

CERTIFICATE POLICY

Document Title : Certificate Policy for CA KEYNECTIS ICS
QUALIFIED (professional)

Auteur : Emmanuel MONTACUTELLI: 02/09/2011

Réf : DS_PC AC K.Sign ICS Qualified Pro_v1.0_GB.doc



Protecteur d'identité
Protecteur de liberté
dans un monde connecté



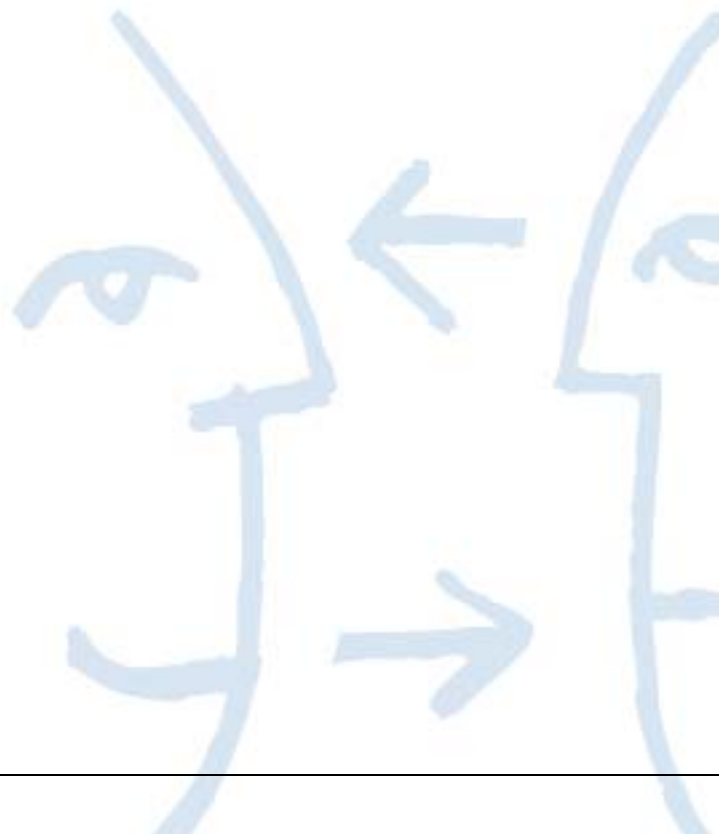


CERTIFICATE POLICY FOR AC KEYNECTIS ICS QUALIFIED (PROFESSIONAL)

Version du document :	1.0	Nombre total de pages :	43
Statut du document :	<input type="checkbox"/> Projet	<input checked="" type="checkbox"/> Version finale	
Rédacteur du document :	Emmanuel Montacutelli	KEYNECTIS	

Liste de diffusion :	<input type="checkbox"/> Externe	<input checked="" type="checkbox"/> Interne KEYNECTIS
	Public	KEYNECTIS

Historique du document :				
Date	Version	Rédacteur	Commentaires	Vérfié par
02/11/2011	1.0	EM	Passage en v1.0	





CONTENTS

WARNING	8
1 INTRODUCTION	9
1.1 Certificate policy overview	9
1.2 Identification of the certificate policy	9
1.3 The components of a Public Key Infrastructure	10
1.3.1 Administrative Authority KEYNECTIS (AAK)	10
1.3.2 Certificate Authority (CA)	10
1.3.3 Registration Authority (RA or AE)	11
1.3.4 Delegated Registration Authority (DRA or AED)	11
1.3.5 Publishing Service	11
1.3.6 Certification Operator (CO)	11
1.3.7 User, EndUser, End user	12
1.3.8 Other Actors	12
1.4 Certificate use and applications concerned by the certificate policy	12
1.4.1 Authorized uses	12
1.4.1.1 CA Certificate	12
1.4.1.2 EndUser Certificate	12
1.4.2 Prohibited uses	12
1.5 Managing the certificate policy	12
1.5.1 Entity managing the CP	12
1.5.2 Contact point	13
1.5.3 Entity determining the conformity of a CPS with this CP	13
1.6 Acronyms and definitions	13
1.6.1 List of acronyms	13
1.6.2 Definitions	13
2 OBLIGATIONS CONCERNING THE AVAILABILITY OF INFORMATION TO BE PUBLISHED	16
2.1 Entities in charge of information availability	16
2.2 Types of information published	16
2.3 Publication Lead Time and frequency	16
2.3.1 Certificate Policy	16
2.3.2 Certificate Revocation List: EndUser Certificate	16
2.3.3 Certificate Revocation List - CA Certificates	16
2.4 Controlled access to published information	16
2.4.1 Certificate Policy	16
2.4.2 Certificate Revocation List	16
3 IDENTIFICATION AND VALIDATION OF IDENTITY FOR CERTIFICATE DELIVERY	17
3.1 Naming	17
3.1.1 Name types	17
3.1.1.1 CA certificate	17
3.1.1.2 EndUser Certificate	17
3.1.2 Using explicit names	18
3.1.3 Users anonymity	18
3.1.4 Rules for interpreting various name formats	18
3.1.5 Uniqueness of names	18
3.2 Initial User enrollment and validation of requests to issue a certificate	18
3.2.1 Method for verifying private key ownership	18
3.2.2 Verification of Public or private organization identity	18
3.2.2.1 RA	18



3.2.2.2	DRA	18
3.2.2.3	Company's Authorized Representative (CAR)	18
3.2.2.4	EndUser	19
3.2.3	Verification of EndUser identity	19
3.2.3.1	No KEYNECTIS RA	19
3.2.3.2	DRA	19
3.2.3.3	Company's Authorized Representative (CAR)	19
3.2.3.4	EndUser via RA	19
3.2.3.5	EndUser via DRA	19
3.2.3.6	EndUser via DRA and CAR	19
3.2.4	Non verified Information	19
3.2.5	Validation of EndUser Authorization	19
3.2.6	Cross certification ability	19
3.3	Authentication of a renewal request	20
3.3.1	Validation in normal renewal situation	20
3.3.2	Validation after revocation	20
3.4	Authentication and validation of a revocation request	20
4	OPERATIONAL REQUIREMENTS FOR CERTIFICATE LIFECYCLES	21
4.1	Types of certificate	21
4.1.1	Origin of the certificate request	21
4.1.2	Enrollment process and responsibilities	21
4.2	Certificate request processing	22
4.2.1	Identification and Authentication	22
4.2.2	Approval or refusal of a certificate request	22
4.2.3	Time to process certificate requests	22
4.3	Certificate issuance	22
4.3.1	CA actions during certificate issuance	22
4.3.2	Notification of certificate issuance	22
4.4	Certificate acceptance	22
4.4.1	Certificate acceptance procedure	22
4.4.2	Publication of a certificate by the CA	22
4.4.3	Notification of certificate issuance by the CA to other entities	22
4.5	Key pair and certificate usage	23
4.5.1	Use of key pairs and certificates	23
4.5.2	Use of public keys and certificates by relying parties	23
4.6	Certificate renewal	23
4.7	Re-key request	23
4.8	Certificate modification	23
4.9	Certificate revocation	23
4.9.1	Circumstances for certificate revocation	23
4.9.1.1	PKI component certificate	23
4.9.1.2	EndUser certificate	23
4.9.2	Who can request revocation	24
4.9.2.1	PKI component certificate	24
4.9.2.2	EndUser certificates	24
4.9.3	Revocation request procedure	25
4.9.3.1	PKI component certificate	25
4.9.3.2	EndUser certificate	25
4.9.4	Time within which a EndUser must make a revocation request	25
4.9.5	Time limit for processing a revocation request	25
4.9.5.1	PKI component certificates	25
4.9.5.2	EndUser certificates	25
4.9.6	Revocation checking requirements for relying parties	25
4.9.7	Frequency of CRL publication	26
4.9.8	Maximum latency for CRLs	26
4.9.9	Availability of an online certificate revocation status verification system	26



4.9.10	Online revocation checking requirements.....	26
4.9.11	Other forms of revocation advertisements available.....	26
4.9.12	Special requirements related to private key compromise.....	26
4.9.13	Circumstances for suspension.....	26
4.9.14	Procedure for a suspension request.....	26
4.9.15	Limits on suspension period.....	26
4.10	Certificate status service.....	26
4.10.1	Operational characteristics.....	26
4.10.2	Service availability.....	26
4.11	End of relationship between the EndUser and the CA.....	26
4.12	Key escrow and recovery.....	27
5	NON-TECHNICAL SECURITY MEASURES FOR OPERATIONS.....	27
5.1	Physical security measures.....	27
5.1.1	Geographic location.....	27
5.1.2	Physical access.....	27
5.1.3	Energy and air conditioning.....	27
5.1.4	Exposure to liquids.....	27
5.1.5	Fire prevention and protection.....	27
5.1.6	Decommissioning of devices.....	27
5.1.7	Off-site back-ups.....	27
5.2	Procedural security measures.....	27
5.2.1	Trust-based roles.....	28
5.2.2	Number of persons required to perform sensitive tasks.....	28
5.2.3	Identification and authentication of roles.....	28
5.2.4	Roles requiring separation of scope.....	28
5.3	Staff security measures.....	28
5.3.1	Required qualifications, skills and authorizations.....	28
5.3.2	Background check procedures.....	28
5.3.3	Initial training requirements.....	28
5.3.4	Continuing training: requirements and frequency.....	29
5.3.5	Profession management.....	29
5.3.6	Penalties for unauthorized actions.....	29
5.3.7	Requirements of staff employed by external service providers.....	29
5.3.8	Documentation provided to staff.....	29
5.4	Procedures for the establishment of audit data.....	29
5.4.1	Types of events to be recorded.....	29
5.4.2	Logging process.....	30
5.4.3	Protecting event logs.....	30
5.4.4	Event log back-up procedures.....	30
5.4.5	Event log collection system.....	30
5.4.6	Vulnerability assessment.....	30
5.5	Archiving data.....	30
5.5.1	Types of data archived.....	30
5.5.2	Archive conservation period.....	31
5.5.3	Archive protection.....	31
5.5.4	Archive back-up procedures.....	31
5.5.5	DATA timestamping requirements.....	31
5.5.6	Archive collection system.....	31
5.5.7	Archive retrieval and verification procedures.....	31
5.6	Rnewal Certificate.....	31
5.6.1	CA Certificate.....	31
5.6.2	End User Certificate.....	31
5.7	Recovery following compromise or disaster.....	31
5.7.1	Incident and compromise escalation and processing procedures.....	31
5.7.2	Recovery procedures in the event of IT resource corruption (hardware, software and/or data) and in the event of the compromise of a component's private key.....	32



5.7.3	Continuity capacities following a disaster	32
5.8	End of the PKI lifecycle.....	32
6	TECHNICAL AND LOGICAL SECURITY MEASURES	33
6.1	Generation and installation of key pairs	33
6.1.1	Generation of key pairs.....	33
6.1.1.1	CA keys	33
6.1.1.2	EndUser certificate keys.....	33
6.1.2	Transfer of the private key to its owner.....	33
6.1.3	Transfer of the public key to the CA	33
6.1.4	CA publication to Third Party	33
6.1.5	Key size.....	33
6.1.6	Key parameter quality control	33
6.1.7	Key use objectives	34
6.2	Security measures for the protection of private keys	34
6.2.1	Standards and security measures for cryptographic modules.....	34
6.2.1.1	Principles	34
6.2.2	Control of the private CA key by several persons.....	34
6.2.3	Private key escrow	34
6.2.4	Back-up copy of the private key.....	34
6.2.5	Private key archiving.....	34
6.2.6	Private key activation method	34
6.2.6.1	CA key	34
6.2.6.2	En User key	34
6.2.7	Private key destruction method.....	34
6.3	Other aspects of key pair management	34
6.3.1	Public key archiving	35
6.3.2	Key pair and certificate lifecycles.....	35
6.4	Activation data	35
6.4.1	Activation data for the CA private key.....	35
6.4.2	Activation data for the EndUser private key.....	35
6.5	IT system security measures	35
6.6	System security measures throughout system lifecycle	35
6.6.1	Security measures relating to system development	35
6.6.2	Security management	35
6.7	Network security measures.....	35
6.8	Security measures for cryptographic modules.....	35
7	PROFILES OF CERTIFICATES AND CERTIFICATE REVOCATION LISTS	37
7.1	Profiles of certificates	37
7.1.1	Certificate Extensions	37
7.1.1.1	CA Certificate	37
7.1.1.2	Basic field	37
7.1.1.3	Certificate Extensions.....	37
7.1.1.4	EndUser certificate	37
7.1.1.5	Certificate Extensions.....	37
7.1.2	Identifiant d'algorithmes	38
7.1.3	Formes de noms	38
7.1.4	Identifiant d'objet (OID) de la Politique de Certification	38
7.1.5	Extensions propres à l'usage de la Politique	38
7.1.6	Syntaxe et Sémantique des qualificateurs de politique	38
7.1.7	Interprétation sémantique de l'extension critique "Certificate Policies"	38
7.2	CRL profile	38
8	CONFORMITY AUDIT AND OTHER EVALUATIONS	39
8.1	Frequency and/or circumstances of evaluations.....	39
8.2	Auditor identity and qualification	39



8.3	Relations between auditors and the entities evaluated	39
8.4	Topics covered by the evaluations.....	39
8.5	Actions taken following evaluation results	39
8.6	Communication of results	39
9	GENERAL PROVISIONS	40
9.1	Price structure	40
9.2	Financial liability.....	40
9.3	Applicable law and jurisdictions.....	40
9.4	Intellectual property rights	40
9.5	Confidentiality policy	40
9.5.1	Types of information considered to be confidential	40
9.5.2	Delivery to authorized authorities	40
9.6	Protection of personal data.....	40
9.7	Certificate policy validity period and early termination	41
9.7.1	Validity period.....	41
9.7.2	Early termination of validity	41
9.7.3	Effects of the end of validity and clauses that remain applicable	41
9.8	Administration of the certificate policy.....	41
9.8.1	Notice period.....	41
9.8.2	Delivery of notice	41
9.8.3	Modifications requiring the adoption of a new policy	41
9.9	Information procedures	41
9.10	Roles and obligations of the PKI and its components.....	41
9.10.1	Certificate Authority.....	42
9.10.2	Registration Authorities	42
9.10.3	User.....	42
9.10.4	Certificate-using applications	42
9.11	Limit of liability	42





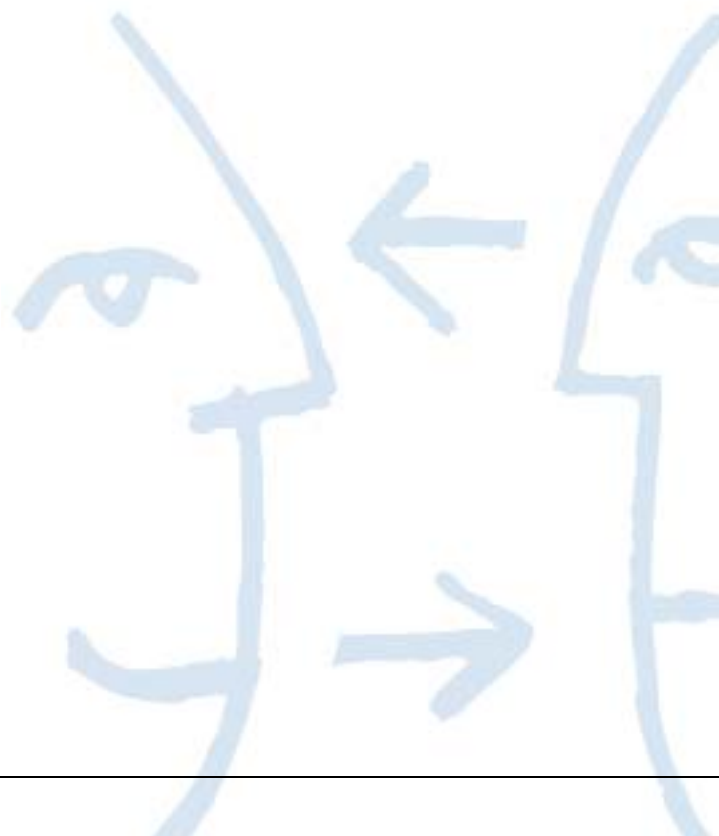
WARNING

This certificate policy is protected by the provisions of the French Intellectual Property Code of 1 July 1992, in particular by those provisions relating to literary and artistic property and copyright, as well as by all applicable international conventions and treaties. These rights are the exclusive property of KEYNECTIS.

Any reproduction or representation (excluding diffusion) of all or part of the content by any method whatsoever (in particular, electronic, mechanic, optical, photocopy, computer record) is strictly prohibited without prior express authorization from KEYNECTIS or its assigns.

Article L.122-5 of French Intellectual Property Code only authorizes: (i) "copy or reproduction that is exclusively reserved for the private use by the copier and not intended for collective use" and (ii) analyses and short quotations for the purpose of providing examples and illustrations. "Any full or partial reproduction or representation is illegal without the consent of the author or its assigns." (Article L.122-4 of French Intellectual Property Code)

Such representation or reproduction, by whatever means, is considered an infringement of copyright, punishable by Articles L. 335-2 et seq. of French Intellectual Property Code.



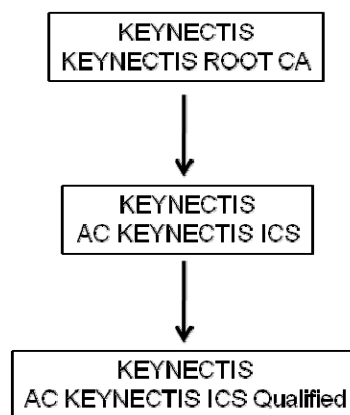
1 INTRODUCTION

1.1 Certificate policy overview

This document is the certificate policy of the company KEYNECTIS acting in its capacity as a Certificate Authority (hereafter referred to as "CA") to fulfill the need to provide Signature and Authentication mechanism through the use of electronic certificate.

Those electronic certificates are delivered by the CA named « KEYNECTIS ICS QUALIFIED 3 CA » base on PKI . This CA issue electronic certificate based on Hardware Cryptographic Module (HSM) named Token in the following document in conformity with ANSSI requirement EAL4+ and listed in the QUALIFICATIO RGS level 3 Document provided by LSTI Lab.

CA « KEYNECTIS ICS QUALIFIED CA » (Named **CA** in the present document) has been issued by CA ICS de KEYNECTIS. **CA** is included in the KEYNECTIS trust domain shown below.



Certificates issued by **CA** Are delivered to Individual People, workers of Private or public Entities. End users or EndUser are authorized only to sign electronically Document.

This Certificate Policy (CPS) describes Live Cycle Management for EndUser and **CA** certificates (Including Key pair)

Electronic Certificate issued by « KEYNECTIS ICS QUALIFIED CA » are qualified regarding ETSI 101456 requirement for Qualified signature level and RGS 3*.

This certificate policy was established based on the following documents:

-RFC 3647 document entitled "Certificate Policy and Certification Practices Framework" by the Internet Engineering Task Force (IETF).

- RFC 3647 : « X.509 Public Key Infrastructure Certificate Policy Certification Practise Statement Framework » by the Internet Engineering Task Force (IETF) ;
- Document : « Electronic Signatures and Infrastructures (ESI) ; policy requirements for certification authority issuing qualified certificates », ETSI TS 101 456, v 1.4.3 (2007- 05) ;
- Document : « X.509 V.3 Certificate Profile for, Certificates Issued to Natural Persons », ETSI TS 102 280 V1.1.1 (2004-03) ;
- Document : « Qualified Certificate profile », ETSI TS 101 862 V1.3.3 (2006-01).

1.2 Identification of the certificate policy

The corresponding certification practices statement (CPS) is referenced by OID: 1.3.6.1.4.1.22234.2.9.3.1.The certificate policy and the associated certification practices statement corresponding to the OIDs indicated above are referred to hereafter as "KEYNECTIS ICS QUALIFIED CA" Certificate policy .

1.3 The components of a Public Key Infrastructure

Preamble: Readers are reminded that the KEYNECTIS electronic certification service for the delivery of certificates requires the implementation and operation of a Public Key Infrastructure (PKI).

The functions of a PKI are broken down and detailed in this section.

The various PKI functions, coordinated by the CA and corresponding to the different stages of key pair and certificate lifecycles, are:

- Registration Certificate Service: This function receives identification and/or authentication information concerning the certificate Requester, and possibly other specific attributes, before sending the associated request to the appropriate PKI function Generation Service.
- Certificate generation Service: This function generates the certificates (template creation, electronic signature using the CA private key) using the information sent by the RA and token public key, provided by the Token cryptographic key pair generation function. Within the framework of this CP, this certificate generation function is performed by KEYNECTIS in its capacity as Certificate Authority.

Token management Service: This function manage the Token issuance including the PIN Management.

- Token delivery service : This function places the User's certificate, associated with the previously generated key pair, under the control of the User.
- Certificate revocation management function: This function provide the possibly to stop validity of the certificate Issued and Publish this information in LCR.
- Certificate status information function: This function provides the certificate-using Applications information on certificate status (revoked or valid). This function is performed by publishing updated information (Certificate Revocation List) once every 24 hours.
- Publication Service : This function provides to certificate Applicant information regarding use of certificate (LCR PC etc..)

1.3.1 Administrative Authority KEYNECTIS (AAK)

AAK is KEYNECTIS. AAK owns CA responsibility by granting conformity to RGS (referential general de security), Security Referential for CA includes PC, General condition of Use (CGU) and process used by the PKI component(s). Authorizing and acknowledging creation and Use of CA components. Submit and process Audit and control Conformity checking ability for Delegated Registration to comply with regulation.

1.3.2 Certificate Authority (CA)

The main function of the CA is to define and enforce certificate policy, thereby guaranteeing a certain level of confidence to Users. KEYNECTIS is the Certificate Authority issuing Certificates Revoking Certificate as requested by Registration Authority . As such, it manages their lifecycles while delegating to

As part of its operational functions, which it assumes directly or entrusts to external entities, the CA, in its capacity as manager of the entire PKI, must fulfill the following obligations:

- Make all services described in its CP accessible to Users and certificate-using Applications that manage and implement certificates.



- Ensure that the requirements of the CP and the procedures described in the associated CPS are applied by all of the PKI components.
- Conduct a risk analysis to determine the specific security objectives required to cover the business risks of the entire PKI, and the associated technical and non-technical security measures to be implemented. It establishes its CPS based on this risk analysis,
- Implement the various functions identified in its CP, in particular with regard to certificate generation, revocation management and certificate status updates.
- Do all that is necessary to fulfill the undertakings defined in this CP, particularly in terms of reliability, quality and security.
- Generate, and renew when necessary, its key pairs and the corresponding certificates (signing of certificates and CRLs), or have its certificates renewed if the CA is attached to a higher-ranking CA.
- Distribute its CA certificate(s) to Users and certificate-using Applications.

1.3.3 Registration Authority (RA or AE)

The RA's role is to verify the identity of the Certificate Requester in order to validate the certificate issue request.

The RA is designated and authorized by the CA on a contractual basis. Consequently, the RA implements procedures for the identification of legal entities and private individuals, in accordance with the rules it has defined based on its needs,

More specifically, the RA performs the following tasks:

- Register and verify, in compliance with defined procedures, the information concerning the certificate Requester certificate request is made.
- Establish and send the certificate request to the CA, after verifying the identity in compliance with the relevant procedures
- Preserve and protect the confidentiality and integrity of Users' personal identification data, including during operations in which this data is exchanged with the other PKI functions.
- RA has to authenticated Requesters Delegated representative (MC)
- RA is performed by KEYNECTIS

The RA provides the link between the CA and the User. It holds the User's personal data, regardless of whether or not it has had physical contact with the User during the identification procedure.

The CA has an obligation to monitor and audit the RA, in compliance with the contractual undertakings defined between the RA and the CA and with the provisions of this document.

KEYNECTIS is authorized to delegate registration Operation to Delegated Registration Authority called (AED) through legal contract describing AED obligations.

As well Keynectis is authorized to delegate All RA business to third party in charge to work in conformity with the following CPS. Condition are describe in the Legal contract signed between Keynectios and 3rd party.

1.3.4 Delegated Registration Authority (DRA or AED)

DRA can be used to implement RA business regarding End User request, revocation request, . DRA must verify identity and authentication of requester and Company's representative . DRA is managed by legal contract.

DRA cannot access to any device or function providing activation or use or any kind of access to keypair associated to the EndUser.

1.3.5 Publishing Service

This function provides to certificate Applicant information regarding use of certificate (LCR PC etc..)

1.3.6 Certification Operator (CO)



The Certification Operator provides technical services, cryptographic in particular, required to complete the certification process, in compliance with this certificate policy and the certification practices defined by the CA. The CO technically holds the private key of the CA used to sign certificates. Its sole responsibility is to comply with the procedures defined by the CA in order to fulfill the requirements of this certificate policy.

In this Certificate Policy, its role and obligations are not distinguished from those of the CA, because KEYNECTIS is its own certification operator.

1.3.7 User, EndUser, End user

Within the framework of this Certificate Policy, the User is the private individual identified by the K.Sign (KSign 101456) whose name is registered in the Certificate activated through the use of Pin Code I, order to apply his/her signature to the electronic document or mail

1.3.8 Other Actors

Certificate Applicant (UC): This is someone providing the validation of a EndUser certificate during a validation signature of document mail or Authentication

Company Authorized Representative: This is Individual person in charge of authentication of Enduser inside a company or organization. Receiving the permission to perform any function during request or revocation process in behalf of the EndUser Excepted any acces to keypair activation.

Representative roles are specified in a specific legal contract between the tree parts Company, Representative and AED

Customer : This is a legal entity wich can order K.sign devices by Keynectis or any VAR. This legal entity name will be included inside the Certificate descriptive name .

1.4 Certificate use and applications concerned by the certificate policy

1.4.1 Authorized uses

1.4.1.1 CA Certificate

CA certificate are used to authenticated EndUser certificates. Private key linked to CA certificate is used to

- Sign LCR
- Sign End User certificate

1.4.1.2 EndUser Certificate

EndUser certificates are only used to sign document, messages and authentication process in conformity with all usage described in ETSI101456.

1.4.2 Prohibited uses

Any use not included in the list of authorized uses above, as well as any unlawful and/or illegal use, is prohibited.

The CA shall not be held liable if a User uses a certificate for purposes other than those authorized in this document.

This Policy describes rules of issuance and has no value to replace Signature Policy which has to be created by any party to implement such Signature policy in respect of The ETSI101456 rules.

1.5 Managing the certificate policy

1.5.1 Entity managing the CP

The entity in charge of certificate policy administration and management is the Administrative Authority (AAK) of the CA. The AAK is in charge of producing, monitoring and modifying, whenever necessary, this Certificate Policy.



To this end, it sets up and coordinates a dedicated organization which, at regular intervals, decides whether the Certificate Policy needs to be modified.

1.5.2 Contact point

The CA's AA is the entity to be contacted should any questions arise concerning this Certificate Policy.

The authorized representative of this AA is:

Mr. Jean-Yves Faurois

Director of Quality & Security at KEYNECTIS

KEYNECTIS – 11 13 rue René Jacques – 92131 Issy les Moulineaux PARIS – FRANCE

Phone: (+33) (0)1 55 64 4 22 00

Fax: (+33) (0)1 55 64 22 01

1.5.3 Entity determining the conformity of a CPS with this CP

For aspects concerning the CA, the persons authorized to determine the conformity of the Certification Practices Statement with this certificate policy are designated by the AA, in particular on the basis of their ability to evaluate the level of security. For aspects concerning the RA, the person authorized to determine the conformity of the Certification Practices Statement with this Certificate Policy is designated by the Customer Organization, in particular on the basis of his/her ability to evaluate the level of security.

1.6 Acronyms and definitions

1.6.1 List of acronyms

AAK	Administrative Authority Keynects
CA	Certificate Authority
CAR	Company's Authorized Representative
DRA	Delegated registration authority
RA	Registration Authority
CC	Common criteria
LCR	Certificate Revocation List
DN	Distinguished name
CPS	Certification Practices Statement
PKI	Public Key Infrastructure
IETF	Internet Engineering Task Force
CO	Certification Operator
CP	Certificate Policy
URL	Uniform Resource Locator

1.6.2 Definitions

The terms below are defined as follows when they are capitalized in this Certificate Policy.

Administrative Authority (AA): The entity that represents the CA and is in charge of the Certificate Policy and the Certification Practices Statement, which it undertakes to respect and enforce. The AA's guarantee to Users and Certificate-using Applications is derived from the quality of the technology deployed and from the regulatory and contractual framework governing the uses and applications it has defined.

Certificate Authority (CA): Entity responsible for the Certificates issued and signed in its name in compliance with the rules defined in the Certificate Policy and the associated certification practices statement.



Registration Authority (RA): Entity that verifies Users' personal data. The RA is a component of the PKI and is dependant on at least one Certificate Authority. The RA's function is to receive and process requests to issue and revoke certificates.

Key pair: Pair comprising a private key (which must be kept secret) and a public key. The key pair is needed to implement a cryptology service based on asymmetric algorithms. A PKI involves two types of key pairs:

- Signature key pairs, in which the private key is used for signature and/or authentication, and the public key for verification.
- Confidentiality key pairs, in which the private key is used by an application to decrypt data, and the public key is used to encrypt this same data.

Electronic certificate: An electronic file stating that a public key belongs to the entity identified by the certificate. It is delivered by a trusted authority, the Certificate Authority. By signing the certificate, the CA validates the link between the entity and the key pair. A certificate contains information such as:

- the User's identity
- the User's public key
- the certificate's lifespan
- the identity of the certificate authority that issued it
- the signature of the CA that issued it

The X509 v3 recommendation provides a standard certificate format.

Public key: A mathematical key (formed at the same time as an associated key and mathematically linked to a private key) that is made public and used to verify the digital signature of a received piece of data that has been signed with a private key.

Private key: A mathematical key associated with the Public Key. The Private Key remains under the User's control and is used to sign electronic data.

Common Name (CN): The identity of the User (certificate EndUser). E.g. CN= John Smith.

PKI Component: Entity formed of a least one workstation, one application and one cryptographic resource, and which plays a specific role within the PKI. A component can be a CA, an RA, a CO, etc.

Certification Practices Statement (CPS): A statement of the certification practices implemented by a Certificate Authority to issue and manage Certificates.

Electronic document: Collection of structured data that can be processed by the IT applications

Timestamping: All of the services required to indicate the time and date on which events have occurred.

Public Key Infrastructure (PKI): Set of technical, human, organizational, documentary and contractual resources to ensure a secure environment for electronic exchange using asymmetric cryptographic systems. The PKI manages the Certificate lifecycle, i.e. certificate generation, distribution, management and archiving.

Integrity: The state of data that is accurate and complete. Within the framework of this document, this state is achieved in stored data by using an electronic KWS signature or integrity certificate, and in exchanged data by using an access control electronic certificate (SSL).

Certificate Revocation List (CRL): List of certificates that have been revoked before the end of their validity period.

Certification Operator (CO): A PKI component with a logically and physically secure IT platform enabling it to manage and issue certificates on behalf of the Certificate Authority, when the CA doesn't have the required technical resources.



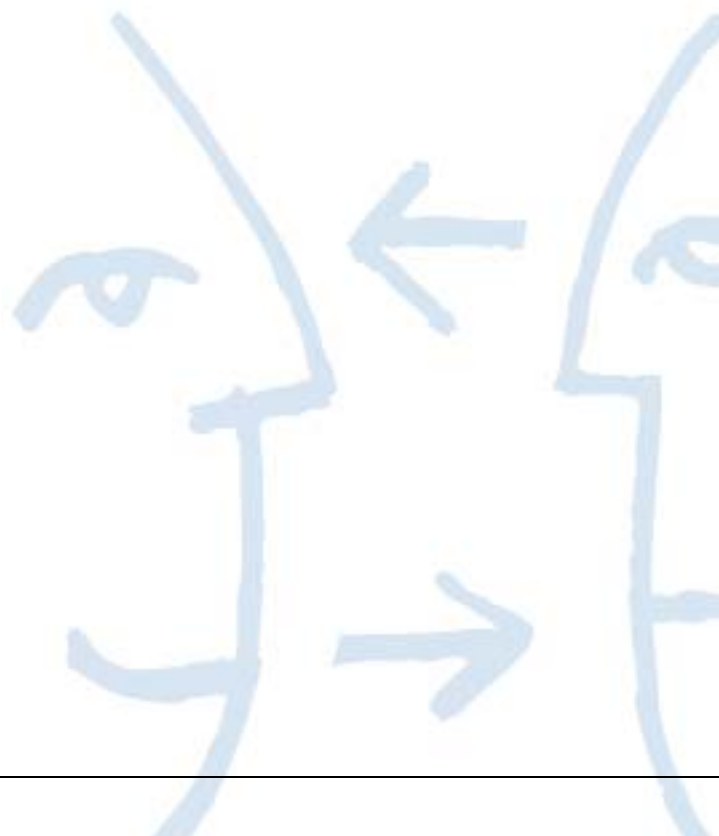
Certificate Policy: Set of rules set forth and published by the CA, describing the general characteristics of the Certificates it delivers. Describes the obligations and responsibilities of the CA, the RA, the Users and all the PKI components involved in the overall lifecycle of a Certificate.

Electronic certification service: Set of services delivered by the Certificate Authority to issue Certificates by applying the procedures stipulated in the Certificate Policy and in any contractual undertakings made to its Users.

Publication function: Operation by which public key certificates issued by a CA are made available to all of the Applications that will be using these certificates to verify signatures or encrypt information.

Electronic signature: Designates, according to Article 1316-4 of French Civil Code, *“the use of a reliable identification process guaranteeing the signature’s link to the document on which it appears”*. Its purpose is to identify the person who applies it and to demonstrate the signatory’s consent with regard to the obligations that result from the signed document.

Uniform Resource Locator (URL): Address of a site or dossier available on the Internet.





2 OBLIGATIONS CONCERNING THE AVAILABILITY OF INFORMATION TO BE PUBLISHED

2.1 Entities in charge of information availability

Within its PKI, the CA sets up a publication function and a function to inform on certificate status.

2.2 Types of information published

The CA publishes

- CPS document : <https://www.keynectis.com/PC/> ;
- CA certificate : <https://www.keynectis.com> ;
- CA trustedlist : <https://www.keynectis.com> ;
- Request certificate Forms : <https://www.keynectis.com> ;
- Non Acceptance Form : <https://www.keynectis.com> ;
- Revocation process : <https://www.keynectis.com> ;
- General condition of Use : <https://www.keynectis.com> ;
- La LCR : http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ICS_ADVANCED_Class_3_CA.crl ;
- La LCR (LDAP):

`ldap://ldap.keynectis.com/cn=KEYNECTIS%20ICS%20ADVANCED%20Class%203%20CA,o=KEYNECTIS?certificateRevocationList;binary?base?objectclass=crlDistributionPoint.`

2.3 Publication Lead Time and frequency

2.3.1 Certificate Policy

The Certificate Policy is accessible 24/7.

Modifications to the Certificate Policy are published in accordance with section 9.8.

2.3.2 Certificate Revocation List: EndUser Certificate

Published Certificate Revocation Lists are accessible 24/7.

They are updated every 24 hours.

2.3.3 Certificate Revocation List - CA Certificates

The CA certificates that can be used to validate certificates are published by the CA to the benefit of Application.

2.4 Controlled access to published information

Access in edit mode to the publication systems (to add, delete or modify published information) is strictly limited to the PKI's authorized internal functions.

2.4.1 Certificate Policy

This Certificate Policy can be viewed from the address indicated as an OID in the Policy Qualifier field of each Certificate.

2.4.2 Certificate Revocation List

Published Certificate Revocation Lists are accessible 24/7 via a URL indicated in the Certificate (field value CrlDp). They are integrity protected.

3 IDENTIFICATION AND VALIDATION OF IDENTITY FOR CERTIFICATE DELIVERY

This section describes the provisions established by the CA regarding Certificate request enrollment.

3.1 Naming

3.1.1 Name types

The names used comply with the specifications of the X.500 standard.

In each certificate, the CA (issuer) and the User (subject) are identified by an X.501-compliant Distinguished Name (DN) whose exact format is specified in § 7– Certificate profiles.

3.1.1.1 CA certificate

Champ de base	Valeur
Issuer	O = KEYNECTIS OU = ICS CN = KEYNECTIS ICS CA C = FR
Subject	O =KEYNECTIS OU =ICS CN =KEYNECTIS ICS QUALIFIED CA OU=0002 478217318 C= FR

3.1.1.2 EndUser Certificate

Champ de base	Valeur
Issuer	O =KEYNECTIS OU =ICS CN =KEYNECTIS ICS QUALIFIED CA OU=0002 478217318 C= FR
Subject	C = Code ISO for country regarding the Location of the company CN = NAME & Surname of Owner; O = Company 's Name as registered officially (Government or representative) ; SN = Serial Number chosen by RA to avoid two same names in a company ; T = Title ; OU= Organization Unit regarding legal identity For ECC customer : <ul style="list-style-type: none"> - ICD = 0002 (France) ; - l'identification Number SIREN or (9 caractères pour le n° SIREN et de 14 caractères pour le n° SIRET. For Outside France Organisation : <ul style="list-style-type: none"> - If no compliance with ISO 6523 No ICD required - If compliance with ISO 6523 ICD is provided (4 digits) followed by other Number for Organization



3.1.2 Using explicit names

The names chosen to designate Users must be explicit and built from legal Name surname provided by an Official government document .

3.1.3 Users anonymity

The use of pseudonym or anonymous IDs to designate Users is not authorized by this Certificate Policy.

3.1.4 Rules for interpreting various name formats

Applicant can use identity information included in the certificate in order to authenticate the EndUser..

3.1.5 Uniqueness of names

A certificate's uniqueness is based on the uniqueness of its serial number within the domain of the CA. Each DN makes it possible to unequivocally identify a User within the PKI . The RA is responsible for ensuring the uniqueness of the names of its Users and for settling any conflicts related to the use of a name. All name-related conflicts shall be handled by the AA in charge of this Certificate Policy.

3.2 Initial User enrollment and validation of requests to issue a certificate

3.2.1 Method for verifying private key ownership

Proof of ownership of the private key corresponding to the EndUser Certificate is provided by the technical and organizational resources defined in the § 6.1.1.1 and 6.1.3

3.2.2 Verification of Public or private organization identity

3.2.2.1 RA

Authentication of a VAR , which plan to Be RA, is based on the check of information during the legal contract built-in and signature

Ra in charge of verification check the organization legally exist in the country and is authorized to use the name . this is done by comparing information provided in the request form and Official external DATABASE like SIREN VAT DUNS number

3.2.2.2 DRA

Authentication of a VAR , which plan to be DRA, is based on the check of information during the legal contract built-in and signature

Ra in charge of verification check the organization legally exist in the country and is authorized to use the name . this is done by comparing information provided in the request form and Official external DATABASE LIKE siren vaT duns NUMBER

3.2.2.3 **Company's Authorized Representative (CAR)**

Authentication of Customer (company) is based on the check of information's provided by the company as follow::

EndUser in a private company

- A CAR designation document sign by the representative and legal authorized person of the company
- An official proof of identity of the CAR Identity (Government CNI Passport).
- Contact information providing a way to contact CRA from RA (Phone Mail etc.)
- Official document of proof of identity of the company (SIREN VAT DUNS ..)
- Company's Official document designing CRA identity

EndUser in a Public company

- A CAR designation document sign by the representative and legal authorized person of the public organisation
- An official proof of identity of the CAR Identity (Government CNI Passport).
- Contact information providing a way to contact CRA from RA (Phone Mail etc.)
- Official document of proof of identity of the public organization (Government publication)



-organization 's Official document designing CRA identity

3.2.2.4 EndUser

The enrollment of a User prior to issuing a Certificate is performed directly by the RA or DRA and is based on Check of Organization reality and authorized to use the name by comparing information provided to the request to official Database (SIREN VAT DUNS)
In any way check of EndUser attachment to the organization is performed.

3.2.3 Verification of EndUser identity

3.2.3.1 No KEYNECTIS RA

RA operator are identified and Authenticated during a face to face with KEYNECTIS RA representative with identity document check (CNI Passport) during legal contract process
RA is then responsible of Other RA operators insides organization and provide KEYNECTIS RA with a list of Authorized R A operator

3.2.3.2 DRA

DRA operator are identified and Authenticated during a face to face with KEYNECTIS RA representative with identity document check (CNI Passport) during legal contract process
DRA is then responsible of Other RA operators insides organization and provide KEYNECTIS RA with a list of Authorized RA operator.

3.2.3.3 Company's Authorized Representative (CAR)

Car are identified during a face to face with RA or DRA using Official government proof document (CNI Passport)

3.2.3.4 EndUser via RA

EndUser is identified during a face to face with RA using Official government proof document (CNI Passport)

3.2.3.5 EndUser via DRA

EndUser is identified during a face to face with DRA using Official government proof document (CNI Passport)

3.2.3.6 EndUser via DRA and CAR

EndUser is identified during a face to face with CAR using Official government proof document (CNI Passport)

3.2.4 Non verified Information

Any non verified information can not be set inside the certificate

3.2.5 Validation of EndUser Authorization

This is done by Company's ownership checking through legal representative

3.2.6 Cross certification ability



End-user receiving a certificate from **CA** can be authenticated in conformity with the Adobe® AATL program and in Application referring to the Certplus class2 Primary CA owned by Keynectis and publish to many worldwide software editors.

3.3 Authentication of a renewal request

3.3.1 Validation in normal renewal situation.

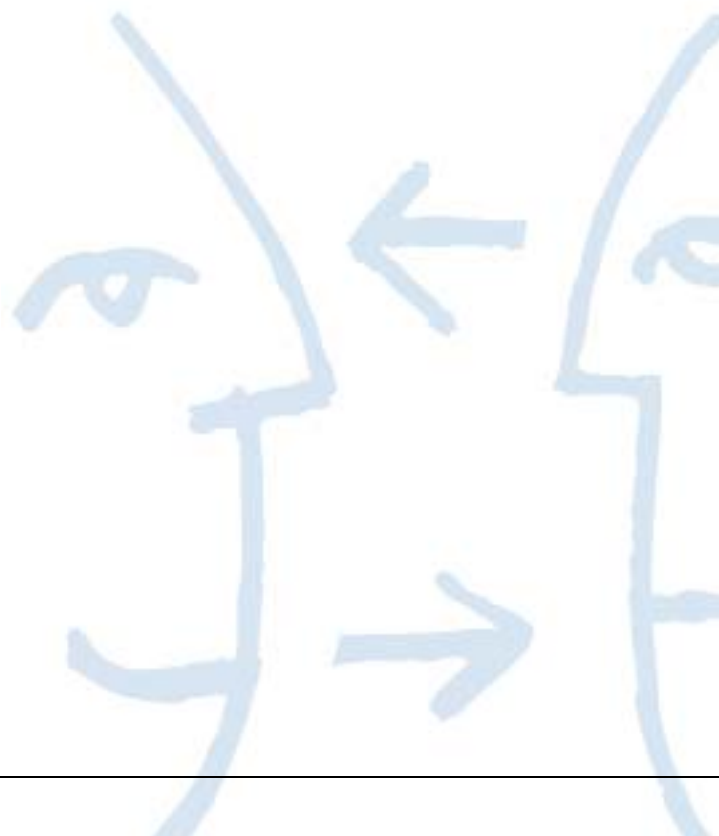
At the end of life renewal is performed through a new Issuance of §3.2

3.3.2 Validation after revocation

After revocation renewal is performed through a new Issuance of §3.2

3.4 Authentication and validation of a revocation request

Request for revocation are validated by RA DRA or CAR when requestor is not the EndUser.



4 OPERATIONAL REQUIREMENTS FOR CERTIFICATE LIFECYCLES

4.1 Types of certificate

4.1.1 Origin of the certificate request

A certificate may be requested by an entity's legal representative or CAR (Company's Authorized Representative). In all circumstances the prior consent of the future certificate EndUser is required.

4.1.2 Enrollment process and responsibilities

The following details must be included in the EndUser certificate request:

- EndUser belonging to an Enterprise:
 - o The certificate request is signed by both the EndUser and a legal representative of the Customer and must be dated no older than 3 months. This certificate request is used as a mandate, naming the EndUser to whom the certificate is to be delivered;
 - If the certificate request cannot be signed by a legal representative of the EndUser an individual who will sign the request must be designated and authorized by a legal representative of the Customer. A document designating the authorized person must be drawn up and signed by both a legal representative of the company and the authorized, designated individual;
 - For certificate requests made by an CAR, the certificate request is signed only by the CAR and the EndUser.
 - o An official identity document belonging to the future EndUser (for example, a national identity card, passport or residence permit). This identity document must be valid and must include a photograph of the EndUser. The RA keeps a copy of this document;
 - o Details required to establish the identity of the EndUser (see § 3.1.1.2 and § 3.1.2);
 - o Information enabling the RA to contact the EndUser (telephone number, email address etc.);
 - o All documentary evidence, valid at the time of the request, proving the identity and legal existence of the company to be named in the certificate (Certificate of incorporation, Kbis, company registration number, SIREN, DUNS number, business certificate number etc.) or by default any other document attesting the unique identity of the company to be named in the certificate (only if the RA or the DRA is unable obtain this document itself);
 - o Any document that proves the official position of the certificate request signatory. The attributes of the signatory are incorporated into the certificate request and are thereby guaranteed by the entity;
 - o The general conditions for use (GCU) signed by the EndUser;
- EndUser belonging to an Administration:
 - o The certificate request is signed by the EndUser and the legal representative of the entity and must be dated no older than 3 months. This certificate request is used as a mandate, naming the EndUser to whom the certificate is to be delivered;
 - If the certificate request cannot be signed by a legal representative of the entity, an individual who will sign the certificate request must be designated and authorized by a legal representative of the entity. A document designating the authorized person must be drawn up and signed by both a legal representative of the entity and the authorized, designated individual;
 - For certificate requests made by an CAR, the request is signed only by the CAR and the EndUser.
 - o An official identity document belonging to the future EndUser (for example, a national identity card, passport or residence permit). This identity document must be valid and must include a photograph of the EndUser. The RA keeps a copy of this document;
 - o Details required to establish the identity of the EndUser (see § 3.1.1.2 and § 3.1.2);
 - o Information enabling the RA to contact the EndUser (telephone number, email address etc.);
 - o A document, valid at the time of registration, delegating or sub-delegating the authority of the Administration;
 - o The general conditions for use (GCU) signed by the EndUser;



Elements for enrollment can be provided in either paper or electronic format. All electronic documents must be sent in accordance with KEYNECTIS procedures for transmission of electronic documents, details of which can be obtained from the RA or DRA.

4.2 Certificate request processing

4.2.1 Identification and Authentication

The request is authenticated (see § 3.2.2 and 3.2.5) and validated by the DRA or the RA.

The RA or the DRA authenticates and identifies the CAR (See § 3.2.2 and 3.2.5). A list of CARs authorized by the Customer is made available to the DRAs by the RA. This avoids the DRAs from re-requesting the CAR's mandate for different EndUser applications from the same Customer.

The RA, DRA or the CAR ensures that the EndUser is aware of the general conditions of use.

The RA keeps a copy of all elements used for enrollment.

4.2.2 Approval or refusal of a certificate request

If the request is approved, the RA (certificate request service) forwards the request to the CA (certificate generation service).

If the request is refused, the RA notifies the EndUser, the CAR or the DRA (depending on the origin of the request) and provides a reason for the refusal. If the CAR or the EndUser is not directly notified by the RA, the DRA must notify the CAR or the EndUser.

4.2.3 Time to process certificate requests

Once the request has been received by the RA, the certificate request is processed as soon as possible.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CA (certificate generation service) authenticates the RA and checks that the request has been generated by an RA authorized by the CA.

The CA generates the EndUser certificate.

The CA forwards the certificate to the Delivery Service (Face to face) at the RA.

If the EndUser is managed by the RA, the EndUser gets his certificate, held on a PIN-code protected physical device, from the RA following authentication (see § 3.2.3 and § 6.1.2).

If the EndUser is managed by the DRA, the EndUser gets his certificate, held on a PIN-code protected device, via the DRA delivery service following authentication (see § 3.2.3 and § 6.1.3).

If the EndUser is managed by the CAR, the EndUser collects the certificate, held on a PIN code-protected device, from the CAR (see § 3.2.3). The CAR will have previously collected the certificate held on a PIN code-protected device from either the RA or DRA delivery service (depending on the initial choice made by the CAR when depositing the request (see § 3.2.3 and § 6.1.3)).

All communications between the different components of the PKI are authenticated and their integrity and confidentiality protected.

4.3.2 Notification of certificate issuance

The EndUser collects his certificate (Delivery Service) during a face-to-face meeting with the RA, DRA or the CAR.

4.4 Certificate acceptance

4.4.1 Certificate acceptance procedure

The EndUser uses his PIN code and the container in order to verify the certificate details. If the EndUser does not wish to accept the certificate he has 15 days to express his non-consent using the non-consent form published by the CA. Beyond this deadline, the certificate is considered accepted.

4.4.2 Publication of a certificate by the CA

The CA certificate is published by the PS.

EndUser certificates are not published by the PS.

4.4.3 Notification of certificate issuance by the CA to other entities

Not applicable.

4.5 Key pair and certificate usage

4.5.1 Use of key pairs and certificates

Key pair and certificate usage is defined in section § 1.4. The use of a key pair and associated certificate is also described in the certificate itself, via the certificate extensions concerning key pair usage (see § 6.1.7). A EndUser's private key can only be used to sign document and mails electronically and for authentication.

4.5.2 Use of public keys and certificates by relying parties

The use of certificates by applicants is described in § 1.4 and § 3.1.4 of this document.

4.6 Certificate renewal

This section addresses the process of renewing a EndUser's certificate without modifying the public key or any other data included in the certificate. Only the certificate validity period and the serial number will change.

This type of operation is not authorized by this CP.

4.7 Re-key request

This section addresses the generation of a new certificate with a modified associated public key.

The modification of a certificate's public key implies the creation of a new certificate. The procedure is therefore identical to the procedures described when issuing the first EndUser certificate (see § 3.3 and § 4.1).

4.8 Certificate modification

This section addresses the generation of a new EndUser certificate while conserving the same key. This operation is only possible if the public key that is to be reused in the certificate continues to conform to the cryptographic security recommendations concerning the length of the key.

This type of operation is not authorized by this CP.

4.9 Certificate revocation

4.9.1 Circumstances for certificate revocation

4.9.1.1 PKI component certificate

The certificate of a PKI component can be revoked under the following circumstances:

- Suspicion of compromise, compromise, loss or theft of the private key of the component;
- Decision to modify the PKI component due to non-conformity of procedures applied within the component with those in the CPS (for example following a negative conformity audit);
- Cessation of activity of the entity operating the PKI component.

4.9.1.2 EndUser certificate

A EndUser certificate shall be revoked when the binding between the public key defined within the certificate and the EndUser is no longer considered valid. Circumstances that invalidate this binding are:

- The information pertaining to the EndUser that is contained in the certificate no longer conforms to the identity or intended use of the certificate (for example, change of entity of an Enterprise or Administration certificate EndUser), prior to the normal certificate expiration date;
- The EndUser, the CAR or the reseller (RA or DRA) has failed to comply with obligations and security rules set out in the CP or CPS;
- An inaccuracy (intentional or unintentional) has been detected in the record or procedure used to enroll the EndUser;
- The death of the EndUser or the cessation of activity of the EndUser's entity (for an Enterprise or Administration certificate);
- Loss of the private key, loss of control of the private key, compromise or suspected compromise of the private key;
- The revocation of the CA;
- The end of life of the CA;
- Modification in the key size imposed by competent national or international institutions.

If one of the above events occurs, the EndUser certificate must be revoked.

4.9.2 Who can request revocation

4.9.2.1 PKI component certificate

Revocation requests for CA certificates are made by the KAA or a judicial authority via a court ruling. The CA initiates certificate revocation requests for PKI components.

4.9.2.2 EndUser certificates

The EndUser can make a revocation request in the following circumstances:

- The information pertaining to the EndUser that is contained in the certificate no longer conforms to the identity or intended use of the certificate (for example, change of entity of an Enterprise or Administration certificate EndUser), prior to the normal certificate expiration date;
- The EndUser, the CAR or the reseller (RA or DRA) has failed to comply with obligations and security rules set out in the CP or CPS;
- An inaccuracy (intentional or unintentional) has been detected in the record or procedure used to enroll the EndUser;
- Loss of the private key, loss of control of the private key, compromise or suspected compromise of the private key;
- Modification in the key size imposed by competent national or international institutions.

The EndUser's parent organization (see § 3.2.2), for Enterprises and Administrations, can request revocation of a EndUser's certificate in the following circumstances:

- The information pertaining to the EndUser that is contained in the certificate no longer conforms to the identity or intended use of the certificate (for example, change of entity of an Enterprise or Administration certificate EndUser), prior to the normal certificate expiration date;
- The EndUser, the CAR or the reseller (RA or DRA) has failed to comply with obligations and security rules set out in the CP or CPS;
- An inaccuracy (intentional or unintentional) has been detected in the record or procedure used to enroll the EndUser;
- The death of the EndUser or the cessation of activity of the EndUser's entity;
- Loss of the private key, loss of control of the private key, compromise or suspected compromise of the private key;
- Modification in the key size imposed by competent national or international institutions.

The CA can request revocation of a EndUser's certificate in the following circumstances:

- The information pertaining to the EndUser that is contained in the certificate no longer conforms to the identity or intended use of the certificate (for example, change of entity of an Enterprise or Administration certificate EndUser), prior to the normal certificate expiration date;
- The EndUser, the CAR or the reseller (RA or DRA) has failed to comply with obligations and security rules set out in the CP or CPS;
- An inaccuracy (intentional or unintentional) has been detected in the record or procedure used to enroll the EndUser;
- Loss of the private key, loss of control of the private key, compromise or suspected compromise of the private key;
- The revocation of the CA;
- The end of life of the CA;
- Modification in the key size imposed by competent national or international institutions.

The RA and the DRA can request revocation of a EndUser's certificate in the following circumstances:

- The information pertaining to the EndUser that is contained in the certificate no longer conforms to the identity or intended use of the certificate (for example, change of entity of an Enterprise or Administration certificate EndUser), prior to the normal certificate expiration date;
- The EndUser, the CAR or the reseller (RA or DRA) has failed to comply with obligations and security rules set out in the CP or CPS;
- An inaccuracy (intentional or unintentional) has been detected in the record or procedure used to enroll the EndUser;



- Loss of the private key, loss of control of the private key, compromise or suspected compromise of the private key;
- Modification in the key size imposed by competent national or international institutions.

4.9.3 Revocation request procedure

4.9.3.1 PKI component certificate

The CPS defines the procedures to be implemented should it be necessary to revoke the certificate of a PKI component.

If a certificate in a certification chain is revoked, the CA notifies all certificate EndUsers affected by this revocation as quickly as possible (if possible by anticipation) informing them that their certificates are no longer valid. To do this, the PKI could, for example, send acknowledgements of receipt to the RA and the DRA. These authorities should then inform the certificate EndUsers that, due to an invalid certificate in the certification chain, their certificates are no longer valid.

The contact point on the website <http://www.references.modernisation.gouv.fr> must be notified immediately when a certificate that is part of a certification chain is revoked. The DGME and the ANSII reserve the right to diffuse the information by any means to the software publishers within Administrative authorities as well as to users.

4.9.3.2 EndUser certificate

A revocation request contains the following details:

- The identity of the certificate EndUser used in the certificate (family name, first name, etc.);
- The name of the individual making the certificate revocation request;
- Any details that enable the certificate to be revoked to be found rapidly (certificate serial number etc.).

The revocation request is logged by the RA.

The revocation request is authenticated as described in § 3.4.

The RA forwards the revocation request to the CA.

The CA (revocation service) authenticates the RA and verifies that the request has been sent by an RA authorized by the CA.

The CA (revocation service) revokes the EndUser's certificate and includes the serial number of the certificate in the next CRL to be issued.

The requester is informed that the EndUser's certificate has been revoked. If the certificate EndUser did not make the revocation request himself the EndUser will also be notified that his certificate has been revoked.

For EndUsers belonging to an Enterprise or an Administration, the parent organization (see § 3.2.2) receives notification when any of its child EndUser certificates are revoked.

4.9.4 Time within which a EndUser must make a revocation request

As soon as a EndUser becomes aware of any circumstance requiring revocation, he must make a revocation request without delay.

4.9.5 Time limit for processing a revocation request

4.9.5.1 PKI component certificates

PKI component certificates are revoked as soon as an event occurs that is described in the circumstances for revoking this type of certificate. The revocation of the certificate becomes effective as soon as the certificate serial number is entered into the revocation list of the CA that issued the certificate.

The revocation of CA signature certificate (signatures of certificates, CRL/ CAL and/or OCSP responses) is effective immediately, particularly in the event of a compromised key.

4.9.5.2 EndUser certificates

The revocation service is available 24h/ 24h and 7 days a week in accordance with the availability rate defined in the CPS.

A EndUser certificate revocation request, authenticated and established by the RA is processed in under 24 hours.

4.9.6 Revocation checking requirements for relying parties



The CU should check the certificate validity status against the CRLs and/or the OCSP service implemented by the CA.

4.9.7 Frequency of CRL publication

The CRL is published every 24 hours.

4.9.8 Maximum latency for CRLs

A newly-generated CRL is published within 30 minutes of its generation.

4.9.9 Availability of an online certificate revocation status verification system

The CA implements an OCSP server at the URL noticed in Certificate Extension

4.9.10 Online revocation checking requirements

See chapter 4.9.6.

4.9.11 Other forms of revocation advertisements available

Not applicable

4.9.12 Special requirements related to private key compromise

For EndUser certificates, entities authorized to request revocation are required to do so as quickly as possible once they are aware that the private key has been compromised.

For CA certificates, notification of revocation following a compromised private key will be clearly diffused on the CA website and if necessary relayed via other means (other institutional websites, magazines etc.) If the CA is revoked, all EndUser certificates are also revoked.

The general conditions for certificate usage clearly state that in the event that a EndUser is aware that his own private key or the private key belonging to the CA that issued his certificate has been compromised, he must immediately and definitively cease using his private key and associated certificate.

4.9.13 Circumstances for suspension

Not applicable.

Origin of a suspension request

Not applicable.

4.9.14 Procedure for a suspension request

Not applicable.

4.9.15 Limits on suspension period

Not applicable.

4.10 Certificate status service

4.10.1 Operational characteristics

The OCSP service is updated using the CRL issued by the CA. The principle certificate status communication mechanism is the CRL published by the CA. In all cases, certificate users can freely consult the CRL and ARL. The CRL and ARL are of V2 CRL format and are published in at least one directory that can be accessed using the LDAP V3 protocol.

4.10.2 Service availability

The OCSP service is updated using the CRL issued by the CA. The service is available 24h/ 24h and 7 days a week in accordance with the availability rate defined in the CPS. When the online certificate status verification function (OCSP) is implemented, the server response time is set at a maximum level defined in the CPS.

4.11 End of relationship between the EndUser and the CA

If the contractual, hierarchical or regulatory relationship between the CA and the EndUser terminates prior to the end of the certificate validity period, for any reason, the EndUser certificate is revoked.



4.12 Key escrow and recovery

The key-pairs and certificates of EndUsers and of CAs issued in conformity with the CP cannot be escrowed or recovered.

5 NON-TECHNICAL SECURITY MEASURES FOR OPERATIONS

5.1 Physical security measures

5.1.1 Geographic location

The operating site of the Certificate Authority is based in Paris (FRANCE) on KEYNECTIS premises. The facility was built in compliance with the regulations and standards in force and takes account of the results of risk analysis specific to the profession of certificate operator, performed according to the EBIOS method. Security measures involve specific requirements relating, for instance, to flooding or explosions (proximity to factories or chemical warehouses, etc.) that must be met by KEYNECTIS.

5.1.2 Physical access

In order to restrict access to PKI applications and information and in order to ensure the availability of the CA operating system, KEYNECTIS has established a security perimeter for its specific needs. The use of this perimeter enables compliance with the principles relating to the separation of trust-based roles as set forth in this Certificate Policy.

Access to the sites of the CO, CA and RA components is restricted to those persons required to perform the services and is based on their individual needs. Access is nominative and traceability is guaranteed. Security is reinforced through the use of passive and active intrusion detection methods. All security incidents are recorded and processed.

The information system supporting electronic certification Services (excluding the RA) is installed within the KEYNECTIS security perimeter.

5.1.3 Energy and air conditioning

Systems designed to protect the electrical power supply and provide air conditioning are deployed by KEYNECTIS to ensure service continuity.

The materials used to deliver services are operated according to the terms and conditions defined by their suppliers or manufacturers.

5.1.4 Exposure to liquids

KEYNECTIS systems have been installed in such a way as to avoid all risk of flooding and other projections or outflow of liquid matter.

5.1.5 Fire prevention and protection

The resources implemented by KEYNECTIS to prevent and fight fire are in line with the requirements and undertakings made by the CA in its CP with regard to the availability of its functions, particularly its certificate management and revocation functions.

5.1.6 Decommissioning of devices

At the end of their lifecycle, devices will be either destroyed or reinitialized for reuse.

5.1.7 Off-site back-ups

The CA conducts off-site back-ups, in line with the procedures agreed upon with KEYNECTIS. These back-ups enable the rapid recovery of certificate management functions following a disaster or any other event that seriously and lastingly affects the performance of these functions.

Further details concerning the back-up methods used are provided in the CPS.

5.2 Procedural security measures



5.2.1 Trust-based roles

Staff must be aware of and understand the implications of the operations for which they are responsible.

Trust-based roles are divided into four groups:

- Operational staff, responsible for maintaining the PKI in sound working order
- Administrative staff, responsible for the technical administration of the PKI components
- Operational staff, responsible for supplying PKI functions
- "Security" staff, responsible for verifying that measures are properly applied and that the PKI component functions smoothly

5.2.2 Number of persons required to perform sensitive tasks

Several roles can be assigned to the same person, provided that this does not compromise the security of the functions being performed.

5.2.3 Identification and authentication of roles

Each entity operating a PKI component has had the identity and authorizations of each staff member working within said component verified before assigning him/her a role and the attendant rights, in particular:

- That his/her name be added to the lists of persons granted controlled access to the site of the entity hosting the component concerned by the role
- That his/her name be added to the list of persons authorized to physically access these systems
- Depending on the role and as needed, that an account be opened in his/her name in these systems
- Possibly, that cryptographic keys and/or a certificate be delivered to him/her to fulfill the role that has been assigned within the PKI

These verifications are described in the CPS of the CA and the RA and are in line with the component's security policy. PKI staff are informed in writing when a role has been assigned to them.

5.2.4 Roles requiring separation of scope

Several roles can be assigned to the same person, provided that this does not compromise the security of the functions being performed. For Truste d role, we recommend that the same person does not own and at least in compliance with the rule below:

Assignment of each role must be describe in the CPS documents.

5.3 Staff security measures

5.3.1 Required qualifications, skills and authorizations

All persons working within one or more PKI components are bound by a confidentiality clause with regard to their employer. Verification is performed to ensure that the roles assigned to staff match their professional skills.

All persons involved in PKI certification procedures are informed of their responsibilities with regard to PKI services, and of all system security and staff verification procedures.

5.3.2 Background check procedures

Each entity operating a PKI component must deploy all the legal means at its disposal to verify the honesty of all staff working within the component. This verification is based on a background check of the person. In particular, it is verified that staff have not been sentenced for a criminal offense in contradiction with the role(s) he/she has been assigned.

Persons who have been assigned a trust-based role mustn't suffer from a conflict of interests that would be harmful to the impartiality of their tasks.

Background checks are conducted prior to the assignment of a trust-based role and are reviewed regularly (at least every three years).

5.3.3 Initial training requirements

Prior to use, staff receive training on the software, hardware and internal operating and security procedures that they implement and must respect, and which correspond to the component in which they operate.



Staff are informed of and understand the implications of the operations for which they are responsible.

5.3.4 Continuing training: requirements and frequency

The relevant staff receive the necessary information and training prior to any changes in the systems, procedures, organization, etc. and based on the nature of these changes.

5.3.5 Profession management

Details are provided in the CPS.

5.3.6 Penalties for unauthorized actions

Details are provided in the CPS.

5.3.7 Requirements of staff employed by external service providers

Details are provided in the CPS.

5.3.8 Documentation provided to staff

Details are provided in the CPS.

5.4 Procedures for the establishment of audit data

Event logging consists in recording events manually or electronically. Information can be entered or automatically generated.

The resulting files, in paper and/or electronic format, must ensure the traceability and accountability of the operations performed.

5.4.1 Types of events to be recorded

Each entity operating a PKI component logs the events concerning the systems involved in the functions it implements as part of the PKI.

- Creation/modification/deletion of user accounts (access rights) and the associated authentication data (passwords, certificates, etc.)
- Starting and shutting down of IT systems and applications
- Events related to logging: starting and stopping of the logging function, modification of logging parameters, actions taken following a logging function failure
- Connection/disconnection of users with trust-based roles, and the associated unsuccessful attempts

Other security-related events that are not automatically produced by the IT systems are also recorded, such as:

- Physical access to sensitive areas
- Maintenance actions and changes to system configuration
- Changes made by staff with trust-based roles
- Actions to destroy or reinitialize devices containing confidential information (keys, activation data, personal information on Users, etc.)

In addition to these logging requirements, which apply to all PKI components and functions, events specific to the various PKI functions are also logged, including:

- Reception of a certificate request (initial request or renewal)
- Validation/denial of a certificate request
- Events relating to signature keys and CA certificates (generation [key ceremony], back-up/recovery, revocation, renewal, destruction, etc.)
- Generation of ENDUSER certificates
- Transmission of certificates to Users and acceptance/refusal by Users
- Publication and update of information relating to the CA
- Generation and publication of CRLs

Each record of an event in a log contains the following fields:

- Type of event
- Name of executor or reference of the system that triggered the event



- Date and time of event
- Outcome of event (failure or success)

All actions are imputable to the executing person, organization or system. The name or ID of the executor is explicitly indicated in a field of the event log.

In addition, depending on the type of event, each record may also contain the following fields:

- Recipient of the operation
- Name of the requester of the operation or reference of the system executing the request
- Name of the persons present (for operations requiring more than one person)
- Cause of the event
- All information qualifying the event (for instance, for the generation of a certificate: the certificate serial number)

5.4.2 Logging process

Logging operations are performed during the process in question.

If information is entered manually, it will be logged on the working day on which the event occurred, barring exceptions.

Details are provided in the CPS.

5.4.3 Protecting event logs

Logging must be designed and implemented so as to limit the risk of event logs being by-passed, modified or destroyed. Integrity control mechanisms must enable any modification of these logs – whether deliberate or accidental – to be detected.

Event log availability must be protected (against partial or total loss and destruction, whether deliberate or accidental).

The definition of event log sensitivity depends on the nature of the information processed and the line of business. It may require specific protection for confidentiality.

5.4.4 Event log back-up procedures

Each entity operating a PKI component implements the requisite measures to ensure the integrity and availability of the event logs for the component in question, in line with the requirements of this CP and based on the results of CA risk analysis.

5.4.5 Event log collection system

Details are provided in the CPS.

5.4.6 Vulnerability assessment

Each entity operating a component of the PKI is capable of detecting any attempt to violate the integrity of the component in question.

Event logs are regularly monitored in order to identify any anomalies resulting from failed attempts.

The logs are analyzed in their entirety at least once a month. This analysis produces a summary in which the important elements are identified, analyzed and explained. The summary must indicate any anomalies or tampering observed. It is regularly sent to the CA.

5.5 Archiving data

Archiving data ensures the longevity of the logs established by the various PKI components.

5.5.1 Types of data archived

For each component, the following data is archived:

- IT equipment software (executables) and configuration files
- Certificate policies
- Certification practices statements



- Contractual agreements with other CAs, if any
- Certificates and CRLs as they were issued or published
- Event logs of the different PKI entities

5.5.2 Archive conservation period

Certificates and CRLs issued by the CA

CA and ENDUSER key certificates, as well as the CRLs/LARs produced, are archived for ten years following the expiration of these certificates.

Event logs

The event logs discussed in section 5.4 are archived for ten years after they are generated. The integrity of the logs is ensured throughout their entire lifecycle.

Other logs

N/A.

5.5.3 Archive protection

Throughout their conservation period, archives and their back-ups will remain:

- Protected in terms of integrity
- Accessible to the authorized persons
- Re-readable and exploitable

5.5.4 Archive back-up procedures

Details are provided in the CPS.

5.5.5 DATA timestamping requirements

Details are provided in the CPS.

5.5.6 Archive collection system

Details are provided in the CPS.

5.5.7 Archive retrieval and verification procedures

Paper archives can be retrieved within a maximum timeframe of two working days. Electronic back-ups can be retrieved within a maximum timeframe of two working days.

5.6 **Rnewal Certificate**

5.6.1 CA Certificate

The CA cannot generate certificates whose expiration date would be after the expiration date of the associated CA certificate. For this, the validity period of the CA certificate must extend beyond that of the certificates it signs.

With respect to the expiration date of this certificate, its renewal must be requested within a timeframe that is at least equal to the lifespan of the certificates signed by the associated private key.

Whenever a new AC key pair is generated, only the new private key can be used to sign certificates.

The previous CA certificate can still be used for operations to manage the validity of any certificates issued using this key, at least until all the certificates signed with the corresponding private key have expired.

5.6.2 End User Certificate

Time life Validity is 3 years max

5.7 **Recovery following compromise or disaster**

5.7.1 Incident and compromise escalation and processing procedures



Procedures and resources for escalating and processing incidents are established for each entity operating a PKI component, in particular through staff awareness-building and training, and through the analysis of the various event logs.

5.7.2 Recovery procedures in the event of IT resource corruption (hardware, software and/or data) and in the event of the compromise of a component's private key

A continuity plan is defined for each PKI component in order to meet the availability requirements of the various PKI functions as set forth in this Certificate Policy and in line with the PKI risk analysis results. This pertains in particular to all functions relating to certificate publication and/or revocation. In the event of the compromise of a CA key, the associated certificate must be immediately revoked.

5.7.3 Continuity capacities following a disaster

The various PKI components have the necessary means to ensure the continuity of their activities, in line with certificate policy requirements.

5.8 End of the PKI lifecycle

One or more PKI components might be required to discontinue its activity or transfer it to another entity.

The transfer of an activity is defined as the discontinuation of the activity of a PKI component bearing no impact on the validity of certificates issued prior to the transfer in question, and the taking over of this activity organized by the CA in collaboration with the new entity.

The cessation of an activity is defined as the discontinuation of the activity of a PKI component bearing an impact on the validity of certificates issued prior to the cessation in question.

Transfer or cessation of an activity affecting a PKI component

In order to ensure a consistent level of trust during and after such events, the CA undertakes, in particular, to:

- Set up procedures whose purpose is to ensure consistent service, in particular with regard to archiving (especially archiving of ENDUSER certificates and information relative to certificates).
- Ensure revocation continuity (registration of revocation requests and publication of CRLs), in line with the availability requirements for these functions defined in this Certificate Policy.

Cessation of activity affecting the CA

The cessation of an activity can be total or partial (for instance: cessation of activity for a given family of certificates only).

The partial cessation of an activity must be progressive so that only the requirements described in 1), 2), and 3) below need to be executed by the CA, or a third-party entity taking over the activities, when the last certificate issued by the CA expires.

In the event of a total cessation of activity, the CA or, in the event of impossibility of performance, an entity replacing the CA by virtue of a law, regulation, legal decision or agreement previously reached with this entity, must perform certificate revocation and CRL publication in line with the undertakings defined in this Certificate Policy.

When the service is discontinued, the CA must:

- 1) Not transmit the private key it used to issue certificates
- 2) Take all necessary measures to destroy or disable this key
- 3) Revoke its certificate



6 TECHNICAL AND LOGICAL SECURITY MEASURES

6.1 Generation and installation of key pairs

6.1.1 Generation of key pairs

6.1.1.1 CA keys

CA signature keys are generated in a secure environment.

CA signature keys are generated and implemented in a CC EAL 4+ certified cryptographic module.

CA signature keys are generated during a key ceremony by staff in trust-based roles and in line with a previously defined process.

Key ceremonies take place under the supervision of at least two persons who have been assigned trust-based roles and in the presence of witnesses, at least one of whom is external to the CA and is impartial. In an objective and factual manner, the witnesses attest that the ceremony is conducted in line with a previously defined script. A public officer (bailiff or notary public) attests that the ceremony is conducted according to previously defined terms and conditions.

6.1.1.2 EndUser certificate keys

KEY Pair generation for EndUser is done directly in the hardware token by RA or EndUser.

If the RA performs Key pair generation following a request through DRA in a Tiers4 location. Key pair is locked inside the Hardware token by the Pin Code Protection.

This process of generation and delivery grant than only the EndUser can use token and Key pair.

There is no way to refund key pair or part of key pair from CA.

6.1.2 Transfer of the private key to its owner

The User's private key is under exclusive control of End User in case of key pair generation by EndUser Itself (Choice of his PIN).

In case of RA Generation CA never track Pin Generation (Send by different way) and Key pair following 2 ways:

- 1) EndUser registration by DRA; RA delivers Token protected by PIN to DRA. Pin Code Send directly to EndUser (Blind Paper) . DRA will have to deliver Hardware to EndUser or representative in Face to face process.
- 2) EndUser registration directly by AE: RA provide directly PIN code to EndUser (Under Blind paper) and Token Protected by Pin in face to face process

6.1.3 Transfer of the public key to the CA

The public key is transferred to the CA in the PKCS#10 format. Through secured communication between RA and CA .

6.1.4 CA publication to Third Party

TRUSTED Chain of certification for CA is provided inside the token for EndUser..

All CA certificates are published .

Upper level of CA are published in Adobe software in compliance with AATL Program .

CA certificate « Class 2 Primary CA », used to cross certified KEYNECTIS ICS Qualified CA is published in all internet browser..

6.1.5 Key size

The size of User keys is 2048 bits for the RSA algorithm with SHA256

The size of CA key pairs is 2048 bits for the RSA algorithm With SH256

6.1.6 Key parameter quality control



The equipment implemented to generate CA key pairs uses parameters that comply with the security standards specific to the algorithm corresponding to the key pair. It is CC EAL 4+ certified.
 EndUser key pair generation are performed by SSCD EAL4+ certified by French ANSI recommendation (ETSI SSCD Compliance)

6.1.7 Key use objectives

"key usage" field Value are :

- CA :
 - o Key CertSign ;
 - o Key CRL Sign ;
- ENdUser :
 - o No Repudiation ;

6.2 Security measures for the protection of private keys

6.2.1 Standards and security measures for cryptographic modules

6.2.1.1 Principles

The cryptographic module of the CA is a CC EAL 4+ certified HSM.
 CA provides Token security module to EndUser and checks:
 Conformity of the token provided by The manufacturer
 Secure intermediate storage of hardware (Tiers 4)

6.2.2 Control of the private CA key by several persons

The CA private signature key is controlled using a secret-sharing tool.
 EndUser is the only responsible of Private key through the code Pin.

6.2.3 Private key escrow

The private keys of the CA and Users are never held in escrow.

6.2.4 Back-up copy of the private key

Back-up copies of Users' private keys are not produced.
 A back-up copy of the CA private key is produced. CA private keys are transferred in an encrypted format.

6.2.5 Private key archiving

The private keys of the CA and Users are not archived.

6.2.6 Private key activation method

6.2.6.1 CA key

The activation of CA private keys in the cryptographic module is controlled using activation data, and requires the involvement of at least two persons who have been assigned trust-based roles.

6.2.6.2 En User key

No copy enabled

6.2.7 Private key destruction method

At the end of a CA private key lifecycle, whether this end is normal or early (revocation), the key and any back-up copies will be destroyed, along with any element potentially enabling reconstruction of the key.

User keys are under exclusive control of EndUser

6.3 Other aspects of key pair management



6.3.1 Public key archiving

The public keys of the CA and Users are archived as part of the archiving process for the associated certificates.

6.3.2 Key pair and certificate lifecycles

CA and EndUser certificates and key pairs of § 7 .

6.4 Activation data

6.4.1 Activation data for the CA private key

The activation data of the CA private key are secrets held by secret EndUsers.

6.4.2 Activation data for the EndUser private key

The activation protocol for the EndUser are done by AE or EndUser.

When performed by RA is unable to get activation Information only known by EndUser (Pin Mailer).

6.5 IT system security measures

A minimum level of assurance regarding the security offered by the IT systems of the PKI is defined in the CPS of the CA. It meets the following security objectives:

- Identification and authentication of CO and RA staff for system access
- Session management
- Protection against computer viruses and all forms of dangerous or unauthorized software, and software updates
- User account management, in particular rapid modification and deletion of access rights
- Protection of the network from intrusion
- Protection of the network so as to ensure the confidentiality and integrity of all data transiting through it
- Audit functions (non-repudiation and nature of the actions performed)
- Possibly, recovery management following an error

Monitoring mechanisms (featuring an automatic alarm) and audit procedures for system configurations (in particular routing elements) are implemented.

6.6 System security measures throughout system lifecycle

6.6.1 Security measures relating to system development

System implementation enabling the deployment of PKI components is documented. The configuration of the system of PKI components as well as all modifications and upgrades is documented and monitored by KEYNECTIS.

6.6.2 Security management

All significant changes in the system of a PKI component are reported to the CA by the component for validation. These changes are documented and included in the internal operating procedures of the component in question.

6.7 Network security measures

Interconnections with public networks are protected by security gateways that have been configured to accept only the protocols that are needed for the component to function within the PKI.

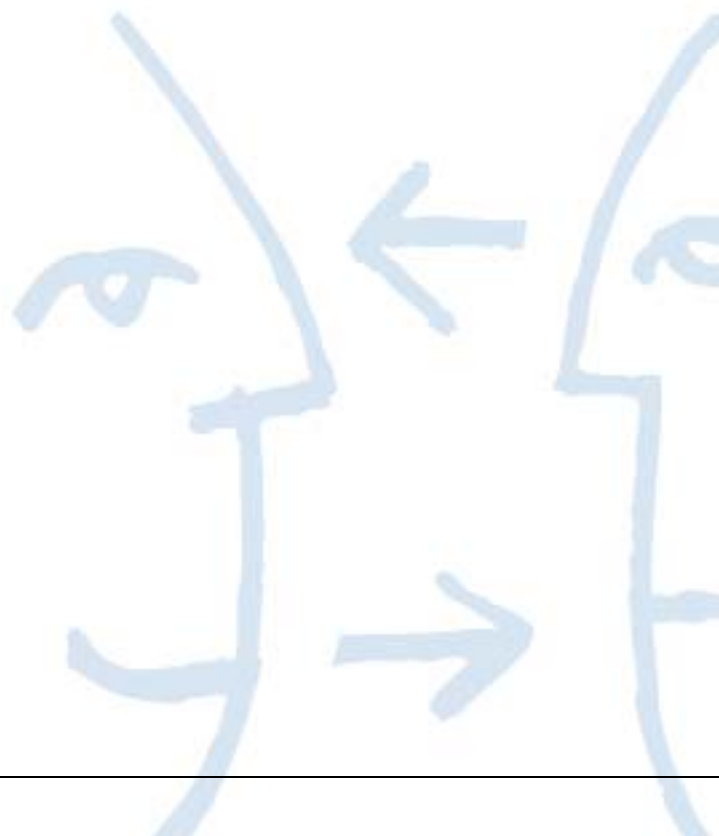
In addition, information exchanged by components within the PKI is protected via specific measures based on the information's sensitivity level (use of separate/isolated networks, implementation of cryptographic mechanisms using control and infrastructure keys, etc.) and defined by the operator KEYNECTIS.

6.8 Security measures for cryptographic modules

The cryptographic modules used by the CA are CC EAL 4+ certified.



They benefit from and are handled according to specific protection measures, under the responsibility of a trusted EndUser.



7 PROFILES OF CERTIFICATES AND CERTIFICATE REVOCATION LISTS

7.1 Profiles of certificates

The certificates issued by the CA are X509 V3 (populate version field with integer "2") contains the following primary fields and extensions regarding RFC 5280.

7.1.1 Certificate Extensions

7.1.1.1 CA Certificate

7.1.1.2 Basic field

Champ de base	Valeur
Issuer DN	O =KEYNECTIS OU =ICS CN =KEYNECTIS ICS CA C= FR
Subject DN	O =KEYNECTIS OU =ICS CN =KEYNECTIS ICS QUALIFIED CA OU=0002 478217318 C= FR
Longueur des clefs de l'AC :	2048
Durée de validité de l'AC :	10 Ans

7.1.1.3 Certificate Extensions

Main informations are :

- Authority Key Identifier ;
- Basic Constraint (critique) ;
- Key Usage (critique) ;
- CRL distribution point ;
- Subject Key Identifier.

7.1.1.4 EndUser certificate

Champ de base	Valeur
Issuer DN	O =KEYNECTIS OU =ICS CN =KEYNECTIS ICS QUALIFIED CA OU=0002 478217318 C= FR
Subject DN	Se reporter au 3.1.1.2
Longueur des clefs de l'AC :	2048
Durée de validité de l'AC :	3 ans

7.1.1.5 Certificate Extensions

- :
- Authority Key Identifier ;
 - Time stamping ;
 - Authority Info Access ;
 - Basic Constraint (critique) ;

- Certificate Policies ;
- CRL Distribution Points ;
- Key Usage (critique) ;
- Extended Key Usage ;
- Subject Alternative Name (adresse email du porteur) ;
- Subject Key Identifier ;
- Private Key Usage Period (égale durée de vie du certificat) ;
- Qualified Certificate Statements (« QC compliance » et « Secure Signature Creation Device »).

7.1.2 Identifiant d'algorithmes

L'identifiant d'algorithme utilisé est Sha-2 WithRSAEncryption: {iso(1) member-body(2) us(840) rsdsi(113549) pkcs(1) pkcs-1(1) 5}.

7.1.3 Formes de noms

Les formes de noms respectent les exigences du § **Erreur ! Source du renvoi introuvable.** pour l'identité des porteurs et de l'AC qui est portée dans les certificats émis par l'AC.

7.1.4 Identifiant d'objet (OID) de la Politique de Certification

Les certificats émis par l'AC contiennent l'OID de la PC qui est donné au § **Erreur ! Source du renvoi introuvable.**

7.1.5 Extensions propres à l'usage de la Politique

Sans objet.

7.1.6 Syntaxe et Sémantique des qualificateurs de politique

Sans objet.

7.1.7 Interprétation sémantique de l'extension critique "Certificate Policies"

Pas d'exigence formulée.

7.2 CRL profile

CRLs include the basic fields as specified in the X509 CRL V2 recommendation. They are:

- **version**: version of the X.509 Certificate Revocation List
- **signature**: identifier of the CA signature algorithm
- **issuer**: name of CA
- **thisUpdate**: issue date of this CRL
- **nextUpdate**: deadline to issue the next CRL
- **revokedCertificates**: list of registered revocations
- **userCertificate**: unique serial number of the revoked Certificate
- **revocationDate**: date of the revocation
- **crlEntryExtensions**: extension not proposed by the CA's CRL
- **crlExtensions**: general extensions of the CRL

In its final format, the CRL contains the following elements:

- **tbsCertList**: all of the fields described above
- **signatureAlgorithm**: the identifier of the algorithm used to produce the list's seal of integrity
- **signatureValue**: the result of this algorithm on all the fields of tbsCertList



8 CONFORMITY AUDIT AND OTHER EVALUATIONS

The audits and evaluations concern the audits initiated by the CA to ensure that its entire PKI is compliant with the undertakings expressed in this CP and with the practices identified in the associated CPS.

8.1 Frequency and/or circumstances of evaluations

The CA regularly and as often as necessary undertakes to verify the conformity of its entire PKI.

8.2 Auditor identity and qualification

The task of verifying a component is assigned by the CA to a team of auditors qualified in IS security and in the field of activity of the component being verified.

The task of verifying the RA is assigned by KEYNECTIS to a team of auditors qualified in IS security and in the field of activity of the component being verified.

8.3 Relations between auditors and the entities evaluated

The audit team must not be affiliated with the entity operating the PKI component being audited, regardless of the component's function, and must be duly authorized to perform the audits in question.

8.4 Topics covered by the evaluations

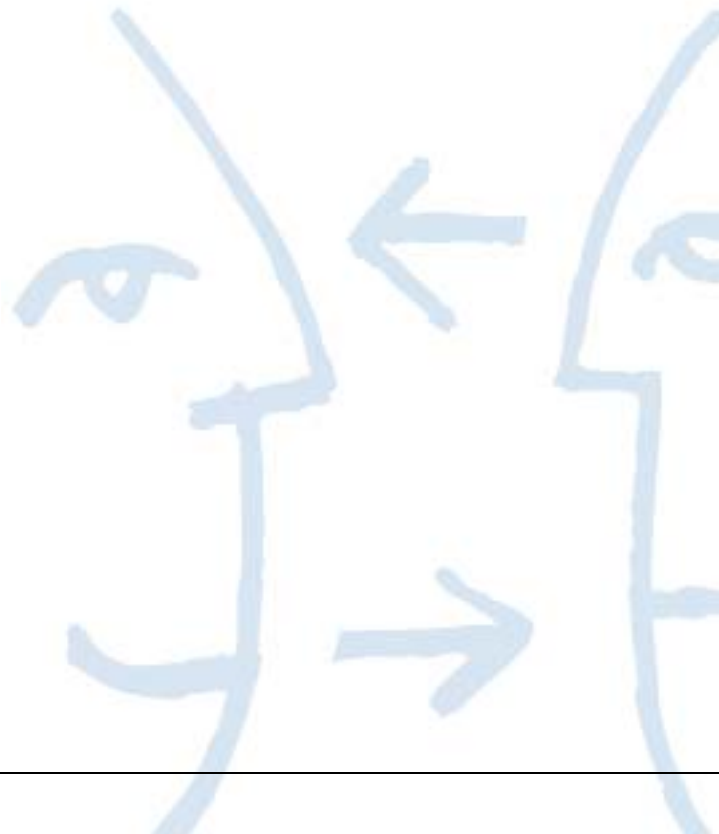
Conformity verifications concern one or more PKI components (one-off verifications) and aim to verify compliance with the undertakings and practices defined in this CP and in the associated CPS.

8.5 Actions taken following evaluation results

Once a conformity evaluation has been completed, the audit team submits its report to the CA. Based on the results for the RA & DRA, the CA, decides which actions must be carried out in order to comply with the applicable documentary framework and within the time allowed.

8.6 Communication of results

The results of conformity audits are saved by the CA and the RA DRA





9 GENERAL PROVISIONS

9.1 Price structure

The provisions relative to the financial terms of the electronic certification Service set forth in this document are included in the contractual documents binding the CA and the RA, and the RA and Users.

9.2 Financial liability

The provisions relative to the insurance of the electronic certification Service set forth in this document are included in the contractual documents binding the CA and the RA, and the RA and Users.

9.3 Applicable law and jurisdictions

The provisions of the Certificate Policy are regulated by French law.

In the event of a dispute relative to the interpretation, establishment or execution of the present policy, and if an amicable settlement is not reached, disputes shall be brought before the Paris court having jurisdiction.

9.4 Intellectual property rights

All intellectual property rights held by the PKI are protected by the applicable laws, regulations and international conventions and treaties.

The forgery of trademarks, business and services, designs and models, distinctive signs, copyright (for example: software, Web pages, databases, original texts, etc.) is punishable by Articles L 716-1 et seq. of the French Intellectual Property Code.

9.5 Confidentiality policy

9.5.1 Types of information considered to be confidential

The following types of information are considered to be confidential:

- The CPS
- User private keys
- The activation data associated with User private keys
- The event logs of CA and RA components
- All data relating to the enrollment of a User, in particular personal data

9.5.2 Delivery to authorized authorities

All CA procedures relative to the handling of confidentiality must be compliant with French legislation.

9.6 Protection of personal data

The French DATA Protection Act of 6 January 1978 (law no. 78-17) applies to the content of all documents collected, held or sent by the CA or the RA as part of Certificate delivery.

Users have the right to access and rectify any data collected by the CA or the RA for the purpose of certificate issuance or certificate lifecycle management. This right can be exercised through the AA (Administrative Authority).

All data collected and held by the CA is considered to be confidential, with the exception of the data contained in the certificate.

By virtue of Articles 323-1 to 323-7 of the French Criminal Code applicable when an offense is committed on French territory, damage or attempted damage to automatic data processing systems is punishable, particularly fraudulent access and maintenance, modification, alteration or pirating of data. The penalties incurred range from one to three years of prison combined with a fine ranging from 15,000 to 225,000 euros for legal entities.



9.7 Certificate policy validity period and early termination

9.7.1 Validity period

The certificate policy of the CA remains in force at least until the end of the lifecycle of the last certificate issued under this certificate policy.

9.7.2 Early termination of validity

The publication of a new version of this Certificate Policy does not require the early renewal of certificates that have already been issued, barring exceptions relating to security.

9.7.3 Effects of the end of validity and clauses that remain applicable

Certain functions of the PKI, in particular archiving and confidential data protection functions, shall be maintained until their term.

9.8 Administration of the certificate policy

This section describes the measures taken by the CA in terms of the administration and management of this Certificate Policy.

9.8.1 Notice period

The CA may modify the present policy without giving advance notice when, based on an evaluation by the Certificate Policy manager, these modifications have no impact on Users.

9.8.2 Delivery of notice

When modifications require advance notice, the CA informs Users of the modifications made to this Certificate Policy using all the means at its disposal, including the CA website, depending on the scope of modifications. Notice of modifications impacting third-party CAs is expressly provided to them.

9.8.3 Modifications requiring the adoption of a new policy

If a modification to this Certificate Policy has, based on the evaluation by the policy manager, a major impact on a large number of Users, the certificate policy manager can, if he/she so wishes, establish a new policy with a new object ID (OID).

9.9 Information procedures

Certain confidential information in the CPS affecting the security of the PKI is not published, or is published at the discretion of the CA. Nevertheless, a summary or excerpts from the CPS can be provided in electronic format, under certain conditions and depending on the source of the information request.

The present Certificate Policy is published and can be accessed from the following address: www.keynectis.com/PC/. A copy can also be obtained by email, on request to the AA.

9.10 Roles and obligations of the PKI and its components

The following obligations are common to all PKI components:

- Protect and guarantee the integrity and confidentiality of their secret and/or private keys
- Use their cryptographic keys (public, private and/or secret) only for their intended purpose when they are issued and with the tools specified in the terms defined by the CP of the CA and the resulting documents
- Comply with and apply the part of the CPS for which they are responsible (this part must be communicated to the corresponding component)
- Undergo the conformity verifications conducted by the audit team mandated by the CA and the qualification organization, and correct any nonconformities that might be revealed
- Comply with all agreements and documents that link components to each other or to Users
- Document their internal operating procedures for the use of their respective staff members who need this information to perform the functions they have been assigned in their capacity as a PKI component
- Deploy all resources (technical and human) necessary to deliver the promised services while ensuring both quality and security



9.10.1 Certificate Authority

The CA must fulfill the following obligations:

- To be able to demonstrate that it has issued a certificate to a given User and that this User has accepted the certificate, in line with the requirements in § 4.1.
- Guarantee and maintain the consistency of its CPS with the CP
- Take all reasonable measures to ensure that its Users are informed of their rights and obligations concerning the use and management of keys and certificates as well as the equipment and software used for the purposes of the PKI
- Publish the information specified in § 2.2
- Comply with or enforce compliance by the CA components with all logging and archiving obligations

The CA is responsible for ensuring the proper application of its certificate policy and recognizes that it has a general responsibility to oversee the security and integrity of the certificates delivered by itself or by one of its components.

9.10.2 Registration Authorities

The role of the RA is to verify the identity of the certificate Requester in line with the commitments it has made to the CA and Users.

As a result, any RA authorized by the CA must comply with all of the requirements stated in this Certificate Policy and with any internal procedures it formalizes, particularly regarding the definition of rules to identify Certificate Requesters for the delivery of Certificates.

9.10.3 User

The User must comply with all of the requirements set forth in this Certificate Policy and with any internal procedures formalized and communicated by the CA or the RA or DRA . The User must use his/her private keys and certificates exclusively for the purposes authorized by this Certificate Policy, in compliance with the laws and regulations in force.

In particular, the User must:

- Communicate accurate, up-to-date information when making a request
- Protect his/her activation data and implement this data as necessary
- Comply with the terms of use pertaining to his/her private key and the associated certificate

9.10.4 Certificate-using applications

Certificate-using applications must:

- Verify and comply with the use for which a certificate was issued
- Verify certificate validity
- For each certificate in the certificate chain, from the certificate to the CA, verify the digital signature of the CA that issued the certificate in question and verify the validity of this certificate (validity dates, revocation status)
- Verify and comply with the obligations of certificate Users stipulated in this Certificate Policy

9.11 Limit of liability

The CA is only bound by a best endeavors obligation for the implementation and operation of the electronic certification Services it provides.

In cases where KEYNECTIS is held liable in its capacity as Certificate Authority for the Customer's failure to fulfill one of its obligations in its capacity as Registration Authority, the Customer shall take the place of KEYNECTIS for the settlement of any disputes or any legal action initiated by a User or third party.

The CA shall not be held liable for the use of certificates that it issued under any conditions and for any purposes other than those set forth in this Certificate Policy as well as in any other associated applicable contractual document.



The CA shall not in any case be held liable for any indirect damage, as such damage is not in any case specified in advance herein.

The CA shall not be held liable for the consequences caused by any delays or loss that could affect electronic messages, letters and documents during their transmission. In addition, it shall not be held liable for the delays, alterations or errors that might occur in the transmission of any telecommunication.

The liability of the CA established herein in the event of damage suffered by one of the PKI components (RA, User, Certificate-using Application) within the framework of this policy is limited, for each annual period and for all damage suffered by each through the elgal or CGU document

The CA shall not be held liable, and assumes no undertaking, for any delay in the execution of obligations or for the inexecution of obligations resulting from this certificate policy, when the circumstances having caused said delay or inexecution and that could be caused by the total or partial interruption of its activity, or by the disruption of its organization, are due to force majeure as defined in Article 1148 of the French Civil Code.

