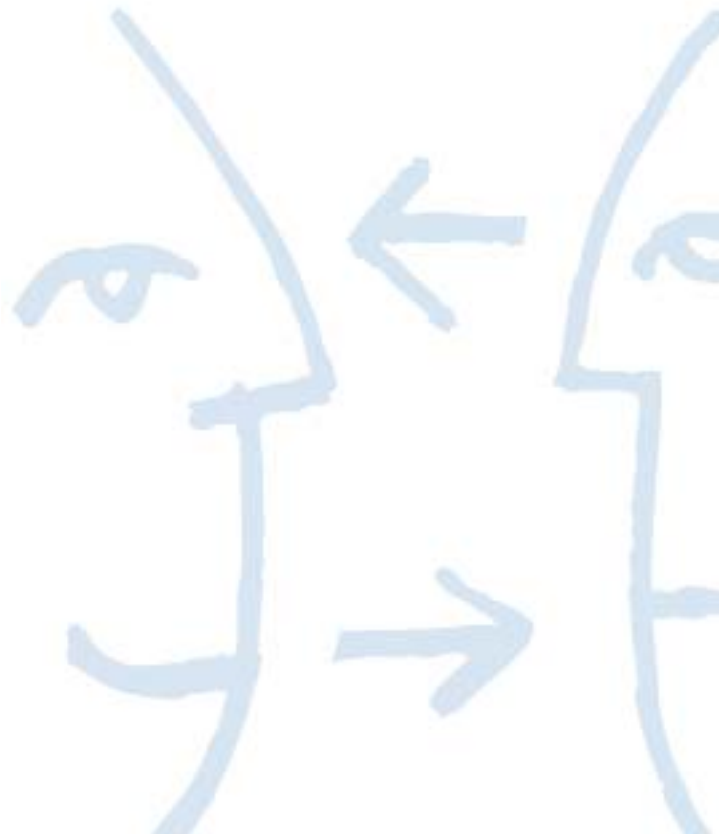
7.3.1 Version Number(s)



Version 1 of the OCSP specification as defined by RFC2560 is supported.

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 KEYNECTIS SSL CA PKI is subject to periodic compliance audits to allow KEYNECTIS SSL RCA to authorize or not (regarding the audit result) KEYNECTIS SSL CA to operate under this CP.

The KMA has the right to require and make a compliance audit of the KEYNECTIS SSL CA PKI and other entities (for instance the RA) that operate under the present CP.

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 compliance auditor must perform such compliance audits as a primary responsibility. The KEYNECTIS SSL CA looks carefully, regarding its own audit requirements base, to the method employed to audit the entities acting as part of the PKI. KEYNECTIS SSL CA selects itself the auditor.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor either is a private firm, which is independent from the entity being audited, or it is 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 is to verify that a component operates in accordance with processes compliant with the present CP and the associated CPS.

8.5 Actions Taken as a Result of Deficiency

The KMA may determine that a KEYNECTIS SSL CA or entity acting on behalf of the KEYNECTIS SSL CA operates in compliance or not with the obligations set forth in this CP. When such a determination is made and according to the non-compliance severity, the KEYNECTIS SSL CA may:

- Stop its activity, or
- suspend operation of the noncompliant KEYNECTIS SSL CA component, or
- stop relation with the affected entity acting on behalf of the KEYNECTIS SSL CA, or
- Decide that corrective actions have to be taken which allow continuing.

When the auditor finds a discrepancy between how the SSL CA is designed or is being operated or maintained and the requirements of this CP, the following actions shall be performed:

- The compliance auditor notes the discrepancy;
- The compliance auditor notifies the Entity where the discrepancy is identified of the discrepancy. The Entity shall notify the KMA promptly;
- The party responsible for correcting the discrepancy determines what further notifications or actions are necessary pursuant to the requirements of this 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 KEYNECTIS SSL CA may decide to stop temporarily operation of a KEYNECTIS SSL CA, to revoke a certificate issued by the RCA, or take other actions it deems appropriate.

8.6 Communications of Results

The Audit Compliance Report, including identification of corrective measures taken or being taken by the component, is provided to the KMA and to KEYNECTIS SSL CA. The report identifies the versions of the CP and CPS used in the assessment. The Audit Compliance Report is not available on Internet for relying party.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

K.SSL Gold certificate	1 year	2 years
	380 €HT	650 €HT

Club SSL - packs	1 year	2 years
Pack 10	2 660 €HT	4 550 €HT
Pack 25	6 460 €HT	11 050 €HT
Pack 50	12 350 €HT	21 125 €HT
Pack 100	22 800 €HT	39 000 €HT
Club SSL – SSL certificates	1 year	2 years
1-12 certificates	266 €HT	455 €HT
13- 25 certificates	258 €HT	442 €HT
26- 50 certificates	247 €HT	422 €HT
51- 100 certificates	228 €HT	390 €HT
101- 200 certificates	210 €HT	376 €HT

9.1.2 Certificate Access Fees

The KEYNECTIS SSL CA PS (that contains RCA certificate and KEYNECTIS SSL CA certificate) is free access on the Internet is free of charge.

9.1.3 Revocation or Status Information Access Fees

The KEYNECTIS SSL CA PS (that contains CRL for CA's certificate and KEYNECTIS SSL CA certificate) is free of charge on the Internet. This publication is not intended to be used by OCSP services or other else similar services but only for relying party to verify if a certificate is valid or not.

9.1.4 Fees for Other Services

General conditions applying to KEYNECTIS SSL CA offers states specific fees if any.

9.1.5 Refund Policy

KEYNECTIS has a refund policy as operating a CA.

Re-issuance of K.SSL Gold or Silver certificate is only possible for an identical request, i.e. same organization, same Certificate Signing Request.

There is no additional cost for a replacement requested within 14 days of the initial request, no additional paperwork is required. From 15 to 90 days, a half applicable fee will apply, no additional paperwork is required.



Over 90 days, the replacement demand is considered as a new demand. Checks and fees are the same as for an initial K.SSL request.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

KEYNECTIS SSL CA maintains reasonable levels of insurance coverage.

9.2.2 Other Assets

KEYNECTIS SSL CA maintains reasonable sufficient financial resource to maintain operations and fulfil duties.

9.2.3 Insurance or Warranty Coverage for End-Entities

If there is a damaged for an SSL customer due to KEYNECTIS SSL CA fault then KEYNECTIS SSL CA will activate its insurance to cover part of the customer damaged in the limit of the KEYNECTIS SSL CA liability.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

KEYNECTIS SSL CA guarantees that only trusted and authorized personnel have access and use these following confidential information:

- Records and archives;
- Personal identity data;
- KEYNECTIS SSL CA private keys;
- KEYNECTIS SSL CA secret activation data;
- Audit result and reports;
- Disaster recovery plans;
- Contractual and agreement with KEYNECTIS SSL CA;
- Internal KEYNECTIS SSL CA security policy and procedures;
- Part of the CPS defined as confidential.

9.3.2 Information Not Within the Scope of Confidential Information

Information published by the PS is not considered as confidential, but is subject to protection according to applicable laws on intellectual property rights.

9.3.3 Responsibility to Protect Confidential Information

KEYNECTIS SSL CA has to respect the requirements described in the European law for the protection of personal data (confidential and personal data).

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

KEYNECTIS SSL CA operates in compliance with the European law on the management and protection of personal data and has a trusted KEYNECTIS SSL CA to be ensured to respect all the law requirements.

9.4.2 Information Treated as Private



KEYNECTIS SSL CA considers that information that are considered as private 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

KEYNECTIS SSL CA components treat and protect all private information in a manner to only authorize access to trusted roles (internal or legal entity).

9.4.5 Notice and Consent to Use Private Information

Private information cannot be used, for the purpose of SSL services, without the explicit consent of the customer. This consent is obtained when retrieving the SSL certificate, through acceptance of the KEYNECTIS SSL CA certificate delivered by the KEYNECTIS SSL CA.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

KEYNECTIS SSL CA is compliant with the national law of the registration country of the legal person, and has protected procedure to give access to the private data for legal entity with authentication and secure controlled access to those data.

9.4.7 Other Information Disclosure Circumstances

KEYNECTIS SSL CA obtains contentment from the SSL customer to transfer its private information in case of activities have to be transferred from an entity to another one, as described in the section 5.8.

9.5 Intellectual Property rights

KEYNECTIS SSL CA retains all intellectual property rights and its proprietary on the present CP and associated CPS, SSL certificate and corresponding revocation information that it issues.

The SSL customer retains all intellectual rights it has on information contained in the SSL certificate delivered by KEYNECTIS SSL CA and for which he/she is the proprietary.

9.6 Representations and Warranties

9.6.1 KEYNECTIS SSL CA Representations and Warranties

The KEYNECTIS SSL CA ensures that all requirements, as detailed in the present CP and in the corresponding CPS, are implemented as applicable to deliver and manage SSL certificates.

The KEYNECTIS SSL CA has the responsibility for conformance with the procedures prescribed in this CP, even when the KEYNECTIS SSL CA functionality is undertaken by sub-contractors. The KEYNECTIS SSL CA provides all its certification services consistent with its certification practice statement.

Common obligations for KEYNECTIS SSL CA components have to:

- Protect and guarantee integrity and confidentiality of their secret data and/or private keys;
- Only use their cryptographic keys and certificates, with associated tools specified in CPS, for what purpose they have been generated;
- Respect and operate CPS part that deals with their duty;
- Let auditors fulfil their tasks and communicate every useful information to them, control and verify the compliance with the present CP and with the applicable CPS sections;



- Respect total or part of agreements that binds it to SSL representatives;
- document their internal procedure 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 Applicant Representations and Warranties

The SSL certificate applicant has the following obligations:

- Submit accurate and complete information to the RA;
- Keep secret information used for authentication purposes with KEYNECTIS SSL CA components confidential;
- Respect the present CP

9.6.3 RA Representation and Warranties

The RA (whether it is SSL administrator or KEYNECTIS customer service) has the following obligations:

- Authenticate the Applicant;
- Proceed to all the required verification for delivery of SSL certificates;
- Authenticate the certificate request;
- Authenticate the revocation request.

9.6.4 TC Representation and Warranties

The TC has the following obligations:

- Keep the secret information used for authentication purposes during SSL certificate retrieval confidential;
- Respect the present CP;
- Exercise reasonable care to avoid unauthorized use of the SSL certificate private key and protect it in a manner to keep it confidential;
- Notify the KEYNECTIS SSL CA immediately for revocation request of the SSL certificate he/she responsible for;
- Take care about the revocation information status about KEYNECTIS SSL CA certificate or RCA certificate.

9.6.5 Representations and Warranties of Other Participants

9.6.5.1 KMA

KMA has the following obligations:

- Elaborate CP and CPS;
- Audit KEYNECTIS SSL CA and SSL CR;
- Control contractual relationship with SLL CR acting as RA.

9.6.5.2 SSL Administrator

SSL Administrator has the following obligations:

- Submit accurate and complete information to the KEYNECTIS SSL CA;
- Only use certificates received from KEYNECTIS SSL CA to act as an RA;
- Respect the present CP and the corresponding CP/CPS as an RA;
- Exercise reasonable care to avoid unauthorized use of the private key of the administrator certificate he/she owns and protect it in a manner to keep it confidential;
- Notify the KEYNECTIS SSL CA immediately for revocation request of the administrator certificate he/she owns;
- Take care about the revocation information status about KEYNECTIS SSL CA certificate or RCA certificate.

9.7 Disclaimers of Warranties

KEYNECTIS guarantee through KEYNECTIS Root CA and SSL CA:

- Identification and authentication of KEYNECTIS Root CA, with self-signed Root CA certificate;
- Identification and authentication of SSL CA, with SSL CA certificate generated by KEYNECTIS Root CA;
- Identification and authentication of domain name hosted by a server, with SSL certificate generated by SSL CA;
- Management of corresponding certificates and certificate status information regarding the present CP.



Not any more guarantee can be pinpointed by the SSL customer and relying party in their contractual relationships (if there any).

9.8 Liability limitation

Regarding the SSL certificates, KEYNECTIS SSL CA is only responsible for the present CP requirements and principles. KEYNECTIS SSL CA is responsible of any damage are caused to a customer or a relying party because of improperly operating of the present CP and corresponding CPS.

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

9.9 Indemnities

In case of a damage to KEYNECTIS' direct customer proved to be under KEYNECTIS SSL CA responsibility, the indemnities are limited to a maximum sum of money that cannot be superior to the amount invoiced for the services covering the yearly period preceding the damage. In case of a damage to the SSL certificate end-user proved to be under KEYNECTIS SSL CA responsibility, the indemnities are limited to a maximum sum of money that cannot be superior to the amount paid by the end-user for the SSL certificates he used.

9.10 Term and Termination

9.10.1 Term

The CP and its amendments become effective upon adoption by the KMA and publication by the PS.

9.10.2 Termination

A new version of the present CP accepted by KEYNECTIS SSL CA and made available by PS may oblige the KEYNECTIS SSL CA components to change their own CPS to keep compliant with the new version of the CP. According to the importance of the changes, the KMA will decide either to audit KEYNECTIS SSL or to give instruction to the KEYNECTIS SSL CA to take action to be compliant in a due delay. Depending on the importance of the CP modification, the KEYNECTIS SSL CA certificate may not have to be re-certified by anticipation.

9.10.3 Effect of Termination and Survival

End of validity of the present CP ends all the obligation and liability for the KEYNECTIS SSL CA.

9.11 Individual Notices and Communications with Participants

KEYNECTIS SSL CA provides new version of CP as soon as the KMA has validated it, via the PS.

9.12 Amendments

9.12.1 Procedure for Amendment

The KEYNECTIS SSL CA reviews its CP and CPS at least once a year. Additional reviews may be enacted at any time at the discretion of the KEYNECTIS SSL CA or on KMA requests. Spelling errors or typographical corrections which do not change the meaning of the CP are allowed without notification. The KEYNECTIS SSL CA may notify the SSL customers of any consequences of the proposed changes.

9.12.2 Notification Mechanism and Period

KEYNECTIS SSL CA notifies its components on its intention to modify CP/CPS, not less than 30 days before to enter the modification process.



9.12.3 Circumstances under Which OID Must be Changed

Present CP OID are changed if the KEYNECTIS SSL CA determines that a change in the CP modify the level of trust provided by CP requirements or CPS material to the SSL certificates it issues.

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 can't find an arrangement the problem will be solved in a French national court.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

This CP is subject to applicable French law, 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, general conditions of use of the KEYNECTIS SSL CA services and / or CPS will identify specific requirements.

9.16.2 Assignment

Except where specified by other contracts, only the KEYNECTIS SSL CA 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 KEYNECTIS SSL CA CP/CPS are to be implemented as described in CP and corresponding CPS without possible waiver of right in the intention of changing any defined rights or obligation.

9.16.5 Act of god

KEYNECTIS SSL CA is not responsible for indirect damage and interruption of services due to act of god that directly caused direct damage to SSL customers and / or relying parties.

9.17 Other Provisions

If there is any, CPS will give details.