KEYNECTIS

CERTIFICATION PRACTICE STATEMENT
KEYNECTIS EV CA

Date: 2009/06/30

Siège social : 30, rue du Château des Rentiers . 75647 Paris Cedex 13 . Tél. : +33 (0)1 53 94 22 00 . Fax : +33 (0)1 53 94 22 01 . www.keynectis.com
S.A au capital de 6 986 000 Euros . RCS Paris B 478 217 318 . TVA Intra communautaire FR 44 478 217 318

KEYNECTIS EV CA CERTIFICATION PRACTICE STATEMENT

Subject:	KEYNECTIS EV CA Certification Practise Statement

Version number:	0.4	**Number of pages:**	71
Status of the document:	☐ Project	☒ Final version	
Writer:	Jean-Yves Faurois	KEYNECTIS	

Mailing list:	☒ External	☒ Internal KEYNECTIS	
EV certificate users			KEYNECTIS

Document history:

Date	Version	Writer	Comments	Validated by
17/11/2008	0.1	JYF	Creation of the document	EM/TdV/BG/EA
23/12/2008	0.2	JYF	Additional information	EM/TdV/BG/EA/MQ
04/05/2009	0.3	JYF	Include clarification before going operational	EM/TdV/BG/EA/MQ
30/06/2009	0.4	JYF	Correction of the URL for publication of the root CA Autority Revocation List and for the publication of EV documentation	TdV

SUMMARY

1 INTRODUCTION

1.1 Overview

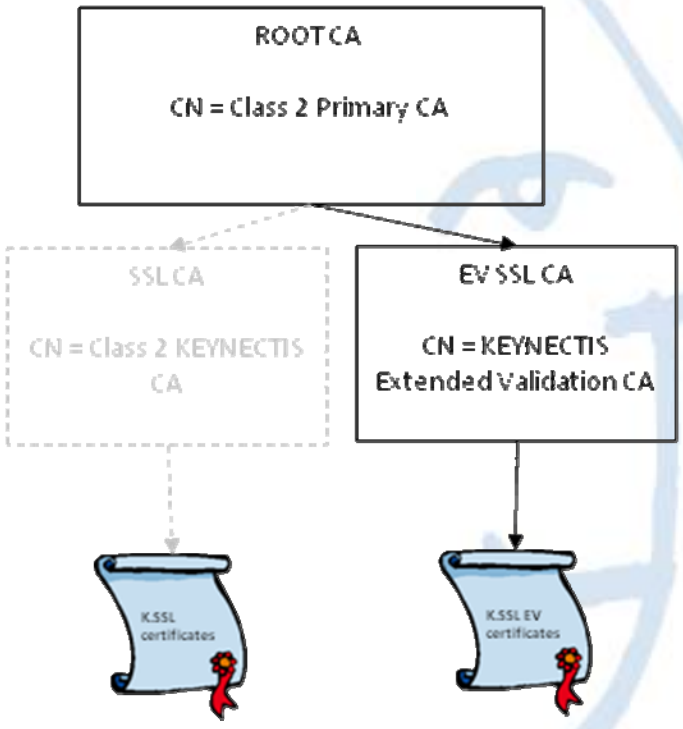
Dematerialization, i.e. the conversion to an electronic format of traditional daily transactions (contracts, mail, invoices, administrative forms, etc.) is primarily a way of expediting business processes. The innovating and technical aspects of these applications require firms to call on specialized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

At the core of the technologies are the electronic certificates. In order to provide their trust services, Trusted Third Parties (Certificate Authority, Time stamping Authority, Validation Authority), firms and organizations that use electronic certificates rely on KEYNECTIS' authorities (CAs, TSAs, VAs) for certificate and time stamp issuance, as well as validation services. In this perspective KEYNECTIS already operates a Root Certification Authority (RCA) that certifies the KEYNECTIS EV CA to delivers EV certificates.

Due to the need to enhance security in Internet website commerce, an open organization of certification authorities and suppliers of Internet, browser software and other applications, named CA/Browser Forum (http://www.cabforum.org), established a set of rules for the Issuance and Management of Extended Validation Certificates (EV certificates). This set of rules consists of a document "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES" that states minimum requirements CA shall meet to issue Extended Validation certificates.

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

an EV certificate adds the capacity to:
- Identifiy the legal entity that controls the website;
- establish the legitimacy of a business claiming to operate a website.



The KEYNECTIS EV CA delivers EV certificates to Private Organizations, Government Entities, Business Entities and Non-Commercial Entities (International Organization Entities,…) through three distinct offers that are:

K.EV:
K.EV requests are proceeded on a unitary basis by the KEYNECTIS EV registration authority. Each time an entity purchase an EV certificate, its representatives have to complete the overall registration toward the KEYNECTIS EV registration authority.

Club EV:
Club EV offer proposes entities, to purchase EV certificates on a quantity basis (Club EV 10 for 10 EV certificates, Club EV 100 for 100 EV certificates). These entities have to issue their EV certificates within one year. Before the EV certificate registration desk is opened at entity level, KEYNECTIS EV registration authority proceeds to:

- the entity and its representative identities,
- All checks required to issue EV Certificates, in accordance with the present CPS.

ISP (Internet Service Providers) EV:
EV certificates are purchased on a quantity basis by Internet Service Providers on behalf of their customers to cover the requirements of the hosted domain names. Before the EV certificate registration desk is opened at ISP level, KEYNECTIS EV registration authority proceeds to:

- ISP and its representative identities checks,
- All checks required to issue EV Certificates, in accordance with the present CPS.

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

The present document is consistent with the "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES" set of rules issued by CA/Browser Forum.

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

1.2 Document Name and Identification

The present CPS is the KEYNECTIS property. This CPS has a registered policy object identifier (OID) that is 1.3.6.1.4.1.22234.2.5.2.3.1for EV certificates signed by KEYNECTIS EV CA.

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

1.3 PKI Participants

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

- Generation of EV CA key: KEYNECTIS EV CA generates its key pair in KEYNECTIS trust center during a specific operation called “Key ceremony”;
- Generation of EV CA certificates: KEYNECTIS EV CA requests KEYNECTIS RCA for a certificate according to the RCA CP;
- Authentication of RA: KEYNECTIS EV CA authenticates the Registration Authority in order to register EV certificate requests;
- Generation of key pair for EV certificates: the EV certificate applicant generates its own cryptographic key pair(s);

- Authentication of the EV certificate applicant : before delivering EV certificates, the RA collects and checks information included in the EV requests;
- Generation of EV certificates: If the applicant request is accurate and validated by the RA, then the KEYNECTIS EV CA generates an EV certificate;
- Revocation of EV certificates: when the binding between the certificate applicant and the public key defined within the certificate delivered by KEYNECTIS EV CA is considered no longer valid, then the EV certificate has to be revoked either by the applicant, either by the RA or KEYNECTIS EV CA ;
- Renewal of EV certificates: renewing an EV certificate means generating a new certificate with the same or different information (key, name …) as the previous certificate. The certificate applicant is responsible of the renewal request;
- Publication services: RCA certificate, EV CA certificate and associated CRLs are published by KEYNECTIS on its web site. Also, the RCA certificate and EV CA certificates are provided to main browsers editors (Microsoft, Mozilla foundation, Opera Software ASA…) by KEYNECTIS to be published in their software.

The following CPS gives the security requirements for all described services. Parts of the present CPS, that give more details on the practises supported by each entity, are not publicly available and may be reviewed by auditors in accordance with § 8 below.

1.3.1 KEYNECTIS EV Certificate Authority (KEYNECTIS EV CA)

KEYNECTIS EV CA is a CA that generates EV certificates for customers (Private Organizations, Government Entities, Business Entities and Non-Commercial Entities) and allows them to set up trusted communications. KEYNECTIS EV CA uses KEYNECTIS Publication Service to publish its certificates and the CRL it issues.

KEYNECTIS EV CA operates its own PKI in accordance with the present CPS.

1.3.2 Registration Authorities (RA)

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

KEYNECTIS EV customer service acts as an RA for EV certificates.

EV Administrators act as RA for the Club EV and the ISP EV offers, (refer to § 1.3.8 below).

1.3.3 Publication Service (PS)

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

1.3.4 Owner of Domain Name (ODN)

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

- The organization mentioned in the Certificate Signing Request (CSR) exists and is legally entitled to the exclusive use of its name;
- The domain name featured in the request belongs to that organization, which is therefore entitled to use it;
- There is either an EV administrator (refer to § 1.3.8 below) acting as the EV certificate Applicant or a technical contact (refer tp § 1.3.7 below) acting as the EV certificate Applicant, who is entitled to submit the request since he belongs to the ODN organization, or a company appointed by the ODN organization, and which authorized him to send the request.

1.3.5 Contract Signer

A Contract Signer is a natural person who is either Applicant, employed by Applicant, or an authorized agent who has express authority to represent Applicant, and who has authority on behalf of Applicant to sign Subscriber Agreements.

1.3.6 Certificate Approver

A Certificate Approver is a natural person who is either Applicant, employed by Applicant, or an authorized agent who has express authority to represent Applicant to (i) act as a Certificate Requester and to authorize other

employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.

1.3.7 Technical contact (TC)

A Technical Contact is a person appointed by the EV Certificate Approver of the organization requesting an EV certificate, and which is authorized to:

- Act as an EV applicant for the generation of EV Certificate Signing Requests (CSR);
- Fulfil and submit EV certificate requests forms;
- Retrieve EV certificates;
- Fulfil and submit EV certificate revocation forms.

The Technical Contact owns the Certificate Requester role as defined in the "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES".

1.3.8 EV administrator

An EV administrator is a person authorized by the EV customer to act as EV certificate approver or requester for Club EV and ISP EV offers. The EV administrator may also revoke certificates on behalf of the EV customer he or she is authorized to act for. The EV administrator act as an RA service.

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

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

An organization that owns its RA service also relies on TC for technical aspects of the EV certificate lifecycle management.

1.3.8.1 EV administrator for Club EV offer

In case of a Club EV offer, the EV administrator is acting as an applicant for the organization that owns the domain names.

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

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

1.3.8.2 EV administrator for ISP EV offer

In case of the ISP EV offer, the EV administrator is acting as an applicant for the ISP which himself is acting on behalf of organizations owning the domain names.

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

- Filling the EV certificate requests on behalf of the (ODN) hosted entities
- Transmitting the EV certificate retrieval codes to the appropriate technical contact
- Revoking the EV certificate
- Authenticate to the KEYNECTIS EV CA as necessary.

1.3.9 Other Participants

1.3.9.1 KEYNECTIS Management Authority (KMA)

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

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

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

1.3.9.2 Root Certificate Authority (RCA)

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

1.3.9.3 Relying party

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

1.4 Certificate Usage

1.4.1 Appropriate Certificate Use

1.4.1.1 EV CA certificate

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

1.4.1.2 EV certificate

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

1.4.2 Prohibited Certificate Use

Only the use mentioned above in § 1.4.1 above are authorized.

KEYNECTIS EV CA will not be deemed responsible for any other use than the one defined in the present CPS.

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

1.5 Policy Administration

1.5.1 Organization Administering the Document

The KMA is responsible for all aspects of this CP.

1.5.2 Contact Person

The Certificate Policy Manager is responsible for the KMA.

KEYNECTIS

Contact: Security and Quality Director
30, rue du Château des Rentiers, 75647 Paris Cedex 13 - FRANCE
Phone: +33 (0)1 53 94 22 00
Fax: +33 (0)1 53 94 22 01
info@keynectis.com

1.5.3 Person Determining CP Suitability for the Policy

KEYNECTIS EV CA is responsible for the implementation, operation and maintenance of the present CPS.

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

1.5.4 CPS Approval Procedure

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

Parts of KEYNECTIS EV CA CPS are remains confidential and are not published. KEYNECTIS EV CA submits its CPS to KMA for approval.

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

Amendments to CPS are issued as a new CPS version. The new version of CPS replaces automatically the previous version and becomes operational as soon as the KMA has established his agreement on the mapping result. A new version of CPS is still compliant with "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES" to permit KEYNECTIS EV CA to refer to this CP to deliver EV certificates.

1.6 Definitions and Acronyms

1.6.1 Definition

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

Applicant: a person authorized by the ODN or the EV customer to proceeds to EV Certificate Signing Requests (CSR). AN applicant may be a certificate requester, a certificate approver or a contract signer (see definitions below).

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

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

Business entity : refer to CAB Forum definition (http://www.cabforum.org/documents.html).

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

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

CA secret activation data: A set of m (fixed integer that is determine in the CPS) activation data (portion of key, secret PIN …) that are used to activate the CA private key. The CPS define the number of n (n>1) necessary activation data that are sufficient to activate the CA private key. Actually a single activation data can't be used to activate the CA private key pair. All the m secret activation data are given to m authorized person that have to protect it in confidentiality and integrity.

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

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

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

Certificate Approver : Refer to § 1.3.6above.

Certificate Requester: Refer to § 1.3.7 above.

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

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

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

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

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

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

Contract Signer : Refer to § 1.3.5 above.

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

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

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

Customer: An organization requiring an EV certificate to secure its website. A customer is able to use and is authorized to use, the private key that corresponds to the public key listed in the Certificate. An EV certificate customer is either a Private Organization, a Government Entity, a Business Entity or a Non-Commercial Entity

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

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

EV Administrator: refer to § 1.3.8 above.

Face-to-face validation: refer to CAB Forum definition stated in Annex A below.

Government entity : refer to CAB Forum definition (http://www.cabforum.org/documents.html).

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

Hash function: A function which maps string of bits to fixed-length strings of bits, satisfying the following two properties:
- It is computationally infeasible to find for a given output an input which maps to this output
- It is computationally infeasible to find for a given input a second input which maps to the same output [ISO/IEC 10118-1]

Independent confirmation from applicant :

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

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

KMA: Describes the authoritative body inside KEYNECTIS. Refer to § 1.3.9.1 for more details.

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

KEYNECTIS Trust Center: The initial purpose of the Trust Center and resources operated by KEYNECTIS is the generation of electronic certificates. These services include:
- Management of certificate authorities' life cycle
- Management of digital certificates' life cycle
- Publishing of the elements associated to those life cycles' management
- Production of time stamping tokens
- Customization of chip cards and other USB tokens
- Verification of electronic signatures or validity status of certificates

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

Non-commercial entity : refer to CAB Forum definition (http://www.cabforum.org/documents.html).

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

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

Policy qualifier: Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate. [RFC 2527]

Principal Individual(s): Individuals of a Private Organization, Government Entity or Business Entity that are either owners, partners, managing members, directors or officers, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance and use of EV Certificates.

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

Private organization : refer to CAB Forum definition (http://www.cabforum.org/documents.html).

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

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

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

Qualified Independent Information Source (QIIS) : a regularly-updated and current publicly available database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information.

Qualified Government Information Source (QGIS) : a regularly-updated and current publicly available database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided they are maintained by a Government Entity, the reporting of data is required by law and false or misleading reporting is punishable with criminal or civil penalties.

Qualified Government Tax Information Sources (QGTIS) : a Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities or Individuals (e.g. the I.R.S. in the United States).

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

Relying Party: refer to § 1.3.9.3 above.

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

Root Certificate Authority (RCA): refer to § 1.3.9.2 above.

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

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

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

Technical contact: refer to § 1.3.7 above.

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

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

Verified accountant letter : refer to CAB Forum definition stated in Annex A below.

Verified legal opinion : refer to CAB Forum definition stated in Annex A below.

1.6.2 Acronyms

ANSI: The American National Standards Institute;
ARL: Authority Revocation List;
CAB Forum : CA / Browser Forum
CP: Certificate Policy:
CPS: Certification Practice Statement;
CRL: Certificate Revocation List;
DN: Distinguished Name;
DNS: Domain Name Server;
EAL: Evaluation assurance level (pursuant to the Common Criteria);
EV: Extended Validation
FIPS: United State Federal Information Processing Standards;
HTTP: Hypertext Transport Protocol;
IP: Internet Protocol;
ISO: International Organization for Standardization;
ISP: Internet Service Provider
KEYNECTIS EV CA : Certificate Authority that delivers EV certificates to customer;
KMA: KEYNECTIS Management Authority;
KTS: KEYNECTIS Trust Center;
LDAP: Lightweight Directory Access Protocol;
OCSP: Online Certificate Status Protocol;
ODN: Owner of a Domain Name
OID: Object Identifier;
PIN: Personal identification number;
PKCS: Public-Key Cryptography Standard;
PKI: Public Key Infrastructure;
PS: Publication Service;
RA: Registration Authority;
RCA: Root Certification Authority;
RFC: Request for comment;
RSA: Rivest, Shamir, Adleman (Public-Key Cryptosystem;
SHA: Secure Hash Algorithm (US Standard);
SSL: Secure Socket Layer;
URL: Uniform Resource Locator.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

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

2.2 Publication of Certificate Information

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

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

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

- www.keynectis.com/PC for the certificate policies
- www.keynectis.com/PC for the CA certificates
- http://www.certplus.com/CRL/class2.crl for the KEYNECTIS ROOT CA CRL
- http://trustcenter-crl.certificat2.com/keynectis/class2keynectisevca.crl for the EV certificates status (CRLs)
- http://www.keynectis.com/fr/support-informations.html for the documentation related to certificates request, retrieval and revocation request.

2.3 Time or Frequency of Publication

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

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

The EV certificate status is made available through CRLs. CRLs are published at least every 24 (twenty four) hours.

2.4 Access Controls on Repositories

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

In application of the KEYNECTIS security policy, only the KEYNECTIS EV CA authorised trusted employees have access to PS repositories for modification purposes. These accesses are subject to proper authentication of the authorised employees, logged and subject to regular audits. Trusted employees that have access to repositories containing information related to certificate validity, whether they are used for CRL issuance or OCSP response purposes, are not cleared to modify these information until the associated certificate expires.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Type of Names

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

Organization	This field contains the Subject's full legal organization name for which the EV certificate is issued. The term 'Organization' is a generic name covering the various types of entities requesting EV certificates (Private Organizations, Government Entities, Business Entities and Non-Commercial Entities). The name of the Organization must be the same than that which is officially present in records of the incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration.
Common Name	The Common Name is the Fully Qualified Domain Name (FQDN). It is the name of the website to be secured. Therefore, the Common Name is all that follows http://, including the extension. The Common Name can never be an IP address.
Business category	This field contains one of the following strings: "V1.0, Clause 5.(b)', 'V1.0, Clause 5.(c)', 'V1.0, Clause 5.(d)' or 'V1.0, Clause 5.(e)' depending whether the Subject respectively qualifies under the terms of Section 5b Private Organizations, 5c Government Entities,5d Business Entities or 5e Non-Commercial Entities of the CAB Forum EV Guidelines
Jurisdiction of Incorporation or Registration	These field(s) contain information only at and above the level of the Incorporating Agency or Registration Agency, depending on the Incorporating Agency or Registration Agency level (Country, State/Province, Locality).
Registration Number	For Private Organizations, this field contains the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration.
Street	This field contains the street address of the physical location of the Subject's Place of Business.
Locality	This field contains the city name of the physical location of the Subject's Place of Business.
Postal code	This field contains the postal code of the physical location of the Subject's Place of Business.
State	This field contains the state, region, or the 'department' of the Subject's Place of Business.
Country	This field contains the 2-letters country code (ISO standard) of the Subject's Place of Business.

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

3.1.2 Need for Names to be Meaningful

The certificates issued pursuant to this CPS are meaningful only if the names that appear in the certificates can be understood and used by relying parties. Names used in the certificates identify the domain in a meaningful way.

3.1.3 Anonymity or pseudonym of Customers

The identity used for the EV certificate is not a pseudonym or an anonymous name.

3.1.4 Rules for Interpreting Various Name Forms

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

KEYNECTIS EV CA has the opportunity to abbreviate the organization prefixes or suffixes in the Organization name, e.g., if the QGIS shows "*Company Name* Société Anonyme" the KEYNECTIS EV CA may decide to include *Company Name* SA. The KEYNECTIS EV CA uses common abbreviations that are generally accepted in the Jurisdiction of Incorporation or Registration of the organisation. In addition, an assumed name or d/b/a name used by the Subject may be included at the beginning of his field, provided that it is followed by the full legal organization name in parenthesis. If the combination of the full legal organization name and the assumed or d/b/a name exceeds 64 characters, as defined by RFC 3280, only the full legal organization name is included in the certificate.

If the Organization name by itself exceeds 64 characters, the KEYNECTIS EV CA abbreviate parts of organization name, and/or omit non-material words in the organization name in such a way that the name in the certificate does not exceed the 64 character limit, and a Relying Party will not be misled into thinking they are dealing with a different Organization. In cases where this is not possible, the KEYNECTIS EV CA will not issue the EV certificate.

3.1.5 Unicity of Names

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

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

3.1.6 Recognition, Authentication, and Role of Trademarks

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

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The Technical Contact, acting as Certificate Requester, proceeds to the generation of the key pairs and EV CSR on behalf of a KEYNECTIS EV customer.

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

3.2.2 Authentication of an Entity

Authentication of an entity identity is based on the verification of information provided by the entity, in compliance with information verification requirements issued from "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES" (refer to Annex A below).

Applicant's existence and identity are verified, including;

- Applicant's legal existence and identity, and
- Applicant's physical existence (business presence at a physical address), and
- Applicant's operational existence (business activity), and
- Verification of Applicant's Domain Name.

3.2.2.1 Verification of Entity legal existence and name

The entity that proceeded to the verification checks that the organization is legally entitled to the exclusive use of its name, by mapping the information provided in the EV certificate application, Club EV or ISP EV contract with information retrieved from official database documentation (Qualified Independent Information Source, Qualified Government Information Source, Qualified Government Tax Information Sources), that confirms the existence of the organization. That database documentation contains trusted information that is filled by the trusted source that registers the legal company.

Information that is subject to verification during the authentication of the organization identity includes the SIREN number, VAT declaration number, DUNS number and apply as follow:

- for Private Organizations (checked against QIIS or QGIS)

  - Legal Existence
  - Organization Name
  - Registration Number
  - Registered Agent
- For Government Entities (checked against QIIS or QGIS)
  - Legal Existence
  - Entity Name
  - Registration Number
- For Business Entities (checked against QIIS or QGIS)
  - Legal Existence
  - Organization Name
  - Registration Number
  - Principal individual
- Non-Commercial Entities (International Organization Entities, checked against QIIS or QGIS))
  - Legal Existence
  - Entity Name
  - Registration Number

3.2.2.2 Verification of an Entity physical existence

Verification of Applicant's physical existence and business presence, is aimed at confirming that the physical address provided by the Applicant is an address where Applicant or a Parent/Subsidiary company conducts business operations (e.g., not a mail drop or P.O. box), and is the address of Applicant's Place of Business. The verification conducted by the KEYNECTIS EV CA includes verification that the telephone number provided by Applicant is a main phone number for Applicant's Place of Business.

3.2.2.3 Verification of an Entity operational existence

As an additional verification, KEYNECTIS EV CA verifies for Applicant has been in existence for less than three years, as indicated by the records of the Incorporating Agency or Registration Agency, and is not listed in either the current version of one Qualified Independent Information Source or a Qualified Governmental Tax Information Source, that Applicant has the ability to engage in business.

3.2.2.4 Verification of an Entity Domain Name

For the purpose of EV certificate delivery, the verification also requires to check that the domain name featured in the request belongs to the Applicant, which is therefore entitled to use it. In this way, verifications are made against domain name database in order to verify Applicant is a registered holder, or has exclusive control, of the domain name to be included in the EV Certificate. Checks on domain names are such that the KEYNECTIS EV CA confirms such domain name satisfies the following requirements:

- The domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN) approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA);
- Domain registration information in the WHOIS is public and shows the name, physical address, and administrative contact information for the organization. For Government Entity Applicants, the CA relies on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name.
- Applicant:
  - is the registered holder of the domain name; or
  - has been granted the exclusive right to use the domain name by the registered holder of the domain name;
- Applicant is aware of its registration or exclusive control of the domain name.

In case an EV Certificate request is made for a domain name containing mixed character KEYNECTIS EV CA visually compares the domain name with mixed character sets with known high risk domains. If a similarity is found then the EV Certificate Request is flagged as High Risk. The CA performs appropriate additional authentication and verification to be certain that Applicant and the target in question are the same organization.

3.2.3 Authentication of Individual identity

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

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

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

A Principal Individual associated with a Business Entity is validated during a face-to-face setting. The CA has the opportunity to rely upon a face-to-face validation of the Principal Individual performed by the Registration Agency, provided that the CA has evaluated the validation procedure and concluded that it satisfies the requirements stated in § 14 of Annex A below. Where no face-to-face validation was conducted by the Registration Agency, or the Registration Agency's face-to-face validation procedure does not satisfy the following requirements, the CA performs face-to-face validation.

3.2.4 Verification of signature

Both the subscription agreement and the EV certificate application are signed. Accepted signatures are handwritten signature or electronic signature (provided elements to check the electronic signature are made available to KEYNECTIS EV CA).

Verification of signature on the subscription agreement consists in authenticating the signature of the Contract signer and the TC. If the TC, acting as Certificate requester do not owns certificate approver rights, the EV certificate application have to be signed by an authorized Certificate Approver. In this case, the signature of the Certificate Approver also has to be verified.

Verification of signature is made by the KEYNECTIS EV RA that phone to the Certificate signer, the TC and the Certificate Approver (where necessary), as verified in § 3.2.2 above, that confirms he or she has signed the document on behalf of the Entity. An alternative method to verify these signatures is to mail a letter to the Applicant at its place of business.

3.2.5 Non-Verified information

Information that is not verified is never included in EV certificates by KEYNECTIS EV CA.

3.2.6 Validation of Authority

An applicant authority is checked during the registration and validation process of EV certificates requests it proceeds to. The validation of authority consists in an administrative phase aimed at verifying authority of the Contract Signer, Certificate Approver et Certificate Requester.

Technical contact and EV administrators act as Certificate Requesters and/or Certificate Approvers for the EV Certificate, their authority has to be checked as part of this validation phase.

The validation of authority occurs before the certificate is generated and consists in verifying:

- name, title, and authority of Contract Signer, Certificate Approver and Certificate Requester;
- the Contract Signer signed the Subscriber Agreement; and
- the Certificate Approver has signed or otherwise approved the EV Certificate Request,
- in case the Applicant will submit multiple future EV request, KEYNECTIS EV CA and the Applicant will enter a written agreement signed by the contract signer that authorizes one or more Certificate Approver acting as EV administrator to originate or approve each EV certificate request on behalf of the Entity.

During this stage, the KEYNECTIS EV CA proceeds to checks as follows:

- Name, title and agency of the and Contract Signer, Certificate Approver are verified contacting the Entity human resources department by mail or phone at the Applicant place of business, or using an Independent Confirmation From Applicant, or a Verified Legal Opinion, or a Verified Accountant Letter,

- Authorization of the and Contract Signer, Certificate Approver are verified obtaining a properly authenticated document (Corporate Resolution) from the Entity the EV certificate is requested on behalf of,
- the TC authority is based on a request sent to the ODN, whether he or she authorize or not the TC to act as an applicant for the domain name he or she made the EV certificate request for,
- the EV administrator authorization is based on a properly authenticated document (Corporate resolution) provided by the entity he request the EV certificate for that gives evidence that the EV administrator is appointed to this position. In case the EV administrator acts as a Certificate Approver, the document issue by the entity shall clearly state that he owns rights to do so.

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

3.2.7 Other verification

3.2.7.1 High Risk Status

KEYNECTIS EV CA seeks to identify Applicants likely to be at a high risk of being targeted for fraudulent attacks, and conducts additional verification activity and takes additional relevant precautions to ensure that such Applicants are properly verified.

KEYNECTIS EV CA identify High Risk Applicants by checking lists of organization names that are most commonly targeted in phishing and other fraudulent schemes, and automatically flaggs EV certificate Requests from Applicants named on these lists for further scrutiny before issuance. Such lists include the lists of phishing targets published by the Anti-Phishing Work Group (APWG), Internet accessible relevant web sites (depending on the country of the Entity requesting the EV certificate, such as http://www.secuser.com/index.htm, http://www.millersmiles.co.uk/search/ksearch.cgi), Internal databases maintained by the CA that include previously revoked EV Certificates and previously rejected EV Certificate Requests due to suspected phishing or other fraudulent usage.

The information is used to flag suspicious new EV Certificate Requests. If an Applicant is flagged as a High Risk Applicant, KEYNECTIS EV CA performs appropriate additional authentication and verification to be certain that Applicant and the target in question are the same organization.

3.2.7.2 Denied Lists and Other Legal Black Lists

KEYNECTIS EV CA verify whether Applicant, the Contract Signer, the Certificate Approver, Applicant's Jurisdiction of Incorporation, Registration, or Place of Business:

- is identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of the CA's jurisdiction(s) of operation; or
- has its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of the CA's jurisdiction prohibit doing business.

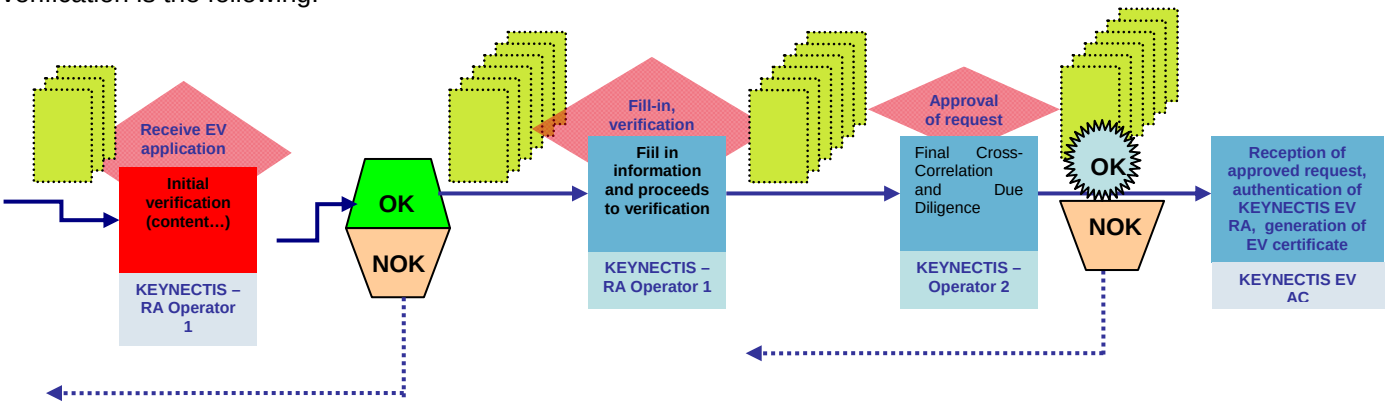
KEYNECTIS EV CA do not issue any EV Certificate to Applicant if either Applicant, the Contract Signer, or Certificate Approver or if Applicant's Jurisdiction of Incorporation or Registration or Place of Business is on any such list.

Denied lists or list of prohibited persons, that are used by KEYNECTIS for verification may be http://www.ustreas.gov/offices/enforcement/ofac/sdn/sdnlist.txt,http://www.bis.doc.gov/dpl/thedeniallist.asp, http://www.treas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf. This list is not exhaustive and KEYNECTIS may rely on any other list as necessary.

KEYNECTIS EV CA verifies French denied lists and export regulations in such a perspective.

3.2.7.3 Final Cross-Correlation and Due Diligence

The verification made by KEYNECTIS EV CA on EV certificate application is handled by KEYNECTIS EV RA, except where an EV administrator acts as the RA (Club EV and ISP EV offer). Its internal process to manage verification is the following:



The results of the verification processes and procedures realized by an initial RA operator (named Operator 1 below), as outlined in previous sections, are reviewed by a second RA operator (named Operator 2 below) who collects information related to Certificate application and look for discrepancies or other details requiring further explanation.

When necessary, Operator 2 requests some further explanation or clarification from Applicant, Certificate Approver, Certificate Requester, Qualified Independent Information Sources, and/or other sources of information, as necessary, to resolve the discrepancies or details requiring further explanation. Where necessary, both operators 1 & 2 work together for final decision about validity of the request.

KEYNECTIS EV CA refrains from issuing an EV Certificate until the entire corpus of information and documentation assembled in support of the EV Certificate is such that issuance of the EV Certificate will not communicate inaccurate factual information that the CA knows, or the exercise of due diligence should discover, from the assembled information and documentation. If satisfactory explanation and/or additional documentation are not received within one month, KEYNECTIS EV CA declines the EV Certificate Request and notifies Applicant accordingly.

KEYNECTIS EV customers are required to provide documentation in English or French Language. In the case where some or all of the documentation used to support the EV certificate application is in a language other than English or French, KEYNECTIS EV CA will request the EV customer to provide documentation in one of these languages. Where the EV customer is not in a position to provide KEYNECTIS EV CA with documentation in English or French, the KEYNECTIS EV CA will rely on language translations, of the relevant portions of the documentation, received from a Translator. Where the cost of the translation is too expensive compared to the value of the EV Certificate purchase, KEYNECTIS EV CA will decide not to approve the application.

3.2.8 Criteria for Interoperation

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

- Operate a PKI that has undergone a successful compliance audit pursuant to section 8 of this CPS, in accordance with "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES",
- Issue EV certificates and certificate status information compliant with the profiles described in § 7.2 below and available to the relying parties.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

A request for re-key can only be made by the customer in the domain name whose keys have been issued. The Applicant identifies itself using the initial identity-proofing process as described in § 3.2 above.

3.3.2 Identification and Authentication for Re-key After Revocation

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

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

3.4 Identification and Authentication for Revocation Request

Revocation requests are authenticated by the KEYNECTIS EV RA.

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

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Origin of a certificate request

4.1.1.1 K.EV offer

Only authorized TC can fill EV application requests.

4.1.1.2 Club EV and ISP EV offers

Only authorized EV administrators can fill EV application requests.

4.1.2 Enrolment Process and Responsibilities

4.1.2.1 K.EV offer

The K.EV offer enrolment process consists of two steps.

First the applicant fills in a form (application request) on KEYNECTIS EV CA website at http://www.keynectis.com/en/ssl-certificates/buy-ssl-certificates.html.The form includes the following fields:

- Identification of the TC, i.e. full name, including surname and given names, e-mail address, function, complete postal address, phone numbers (standard and direct numbers)
- Identification data of the organization for which an EV certificate is requested, i.e. the subject's full legal name for which the EV certificate is requested, the Fully Qualified Domain Name (FQDN), the business category of the Applicant Entity, the Jurisdiction of Incorporation or Registration, the Registration Number, street, locality, postal code, state or province (if any) and the country where the Applicant Entity place of business
- Public key in PKCS#10 format
- Domain name identification
- Secret information for KEYNECTIS EV CA registration authority to proceed to verification of he request
- Secret code for EV certificate retrieval by the TC.

The applicant has the opportunity to pay online.

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

In a second step, the applicant transmits a subscription agreement to the KEYNECTIS EV CA accompanied with:

- a copy of its ID card (national issued identity document including a picture of him or her),
- the payment (in case he or she did proceeded to online payment) at the following address:

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

The validation process of the EV certificate request cannot start before the KEYNECTIS EV customer service receives the payment.

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

4.1.2.2 Club EV and ISP EV offers

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

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

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

Application for EV certificates requires entering into a contractual agreement with the KEYNECTIS EV CA prior to the registration desk to be available. This contractual step includes verification by KEYNECTIS that all information necessary to authenticate the organization and the administrators are complete and valid, in accordance with "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES".

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

4.2.1.1 K.EV offer

Once the KEYNECTIS EV CA has received the subscription agreement, the EV certificate application, the copy of the ID of the applicant and the payment, the identification and authentication process starts.

The KEYNECTIS EV customer service proceeds to the following operations:

- The KEYNECTIS EV customer service operator 1 checks that the subscription agreement, the EV certificate application and the payment are complete and correct;
- The KEYNECTIS EV customer service operator 1 proceeds to all verification to authenticate the organization according to § 3.2.2.1, 3.2.2.2, 3.2.2.3 above
- The KEYNECTIS EV customer service operator 1 checks customer organization owns the domain name according to § 3.2.2.4
- The KEYNECTIS EV customer service operator 1 checks that the TC is acting on behalf of the SSL customer according to § 3.2.3 above
- The KEYNECTIS EV customer service operator 1 checks that the signatures on both the subscription agreement, the EV certificate application are valid according to § 3.2.4
- The KEYNECTIS EV customer service operator 1 checks that the ODN organization accepts the EV customer request EV certificates for the domain names he or she owns according to § 3.2.6
- The KEYNECTIS EV customer service operator 1 checks that the according to §
    - the Applicant, the Contract Signer, the Certificate Approver, Applicant's Jurisdiction of Incorporation, Registration, or Place of Business are not identified on any government denied list, list of prohibited persons, or other list according to § 3.2.7.1 above, and
    - the Applicant has not its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of the CA's jurisdiction prohibit doing business according to § 3.2.7.2 above
- The KEYNECTIS EV customer service operator 2 proceeds to final correlation checks and due diligence according to § 3.2.7.3

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

4.2.1.2 Club EV offer

Once KEYNECTIS EV CA has received the subscription agreement for Club EV, the identification and authentication process starts. Club EV Customers cannot start proceeding to EV certificates enrolment before their identification and authentication process conducted by KEYNECTIS EV CA successfully ends.

The KEYNECTIS EV customer service proceeds to the following operations:

For the delivery of EV administrator electronic certificate:

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

For the opening of the Club EV registration desk:

- The KEYNECTIS EV customer service operator 1 checks that the subscription agreement, the EV certificate application and the payment are complete and correct;
- The EV customer service operator 1 proceeds to all verification to authenticate the organization according to § 3.2.2.1, 3.2.2.2, 3.2.2.3 above
- The EV customer service operator 1 checks customer organization owns the domain name according to § 3.2.2.4
- The EV customer service checks that the appointed SSL administrator is acting on behalf of the ISP EV customer according to § 3.2.3 above;
- The EV customer service operator 1 checks that the TC is acting on behalf of the EV customer according to § 3.2.3 above
- The EV customer service operator 1 checks that the signatures on both the subscription agreement, the EV certificate application are valid according to § 3.2.4
- The EV customer service operator 1 checks that the ODN organization accepts the EV customer request EV certificates for the domain names he or she owns according to § 3.2.6
- The EV customer service operator 1 checks that the according to §
    - the Applicant, the Contract Signer, the Certificate Approver, Applicant's Jurisdiction of Incorporation, Registration, or Place of Business are not identified on any government denied list, list of prohibited persons, or other list according to § 3.2.7.1 above, and
    - the Applicant has not its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of the CA's jurisdiction prohibit doing business according to § 3.2.7.2 above
- The EV customer service operator 2 proceeds to final correlation checks and due diligence according to § 3.2.7.3

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

4.2.1.3 ISP EV offer

Once KEYNECTIS EV CA has received the subscription agreement for Club EV, the identification and authentication process starts. Club EV Customers cannot start proceeding to EV certificates enrolment before their identification and authentication process conducted by KEYNECTIS EV CA successfully ends.

The KEYNECTIS EV customer service proceeds to the following operations:

For the delivery of EV administrator electronic certificate:

- The KEYNECTIS EV customer service checks the identity of the named ISP EV administrator(s)
- The KEYNECTIS EV customer service checks the administrator has clearly been appointed by the ISP EV entity to act on its behalf

For the opening of the ISP EV registration desk:

- The KEYNECTIS EV customer service operator 1 checks that the subscription agreement, the EV certificate application and the payment are complete and correct;
- The KEYNECTIS EV customer service operator 1 proceeds to all verification to authenticate the organization according to § 3.2.2.1, 3.2.2.2, 3.2.2.3 above
- The KEYNECTIS EV customer service operator 1 checks customer organization is authorized to request EV certificates for the domain names it declares according to § 3.2.2.4 above
- The KEYNECTIS EV customer service checks that the appointed EV administrator is acting on behalf of the ISP EV customer according to § 3.2.3 above;
- The EV customer service operator 1 checks that the TC is acting on behalf of the EV customer according to § 3.2.3 above
- The KEYNECTIS EV customer service operator 1 checks that the signatures on both the subscription agreement, the EV certificate application are valid according to § 3.2.4
- The KEYNECTIS EV customer service operator 1 checks that the ODN organization accepts the EV customer request EV certificates for the domain names he or she owns according to § 3.2.6
- The KEYNECTIS EV customer service operator 1 checks that the according to §

- the Applicant, the Contract Signer, the Certificate Approver, Applicant's Jurisdiction of Incorporation, Registration, or Place of Business are not identified on any government denied list, list of prohibited persons, or other list according to § 3.2.7.1 above, and
- the Applicant has not its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of the CA's jurisdiction prohibit doing business according to § 3.2.7.2 above

- The KEYNECTIS EV customer service operator 2 proceeds to final correlation checks and due diligence according to § 3.2.7.3

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

4.2.2 Approval or Rejection of Certificate Applications

4.2.2.1 K.EV offer

Approval or rejection of EV certificates applications are proceeded by the EV customer service, based on the results of the actions described at § 4.2.1.1 above.

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

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

4.2.2.2 Club EV and ISP EV offers

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

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

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

4.2.3 Time to Process Certificate Applications

4.2.3.1 K.EV offer

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

4.2.3.2 Club EV and ISP EV offer

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

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance (K.EV offer, Club EV and ISP EV offers)

Before generating the EV certificate, the KEYNECTIS EV CA checks that the certificate to be signed includes all fields and extensions are properly populated.

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

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

4.3.2 Notifications to Customer by the CA of Issuance of Certificate

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

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the CA

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

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

4.5 Key Pair and Certificate Usage

4.5.1 EV Private Key and Certificate Usage

The EV key pair is used to set SSL protocol.

4.5.2 Relying Party Public Key and Certificate Usage

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

4.6 Certificate Renewal

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

4.6.1 Circumstances for Certificate Renewal

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

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

The KEYNECTIS EV CA sends warning messages, via emails, to the TC to alert him/her on the incoming expiration of its EV certificate.

Certificate renewal has to be submitted by the TC to the KEYNECTIS EV customer service in accordance to § 4.1 above.

4.7 Certificate Re-Key

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

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

Certificate modification has to be submitted by the TC to the KEYNECTIS EV customer service in accordance to § 4.1 above.

4.8 Certificate Modification

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

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

Certificate modification has to be submitted by the TC to the KEYNECTIS EV customer service in accordance to § 4.1 above.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

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

- The Subscriber requests revocation of its EV Certificate;
- The Subscriber indicates that the original EV Certificate Request was not authorized and does not retroactively grant authorization;
- The CA obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the EV Certificate) has been compromised, or that the EV Certificate has otherwise been misused;
- The CA receives notice or otherwise becomes aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
- The CA receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the EV Certificate, or that the Subscriber has failed to renew its domain name;
- The CA receives notice or otherwise becomes aware of a material change in the information contained in the EV Certificate;
- A determination, in the CA's sole discretion, that the EV Certificate was not issued in accordance with the terms and conditions of these Guidelines or the CA's EV Policies;
- The CA determines that any of the information appearing in the EV Certificate is not accurate.
- The CA ceases operations for any reason and has not arranged for another EV CA to provide revocation support for the EV Certificate;
- The CA's right to issue EV Certificates under these Guidelines expires or is revoked or terminated, unless the CA makes arrangements to continue maintaining the CRL/OCSP Repository;
- The Private Key of the CA's Root Certificate used for issuing that EV Certificate is suspected to have been compromised;
- The CA receives notice or otherwise becomes aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of the CA's jurisdiction of operation as described in Section 23 of "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES".

Whenever any of the above circumstances occurs, the associated EV certificate is revoked and placed in the next CRL to be published.

4.9.1.1 Origin of Revocation Request (K.EV offer, Club EV and ISP EV offers)

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

- The subscriber requires the EV certificate revocation;
- The original EV Certificate Request was not authorized;
- DN information are filled incorrectly;
- Domain name registration or the organization's name changed and the applicant is no longer authorized to use the domain name;
- The private key corresponding to the public key in the EV certificate has been lost or compromised;
- The EV certificate has been misused.

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

- The KEYNECTIS EV CA ceases operations for any reason and has not arranged for another EV CA to provide revocation support for the EV Certificate;
- The KEYNECTIS EV CA right to issue EV Certificates under "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES" expires or is revoked or terminated, unless the CA makes arrangements to continue maintaining the CRL/OCSP Repository;
- The Private Key of the KEYNECTIS EV CA Root Certificate used for issuing that EV Certificate is suspected to have been compromised;
- The KEYNECTIS EV CA can be shown to have violated the stipulations of its agreement with KEYNECTIS;
- The KEYNECTIS EV CA is revoked;
- The KEYNECTIS EV CA obtains reasonable evidence that the Subscriber's Private Key has been compromised;
- The KEYNECTIS EV CA obtains reasonable evidence that the Subscriber's EV Certificate has otherwise been misused;
- The KEYNECTIS EV CA receives notice or otherwise becomes aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
- The KEYNECTIS EV CA receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the EV Certificate, or that the Subscriber has failed to renew its domain name;
- The KEYNECTIS EV CA receives notice or otherwise becomes aware of a material change in the information contained in the EV Certificate;
- The KEYNECTIS EV CA determines that the EV Certificate was not issued in accordance with the terms and conditions of its EV Policies;
- The KEYNECTIS EV CA determines that any of the information appearing in the EV Certificate is not accurate.
- The CA receives notice or otherwise becomes aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of the CA's jurisdiction of operation as described in Section 23 of "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES".

KEYNECTIS EV CA provides certificate users with clear instructions for reporting complaints or suspected Private Key compromise, EV Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to EV Certificates, called "Certificate Problem Reports", on its website at http://www.keynectis.com/en/contact-us.html (email to alert.evssl@keynectis.com).

KEYNECTIS EV CA maintains a continuous 24x7 ability to internally respond to any high-priority Certificate Problem Report, and where appropriate, forward such complaints to law enforcement and/or revoke an EV Certificate that is the subject of such a complaint.

4.9.2 Procedure for Revocation Request

4.9.2.1 K.EV offer

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

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

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

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

All the operation are protected in a manner to guarantee the integrity, confidentiality (when it is necessary) and origin of transmitted data and secure link between operation and components.
Once the EV certificate is revoked, the KEYNECTIS EV CA notifies the TC of the change of the EV certificate status. Once a certificate is revoked it cannot be re-certified.

4.9.2.2 Club SSL and ISP SSL offers

The TC and the EV administrator have rights to request for an EV certificate revocation.

4.9.2.2.1 Revocation by the TC

The TC transmits a revocation request form, to the KEYNECTIS EV CA, that contains at a minimum:

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

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

The EV customer service authenticates and authorizes revocation requests. In case the authentication is successful, the EV customer service transmits the revocation request to KEYNECTIS EV CA that authenticates the EV customer service and revokes the EV certificate (using the EV CA private key).All the operation are protected in a manner to guarantee the integrity, confidentiality (when it is necessary) and origin of transmitted data and secure link between operation and components.

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

4.9.2.2.2 Revocation by the EV administrator

The EV administrator connects to its registration desk using its EV administrator certificate and proceeds to EV certificate revocation.

The revocation request is then sent to KEYNECTIS EV CA that authenticates the registration desk and revokes the EV certificate (using the EV CA private key).All the operation are protected in a manner to guarantee the integrity, confidentiality (when it is necessary) and origin of transmitted data and secure link between operation and components.

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

In case where the EV administrator cannot connect himself on its registration desk, he have the opportunity to proceed as a TC to request for the revocation of the EV certificate (refer to § 4.9.2.2.1 above).

4.9.3 Revocation Request Grace Period

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

4.9.4 Time within Which CA Must Process the Revocation Request

KEYNECTIS EV CA online revocation management services are available 24 hours a day, 7 days a week.

KEYNECTIS EV customer service for revocation is available from 9:00 am to 06:00 pm Monday to Friday, except during bank holidays.

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

4.9.5 Revocation Checking Requirements for Relying Parties

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

4.9.6 CRL Issuance Frequency

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

4.9.7 Maximum Latency for CRL

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

4.9.8 On-Line Revocation/Status Checking Availability

No stipulation.

4.9.9 On-Line Revocation Checking Requirements

No stipulation.

4.9.10 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.11 Special Requirements regarding Key Compromise

No stipulation.

4.9.12 Circumstances for Suspension

Suspension of EV certificate is not supported by KEYNECTIS EV CA.

4.9.13 Who Can Request Suspension

Not applicable.

4.9.14 Procedure for Suspension Request

Not applicable.

4.9.15 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

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

4.10.2 Service Availability

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

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

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

4.12 Key Escrow and Recovery

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

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

KEYNECTIS EV CA physical and environmental security policy for systems used for EV certificate life cycle management addresses the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery, etc. Controls are implemented to avoid loss, damage or compromise of assets and interruption to business activities and theft of information and information processing facilities.

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

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

5.1.3 Power and Air Conditioning

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

Media used within the KEYNECTIS EV CA are securely handled to protect them from damage, theft and unauthorized access. Media management procedures are protected against obsolescence and deterioration of media within the period of time that records are required to be retained. All media are handled securely in accordance with requirements of the information classification scheme and media containing sensitive are securely disposed of when no longer required.

5.1.7 Waste Disposal

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

5.1.8 Off-Site Backup

Full system backups of KEYNECTIS EV CA, sufficient to recover from system failure, are made periodically as described in corresponding CPS. Back-up copies of essential business information and software are taken regularly. Adequate back-up facilities are provided to ensure that all essential business information and software

can be recovered following a disaster or media failure. Back-up arrangements for individual systems are regularly tested to ensure that they meet the requirements of business continuity plans. At least one full backup copy is stored at an offsite location (at a location separate from the KEYNECTIS EV CA equipment). The backup are stored at a site with physical and procedural controls commensurate to that of the operational KEYNECTIS EV CA.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

- Security Officer: Overalls responsibility for administering the implementation of the security practices;
- Administrator: Approves the generation/revocation/suspension of certificates;
- System Engineer: Authorized to install, configure and maintain the KEYNECTIS EV CA systems used for EV certificate life cycle management;
- Operator: Responsible for operating the KEYNECTIS EV CA systems on a day to day basis. Authorized to perform system backup and recovery;
- Auditor: Authorized to view archives and audit logs of the KEYNECTIS EV CA trustworthy systems;
- KEYNECTIS EV CA activation data holder: authorized person that hold KEYNECTIS EV CA activation data that are necessary for CA hardware security module operation.

5.2.2 Number of Persons Required per Task

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

5.2.3 Identification and Authentication for Each Role

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

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

5.2.4 Roles Requiring Separation of Duties

Roles separation may be enforced either by the KEYNECTIS EV CA equipment, or procedurally or by both means. Individual KEYNECTIS EV CA personnel are specifically designated to the five roles defined in section 5.2.1 above. It is forbidden to own at the same time the following roles:

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

No individual shall be assigned more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

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

employee training and awareness. KEYNECTIS EV CA personnel shall be formally appointed to trusted roles by senior management responsible for security.

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

5.3.2 Background Check Procedures

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

5.3.3 Training Requirements

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

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

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

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

Contractor personnel employed for KEYNECTIS EV CA operation, have to perform KEYNECTIS EV CA functions operations according to the same requirements than KEYNECTIS personnel.

5.3.8 Documentation Supplied to Personnel

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

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

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

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

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

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

Information related to Subscriber EV Certificate lifecycle management, that are recorded, include:

- EV Certificate Requests, renewal and re-key requests, and revocation;
- Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
- Acceptance and rejection of EV Certificate Requests;
- Issuance of EV Certificates; and
- Generation of EV Certificate Revocation Lists (CRLs); and OCSP entries.

5.4.2 Frequency of Processing Log

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

5.4.3 Retention Period for Audit Log

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

5.4.4 Protection of Audit Log

The events are logged in a way that they cannot be deleted or destroyed (except for transfer to long term media) within the period of time that they are required to be held.
The events are logged in a manner to ensure that only authorized trusted access can make operation regarding their profile role without modifying integrity, authenticity and confidentiality of the data.
The events are protected in a manner to keep them still readable in the time of their storage.
The events are date in a secure manner that guarantees, from the date of creation of the record to the end of the archive period, the trusted link between the event and the time of its realisation.

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system is internal to KEYNECTIS EV CA components. Audit processes are invoked at system start up and end only at system shutdown. The audit collection system ensures integrity and availability of the data collected. If necessary, the audit collection system protects the data in confidentiality. In case a problem

occurs during the process of the audit collection system then KEYNECTIS EV CA determines whether to suspend KEYNECTIS EV CA operation until the problem is solved and inform the impacted components.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

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

5.5 Records Archival

5.5.1 Types of Records Archived

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

- Information related to Subscriber EV Certificate lifecycle management, including:
  - EV Certificate Requests, renewal and re-key requests, and revocation;
  - Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
  - Acceptance and rejection of EV Certificate Requests;
  - Issuance of EV Certificates; and
  - Generation of EV Certificate Revocation Lists (CRLs); and OCSP entries.
- KEYNECTIS EV CA events records;
- KEYNECTIS EV CA audit documentation;
- KEYNECTIS EV CA CP document;
- KEYNECTIS EV CA CPS documents;
- Any contractual agreements between an EV certificate customer and KEYNECTIS EV CA (Club and ISP SSL offers);
- System equipment configuration;
- Certificates and CRLs (or other revocation information);
- Other data or applications sufficient to verify archive contents;
- All work related communications to or from KEYNECTIS EV CA and compliance auditors.

5.5.2 Retention Period for Archive

The minimum retention period for archive data is 7 years after the certificate cease to be valid.

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

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

5.5.7 Procedures to Obtain and Verify Archive Information

Media storing of KEYNECTIS EV CA archive information are checked upon creation. Periodically, statistical samples of archived information are tested to check the continued integrity and readability of the information.
Only authorised KEYNECTIS EV CA equipment, trusted role and other authorized person (legal person …) are allowed to access the archive.

5.6 Key Changeover

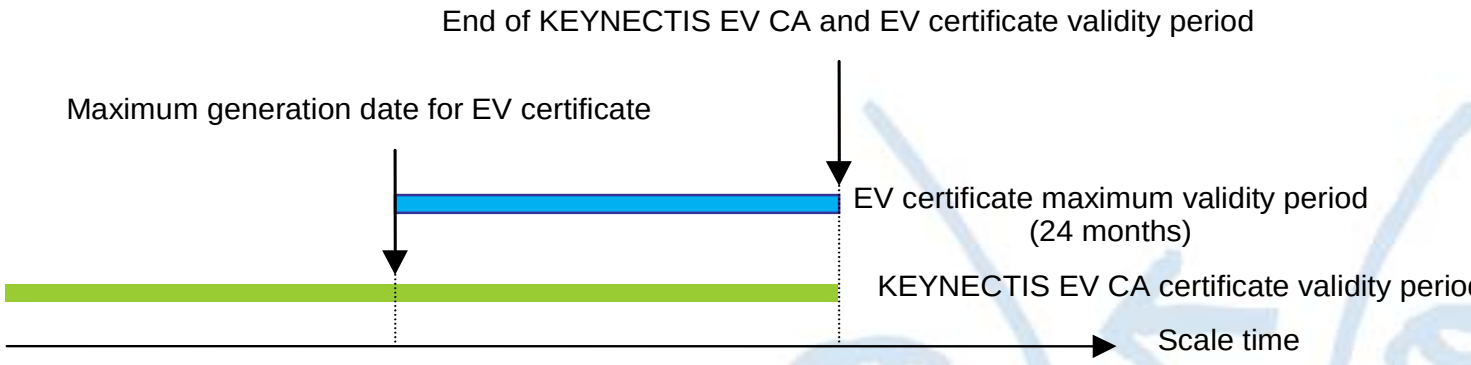
5.6.1 EV certificate

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

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

5.6.2 KEYNECTIS EV CA certificate

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



As soon as a new KEYNECTIS EV CA key pair is generated, only the new EV CA private key is used to sign EV certificates and CRL.
The previous EV CA certificate stays valid for validation process of certification path until the EV certificates are all expired.

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

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

KEYNECTIS EV CA established business continuity procedures for the KEYNECTIS EV CA PKI that outlines the steps to be taken in the event of the corruption or loss of computing resources, software and/or data that could disturb or compromise the KEYNECTIS EV CA services. KEYNECTIS EV CA carries out a risk assessment to evaluate business risks and determines the necessary security requirements and operational procedures and

elaborates in consequences its disaster recovery plan. This risk analysis is regularly reviewed and revised if necessary (threat evolution, vulnerability evolution …). This business continuity is in the scope of the audit process as described in section 8 to validate what are the operations that are first maintained after a disaster and the recovery plan.

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

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

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

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

If KEYNECTIS EV CA equipment is damaged or rendered inoperative, but the signature keys are not destroyed, the operation is re-established as quickly as possible, giving priority to the ability to generate certificates status information according to the KEYNECTIS EV CA disaster recovery plan.

5.7.3 Entity private key compromise procedures

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

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

5.7.4 Business continuity capabilities after a Disaster

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

5.8 EV CA component termination

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

.

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

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

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

KEYNECTIS EV CA key generation is realized during a key ceremony that is undertaken in a physically secured environment by personnel in trusted roles under, at least, dual control. KEYNECTIS EV CA key generation is carried out within Hardware Security Modules.

EV customer key pairs are generated by the customers themselves.

6.1.2 Private Key Delivery to Customer

As customers proceed to key pair generation on their own, the KEYNECTIS EV CA do not deliver private keys to its EV certificate customers.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

EV CA certificate is available to relying parties through the PS (refer to § 2.2 above).

6.1.5 EV certificate Key Size

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

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

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

6.1.6 Public Key Parameters Generation and Quality Checking

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

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

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

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

6.2 Private Key Protection and Cryptographic Module Engineering

6.2.1 Cryptographic Module Standards and Controls

KEYNECTIS EV CA HSM used for EV certificate generation purposes are certified according to ISO 15408 Common Criteria or approved according to NIST FIPS 140-2 standard.

EV certificate customers are responsible for the choice of the cryptographic provider they use to generate, use and store their private keys.

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

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

The TC is responsible to protect and control the private key of the EV certificate customer he or she act for, in a manner to be sure that only authorized use of it is made.

6.2.3 Private Key Escrow

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

6.2.4 Private Key Backup

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

6.2.5 Private Key Archival

KEYNECTIS EV CA private keys are not archived.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

KEYNECTIS EV CA private keys are generated activated and stored in a hardware security module. When private keys are outside the hardware security module (either for storage or transfer), they are encrypted using the AES or the Triple DES algorithm. An encrypted private key cannot be decrypted other than in a cryptographic module under multiple control with trusted role.

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

KEYNECTIS EV CA private key is activated under the necessary minimum 4 persons in trusted roles.

6.2.9 Method of Deactivating Private Key

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

6.2.10 Method of Destroying Private Key

KEYNECTIS EV CA private keys are destroyed when they are no longer needed or when the certificates to which they correspond expired or are revoked. Destroying private key requires destroying all associated activation data in a manner that no information can be used to deduce any part of the private key. Internal KEYNECTIS policies apply to ensure destruction, including physical destruction of materials that support private keys.

6.2.11 Cryptographic Module Rating

KEYNECTIS EV CA hardware security modules are certified at least certified ISO 15408 Common Criteria at EAL 4+ level in accordance to protection profile CWA 14167-2 " Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)".

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public keys are archived as part of the certificate archival process, as described in § 5.5.2 above.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

KEYNECTIS EV CA and EV certificate have validity periods defined in § 5.6 above.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of KEYNECTIS EV CA data used to activate KEYNECTIS EV CA private keys are made during a key ceremony (Refer to section 6.1.1 above). Activation data are generated automatically and delivered to the activation data holders who are KEYNECTIS employees in trusted roles, in a manner to ensure confidentiality and integrity of activation data.

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

6.4.2 Activation Data Protection

KEYNECTIS EV CA activation data are protected from disclosure by a combination of cryptographic and physical access control mechanisms. KEYNECTIS EV CA activation data are stored in smart cards, managed in accordance with KEYNECTIS sensitive item management policy and protected in accordance with measure described in KEYNECTIS physical security policy.

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

6.4.3 Other Aspects of Activation Data

KEYNECTIS EV CA activation data are only held by KEYNECTIS employees in trusted roles, in accordance with KEYNECTIS segregation of duties policy.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions are provided by the operating system, or through a combination of operating systems, software, and physical safeguards. KEYNECTIS EV CA PKI components support the following functionalities:

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

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

6.5.2 Computer Security Rating

All KEYNECTIS EV CA PKI components software are compliant with requirements of protection profiles issued from the French infosec agency (PP_IGC, PP_AC and PP_AE available at www.ssi.gouv.fr).

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The System Development Controls for the KEYNECTIS EV CA are as follows:

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

6.6.2 Security Management Controls

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

6.6.3 Life Cycle Security Controls

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

6.7 Network Security Controls

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

6.8 Time-Stamping

All KEYNECTIS EV CA components are regularly synchronized using a Network Time Protocol (NTP) Service which get time form GPS receivers. Time derived from the time service is be used for establishing the time of:

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

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

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

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

Basic Certificate fields	Value
Version	2 (=version 3)
Serial number	Determined by KEYNECTIS Extended Validation CA
Key length	1024 or 2048 bits
Validity duration	1 or 2 years (depending on key length)
Issuer DN	O = Certplus OU = Entity of KEYNECTIS for CA services CN = KEYNECTIS Extended Validation CA C = FR
Subject DN (information related to subject's business place)	CN=<DNS Name> O=<Requesting Entity> OU=<Requesting Entity Sub-Division> (if any) C=<countryName> Postal code = <postalCode> S=<stateOrProvinceName> (if any) L=<localityName> STREET = <streetAddress> 2.5.4.15 = V1.0, clause 5.(b)', 'V1.0, Clause 5.(c)', 'V1.0, Clause 5.(d)' or 'V1.0, Clause 5.(e), as applicable SERIAL NUMBER = <Number assigned to the Subject by the incorporating or Registration Agency> 1.3.6.1.4.1.311.60.2.1.3 = <jurisdictionOfIncorporationCountryName>
Public Key Algorithm	sha1WithRSAEncryption (1.2.840.113549.1.1.5)
Parameters	NULL

7.1.1 Certificate Extensions

Standard Extensions	OID	Included	Critical	Value
Authority Key Identifier	{id-ce 35}	**X**	**FALSE**	
Methods of generate key ID				**Method 1**
Select AKI Fields				**Key Identifier**
Certificate Policies	{id-ce 32}			
policyIdentifiers		**X**		**[1.3.6.1.4.1.22234.2.5.2.3.1]**
policyQualifierID		**X**		
OID				[id-qt-cps]
cPSuri				http://www.keynectis.com/PC
CRL Distribution Points	{id-ce 31}	**X**	**FALSE**	
distributionPoint				URL= http://trustcenter-crl.certificat2.com/keynectis/class2keynectisevca.crl
Authority Info Access	(1.3.6.1.5.5.7.1.1)			n/a
Key Usage	{id-ce 15}	**X**	**FALSE**	

Digital Signature				**Set**
Non Repudiation				**Clear**
Key Encipherment				**Set**
Data Encipherment				**Clear**
Key Agreement				**Clear**
Key CertSign				**Clear**
Key CRL Sign				**Clear**
Extended Key Usage	{id-ce 37}	**X**	**FALSE**	
Client Authentication	1.3.6.1.5.5.7.3.2			**Set**
Server Authentication	1.3.6.1.5.5.7.3.1			**Set**
Subject Key Identifier	{id-ce 14}	**X**	**FALSE**	
Methods of generating key ID				**Method 1**

7.1.2 Algorithm Object Identifiers

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

7.1.3 Name Forms

Name forms follow requirements described in § 3.1 above.

7.1.4 Certificate Policy Object Identifier

EV certificates contain the OID defined in the KEYNECTIS EV CA CPS (refer to § 1.2 above).

7.1.5 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.6 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

KEYNECTIS EV CA issues X.509 version two (v2) CRLs (populate version field with integer "1").

The CRL fields are those defined in RFC 3280.

7.2.1 CRL and CRL Entry Extensions

CRL extensions are:
- CRLNumber
- AKI

CRL entry extensions are:
- RevocationReason

7.3 OCSP Profile

If an OCSP is used, then it is compliant with RFC2560.

7.3.1 Version Number(s)

If an OCSP is used, version 1 of the OCSP specification, as defined by RFC2560, is supported.

7.3.2 OCSP Extensions

If an OCSP is used, CPS will give details on OCSP extensions.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency and Circumstances of Assessment

The KEYNECTIS EV CA is subject to periodic compliance audits to allow KEYNECTIS SSL RCA to authorize or not (regarding the audit result) KEYNECTIS EV CA to operate under this CPS. The KMA has the right to require and make a compliance audit of the KEYNECTIS EV CA PKI components and other entities (for instance RA) that operate for EV certificate issuance purposes.

8.1.1 Internal audits

KEYNECTIS EV CA controls its service quality by performing ongoing self audits against a randomly selected sample of at least three percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken. These audits are realized at CA premises by KEYNECTIS EV CA auditors on behalf of the KMA.

For Club EV and ISP EV offer Certificates where the final cross correlation and due diligence requirements, the CA controls its service quality by performing ongoing self audits against a randomly selected sample of at least six percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken. These audits are realized at RA premises by KEYNECTIS EV CA auditors on behalf of the KMA.

8.1.2 External audits

The KEYNECTIS EV CA is subject to annual:

- ETSI TS101456 compliance audits, as part of the European DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures audit scheme, and
- Webtrust for EV audits in order to demonstrate it operates in compliance with "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES".

8.2 Identity/Qualifications of Assessor

8.2.1 Internal audits

Auditors in charge of internal audits are issued from the security & quality department of KEYNECTIS. They are have competence in the field of compliance audits and are familiar with PKI components operation. Audits are directed by a certified ISO 27001 lead auditor.

8.2.2 External audits

The compliance auditors have competence in the field of compliance audits and are familiar with requirements of "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES". They use to perform such compliance audits as a primary responsibility.

KEYNECTIS EV CA selects itself the auditors among auditors that are cleared to realize ETSI TS 101456 and currently licensed to perform WebTrust for CA audits and WebTrust EV Program audits.

8.3 Assessor's Relationship to Assessed Entity

8.3.1 Internal audits

Auditors in charge of internal audits are either KEYNECTIS employees from the security & quality department, either employees of a company approved by the KEYNECTIS security & quality department to run internal audits on KEYNECTIS PKI components.

8.3.2 External audits

The compliance auditors act on behalf of a third party auditor which is a private public accounting firm, independent from KEYNECTIS EV CA.

The KMA determines whether a compliance auditor meets this requirement.

8.4 Topics Covered by Assessment

8.4.1 Internal audits

Topics covered by internal audits are:

- EV certificate issuance quality of service, and
- Any other topic identified in the KEYNECTIS audit policy on PKI components providing services to KEYNECTIS.

8.4.2 External audits

The purpose of a compliance audit is to verify that all components operating on behalf of KEYNECTIS EV CA operates in compliance with:

- ETSI 101456 standard which defines requirements for certification authorities issuing qualified certificates;
- the present CPS and "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES".

8.5 Actions Taken as a Result of Deficiency

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

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

When the auditor finds a discrepancy between how the EV CA is designed or is being operated or maintained and the requirements of this CPS, the following actions are performed:

- the compliance auditor notes the discrepancy;
- the compliance auditor notifies the KMA and the component where the discrepancy is identified of the discrepancy;
- the party responsible for correcting the discrepancy determines what further notifications or actions are necessary pursuant to the requirements of this CPS, and then proceed to make such notifications and take such actions without delay in relation with the approval of KMA.

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

8.6 Communications of Results

8.6.1 Internal audits

Internal audit reports, including identification of corrective measures taken or being taken by the component, are provided to the KMA that inform the audited components of the results of internal audits. Internal audit reports are not available on Internet for relying party.

8.6.2 External audits

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

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal issuance Fees

The issuance of KEYNECTIS EV CA Certificates is subject to fees indicated on the KEYNECTIS web site www.keynectis.com, or throught requested quoted.

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

The KEYNECTIS EV CA PS access (that contains CRL issued by KEYNECTIS RCA and CRL for EV certificates) is free access on the Internet, free of charge. This publication is not intended to be used by OCSP services or other else similar services but only for relying party to verify that an EV certificate is valid or not.

9.1.4 Fees for Other Services

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

9.1.5 Refund Policy

KEYNECTIS has a refund policy as operating a CA.

Re-issuance of EV certificate is only possible for an identical request, i.e. same requesting entity, same Certificate Signing Request.

There is no additional cost for a replacement requested by written within 14 days of the initial request, no additional paperwork is required. From 15 to 90 days, a half applicable fee will apply, no additional paperwork is required. Over 90 days, the replacement demand is considered as a new demand. Checks and fees are the same as for an initial EV certificate request.

9.2 Financial Responsibility

Keynectis maintains an appropriate insurance related to its respective performance and obligations under this CPS and the EV Guidelines.

Services provided by KEYNECTIS in accordance with the terms and conditions specified and defined herein are covered by an insurance policy “Commercial General liability” (including Products and Completed Operations coverage and Contractual Liability Coverage) with limits of not less than (the equivalent of) 7.500.000 euro. Coverage has been affected in respect of Keynectis responsibilities hereunder, in particular this insurance policy applies to any loss as a result of an error in the identification process that may be committed by Keynectis employee.
Upon Subscriber request, Keynectis shall furnish to Subscriber a Certificate of Insurance.

KEYNECTIS maintains reasonable sufficient financial resources to maintain its operations and fulfil its duties under this CPS.

If there is a damage for an EV customer due to KEYNECTIS EV CA fault then KEYNECTIS EV CA will activate its insurance to cover part of the customer damage in the limit of the KEYNECTIS EV CA liability even if damages exceed the amount set by Keynectis.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

KEYNECTIS EV CA guarantees that only trusted and authorized personnel have access and use these following confidential information, in accordance with its segregation of duty and protection of information policies:

- Records and archives;

- Personal identity data;
- KEYNECTIS EV CA private keys;
- KEYNECTIS EV CA secret activation data;
- Audit result and reports;
- Disaster recovery plans;
- Customer purchase orders
- Internal KEYNECTIS EV CA security policy and procedures;
- Part of the CPS defined as confidential.

9.3.2 Information Not Within the Scope of Confidential Information

Information published by the PS (certificate and their content, status of a certificate) is not considered as confidential, but is subject to protection according to applicable laws on intellectual property rights.

9.3.3 Responsibility to Protect Confidential Information

KEYNECTIS EV CA has to respect the requirements described in the European law for the protection of personal data (confidential and personal data), completed by French law on privacy data protection.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

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

9.4.2 Information Treated as Private

KEYNECTIS EV CA considers that information that are considered as private are:

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

9.4.3 Information Not Deemed Private

No stipulation.

9.4.4 Responsibility to Protect Private Information

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

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

KEYNECTIS EV CA is compliant with French law on privacy data protection, and has protected procedure to give access to the private data for legal entity with authentication and secure controlled access to those data.

9.4.7 Other Information Disclosure Circumstances

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

9.5 Intellectual Property rights

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

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

9.6 Representations and Warranties

9.6.1 KEYNECTIS EV CA Representations and Warranties

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

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

Common obligations for KEYNECTIS EV CA components have to:

- Protect and guarantee integrity and confidentiality of their secret data and/or private keys;
- Only use their cryptographic keys and certificates, with associated tools specified in CPS, for what purpose they have been generated;
- Respect and operate CPS part that deals with their duty;
- Let auditors fulfil their tasks and communicate every useful information to them, control and verify the compliance with the present CPS;
- Respect total or part of agreements that binds it to EV representatives;
- document their internal procedure to complete global CPS;
- Use every means (technical and humans) necessary to achieve the realization of the CPS it has to implement and they are responsible for.

9.6.2 Applicant Representations and Warranties

The EV certificate applicant has the following obligations:

- Submit accurate and complete information to the RA;
- Keep secret information used for authentication purposes with KEYNECTIS EV CA components confidential;
- Respect the present CPS and the Keynectis EV CA associated subscriber agreement.

9.6.3 RA Representation and Warranties

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

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

9.6.4 Applicant Technical Contact Representation and Warranties

The applicant Technical Contact has the following obligations:

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

9.6.5 Representations and Warranties of Other Participants

9.6.5.1 KMA

KMA has the following obligations:

- Approve the KEYNECTIS EV CPS;
- Audit KEYNECTIS EV CA and KEYNECTIS and EV entities acting as RA;
- Control contractual relationship with EV entities acting as RA.

9.6.5.2 EV Administrator

EV Administrator has the following obligations:

- Submit accurate and complete information to the KEYNECTIS EV CA ;

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

9.7 Disclaimers of Warranties

This section includes disclaimers of express warranties of Keynectis EV CA.

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

9.8 Limitations on Keynectis EV Certificate Liability

9.8.1 Subscribers and Relying Parties.

According to EV Certificate Guidelines, in cases where Keynectis has issued and managed the EV Certificate in compliance with these Guidelines and this CPS, Keynectis disclaims liability to the EV Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such EV Certificate beyond those specified in this CPS.

In cases where Keynectis has not issued or managed the EV Certificate in complete compliance with these Guidelines and this CPS, Keynectis limits its liability to the Subscriber and to Relying Parties for any cause of action or legal theory involved for claims, losses or damages suffered as a result of the use or reliance on such EV Certificate to a maximum monetary amount of 100.000 euros per EV Certificate even if damages exceed this amount.

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

In no event (except for fraud or wilful misconduct) is Keynectis liable for:
- Any loss of profits.
- Any loss of data.
- Any indirect or consequential damages arising from or in connection with the use of certificates.
- Any other damages except for information featured on, free, test or demo certificates.
- Any liability incurred in any case if the error in such verified information is the result of fraud or wilful misconduct of the applicant.

9.8.2 Indemnification of Application Software Vendors.

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, Keynectis acknowledges that the Application Software Vendors who have a root certificate distribution agreement in place do not assume any obligation or potential liability of the CA under the EV Guidelines or that otherwise might exist because of the issuance or maintenance of EV Certificates or reliance thereon by Relying Parties or others. Thus, Keynectis shall defend, indemnify, and hold harmless each Application Software Vendor for any and all claims, damages, and losses suffered by such Application Software Vendor related to an EV Certificate issued by the CA, regardless of the cause of action or legal theory involved.
This shall not apply, however, to any claim, damages, or loss suffered by such Application Software Vendor related to an EV Certificate issued by Keynectis where such claim, damage, or loss was directly caused by such Application Software Vendor's software displaying as not trustworthy an EV Certificate that is still valid, or displaying as trustworthy: (1) an EV Certificate that has expired, or (2) an EV Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the browser software either failed to check such status or ignored an indication of revoked status).

9.9 Root CA Indemnification

Non applicable.

9.10 Term and Termination

9.10.1 Term

The CPS and its amendments become effective upon adoption by the KMA and publication on the website by the Keynectis CA.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

End of validity of the present CPS ends all the obligation and liability for the KEYNECTIS EV CA.

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

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

9.12.3 Circumstances under Which OID Must be Changed

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

9.13 Dispute Resolution Provisions

KEYNECTIS proposes to solve dispute on identity to set in the certificate, and in the case that parties in conflict can't find an arrangement the problem will be solved in a French national court.

9.14 Governing Law

The applicable laws that govern the CPS applicability are the laws of France. This choice of law is made to ensure uniform procedures and interpretation for all EV customers with no matter at where they are located.

9.15 Compliance with Applicable Law

This CPS is subject to applicable French law, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing cryptographic software, hardware, or technical information.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

If there is any, general conditions of use of the KEYNECTIS EV CA services and / or CPS will identify specific requirements.

9.16.2 Assignment

Except where specified by other contracts, only the KEYNECTIS EV CA may assign and delegate this CPS to any party of its choice.

9.16.3 Severability

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

9.16.4 Waiver of Rights

The requirements defined in the KEYNECTIS EV CA CPS are to be implemented as described in the present CPS without possible waiver of right in the intention of changing any defined rights or obligation.

9.16.5 Act of god

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

9.17 Other Provisions

No other provisions.

Annex A - INFORMATION VERIFICATION REQUIREMENTS issued from "GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES"

F. INFORMATION VERIFICATION REQUIREMENTS

13. General Overview This part of the Guidelines sets forth Verification Requirements and Acceptable Methods of Verification for each such Requirement**.**

(a) Verification Requirements – Overview Before issuing an EV Certificate, the CA MUST ensure that all Subject organization information in the EV Certificate conforms to the requirements of, and has been verified in accordance with, these Guidelines and matches the information confirmed and documented by the CA pursuant to its verification processes. Such verification processes are intended to accomplish the following:

(1) Verify Applicant's existence and identity, including;

(a) Verify Applicant's legal existence and identity (as more fully set forth in Section 14 herein),

(b) Verify Applicant's physical existence (business presence at a physical address), and

(c) Verify Applicant's operational existence (business activity).

(2) Verify Applicant is a registered holder, or has exclusive control, of the domain name to be included in the EV Certificate;

(3) Verify Applicant's authorization for the EV Certificate, including;

(a) Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester;

(b) Verify that Contract Signer signed the Subscriber Agreement; and

(c) Verify that a Certificate Approver has signed or otherwise approved the EV Certificate Request.

(b) Acceptable Methods of Verification – Overview As a general rule, the CA is responsible for taking all verification steps reasonably necessary to satisfy each of the Verification Requirements set forth in the sections below. The Acceptable Methods of Verification set forth in each of Sections 14 through 25 below (which usually include alternatives) are considered to be the minimum acceptable level of verification required of the CA. In all cases, however, the CA is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement.

14. Verification of Applicant's Legal Existence and Identity

(a) Verification Requirements To verify Applicant's legal existence and identity, the CA MUST do the following:

(1) Private Organizations

a. Legal Existence Verify that Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration, and not designated on the records of the Incorporating or Registration Agency by labels such as "inactive", "invalid", "not current", or the equivalent.

b. Organization Name Verify that Applicant's formal legal name as recorded with the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration matches Applicant's name in the EV Certificate Request.

c. Registration Number Obtain the specific Registration Number assigned to Applicant by the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration. Where the Incorporating or Registration Agency does not assign a Registration Number, the CA SHALL obtain Applicant's date of Incorporation or Registration.

d. Registered Agent Obtain the identity and address of Applicant's Registered Agent or Registered Office (as applicable in Applicant's Jurisdiction of Incorporation or Registration).

(2) Government Entities

a. Legal Existence Verify that Applicant is a legally recognized Government Entity, in existence in the political subdivision in which such Government Entity operates.

b. Entity Name Verify that Applicant's formal legal name matches Applicant's name in the EV Certificate Request.

c. Registration Number The CA SHOULD obtain Applicant's date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity. In circumstances where this information is not available, the CA MUST enter appropriate language to indicate that the Subject is a Government Entity

(3) Business Entities

a. Legal Existence Verify that Applicant is engaged in business under the name submitted by Applicant in the Application.

b. Organization Name Verify that Applicant's formal legal name as recognized by the Registration Authority in Applicant's Jurisdiction of Registration matches Applicant's name in the EV Certificate Request.
c. Registration Number Obtain the specific unique Registration Number assigned to Applicant by the Registration Agency in Applicant's Jurisdiction of Registration. Where the Registration Agency does not assign a Registration Number, the CA SHALL obtain Applicant's date of Registration.
d. Principal Individual Verify the identity of the identified Principal Individual.
(4) Non-Commercial Entities (International Organization Entities)
a. Legal Existence Verify that Applicant is a legally recognized International Organization Entity.
b. Entity Name Verify that Applicant's formal legal name matches Applicant's name in the EV Certificate Request.
c. Registration Number The CA SHOULD obtain Applicant's date of formation, or the identifier for the legislative act that created the International Organization Entity. In circumstances where this information is not available, the CA MUST enter appropriate language to indicate that the Subject is an International Organization Entity.

(b) Acceptable Method of Verification

(1) Private Organizations: All items listed in subsection (a)(1) above MUST be verified directly with, or obtained directly from, the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration. Such verification MAY be through use of a Qualified Government Information Source operated by, or on behalf of, the Incorporating or Registration Agency, or by direct contact with the Incorporating or Registration Agency in person or via mail, e-mail, web address, or telephone, using an address or phone number obtained from a Qualified Independent Information Source.
(2) Government Entities: All items listed in subsection (a)(2) above MUST either be verified directly with, or obtained directly from, one of the following: (i) a QGIS in the political subdivision in which such Government Entity operates; (ii) a superior governing Government Entity in the same political subdivision as Applicant (e.g. a Secretary of State may verify the legal existence of a specific State Department), or (iii) from a judge that is an active member of the federal, state or local judiciary within that political subdivision, or (iv) an attorney representing the Government Entity.
Any communication from a judge SHALL be verified in the same manner as is used for verifying factual assertions that are asserted by an Attorney as set forth in Section 22(a) below. Such verification MAY be by direct contact with the appropriate Government Entity in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained from a Qualified Independent Information Source.
(3) Business Entities: All items listed in subsection (a)(3) above, MUST be verified directly with, or obtained directly from, the Registration Agency in Applicant's Jurisdiction of Registration. Such verification MAY be through use of a Qualified Government Information Source, a Qualified Governmental Tax Information Source, or by direct contact with the Registration Agency in person or via mail, e-mail, web address, or telephone, using an address or phone number obtained from a Qualified Independent Information Source. In addition, the CA MUST validate a Principal Individual associated with the Business Entity pursuant to the requirements in subsection (4) below.
(4) Principal Individual: A Principal Individual associated with the Business Entity MUST be validated in a face-to-face setting. The CA MAY rely upon a face-to-face validation of the Principal Individual performed by the Registration Agency, provided that the CA has evaluated the validation procedure and concluded that it satisfies the requirements of the Guidelines for face-to-face validation procedures. Where no face-to-face validation was conducted by the Registration Agency, or the Registration Agency's face-to-face validation procedure does not satisfy the requirements of the Guidelines, the CA SHALL perform face-to-face validation.
(a) Face-to-face validation: The face-to-face validation MUST be conducted before either an employee of the CA, a Latin Notary, a Notary (or equivalent in Applicant's jurisdiction), a Lawyer, or Accountant ("Third-Party Validator"). The Principal Individual(s) MUST present the following documentation ("Vetting Documents") directly to the Third-Party Validator:
(i) A Personal Statement that includes the following information:
1. Full name or names by which a person is, or has been, known (including all other names used);
2. Residential Address at which he/she can be located;
3. Date of birth;
4. An affirmation that all of the information contained in the Certificate Request is true and correct.
(ii) A current signed government-issued identification document that includes a photo of the Individual and is signed by the Individual such as:
1. A passport;
2. A drivers license;
3. A personal identification card;
4. A concealed weapons permit;
5. A military ID.

(iii) At least two secondary documentary evidences to establish his/her identity that include the name of the Individual, one of which MUST be from a financial institution.
1. Acceptable financial institution documents include:
a. A major credit card, provided that it contains an expiration date and it has not expired.
b. A debit card from a regulated financial institution, provided that it contains an expiration date and it has not expired.
c. A mortgage statement from a recognizable lender that is less than six months old.
d. A bank statement from a regulated financial institution that is less than six months old.
Acceptable non-financial documents include:
1. Recent original utility bills or certificates from a utility company confirming the arrangement to pay for the services at a fixed address (not a mobile/cellular telephone bill).
2. A copy of a statement for a payment of a lease provided the statement is dated within the past six months.
3. A certified copy of a birth certificate.
4. A local authority tax bill for the current year.
5. A certified copy of a court order, such as a divorce certificate, annulment papers, or adoption papers.
The Third-Party Validator performing the face-to-face validation MUST:
1. Attest to the signing of the Personal Statement and the identity of the signer; and
2. Identify the original Vetting Documents used to perform the identification. In addition, the Third-Party Validator MUST attest on a copy of the current signed government-issued photo identification document that it is a full, true, and accurate reproduction of the original.
(b) Cross-checking of Information: The CA MUST obtain the original signed and attested Personal Statement together with the attested copy of the current signed government-issued photo identification document. The CA must review the documentation to determine that the information is consistent, matches the information in the application and identifies the Individual.
(c) Verification of Third-party validator: The CA MUST independently verify that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in Applicant's jurisdiction), Lawyer, or Accountant in the jurisdiction of the Individual's residency, and that the Third-Party Validator actually did perform the services and did attest to the signature of the Individual.
(5) Non-Commercial Entities (International Organization Entities):
All items listed in subsection 14(a)(4)(1) MUST be verified either:
(a) With reference to the constituent document under which the International Organization was formed; or
(b) Directly with a signatory country's government in which the CA is permitted to do business. Such verification may be obtained from an appropriate government agency or from the laws of that country, or by verifying that the country's government has a mission to represent it at the International Organization; or
(c) Directly against any current list of qualified entities that the CABForum may maintain at www.cabforum.org.
(d) In cases where the International Organization applying for the EV certificate is an organ or agency - including a non-governmental organization (NGO) of a verified International Organization, then the CA may verify the International Organization applicant directly with the verified umbrella International Organization of which the applicant is an organ or agency.

15. Verification of Applicant's Legal Existence and Identity – Assumed Name
(a) Verification Requirements If, in addition to Applicant's formal legal name as recorded with the applicable Incorporating Agency or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration, Applicant's identity as asserted in the EV Certificate is to contain any assumed name (also known as "doing business as", "DBA", or "d/b/a" in the US, and "trading as" in the UK) under which Applicant conducts business, the CA MUST verify that: (i) Applicant has registered its use of the assumed name with the appropriate government agency for such filings in the jurisdiction of its Place of Business (as verified in accordance with these Guidelines), and (ii) that such filing continues to be valid.
(b) Acceptable Method of Verification To verify any assumed name under which Applicant conducts business:
(1) The CA MAY verify the assumed name through use of a Qualified Government Information Source operated by, or on behalf of, an appropriate government agency in the jurisdiction of Applicant's Place of Business, or by direct contact with such government agency in person or via mail, e-mail, web address, or telephone; or
(2) The CA MAY verify the assumed name through use of a Qualified Independent Information Source provided that the QIIS has verified the assumed name with the appropriate government agency.
(3) The CA MAY rely on a Verified Legal Opinion, or a Verified Accountant Letter that indicates the assumed name under which Applicant conducts business, the government agency with which the assumed name is registered, and that such filing continues to be valid.
16. Verification of Applicant's Physical Existence

(a) Address of Applicant's Place of Business

(1) Verification Requirements To verify Applicant's physical existence and business presence, the CA MUST verify that the physical address provided by Applicant is an address where Applicant or a Parent/Subsidiary Company conducts business operations (e.g., not a mail drop or P.O. box), and is the address of Applicant's Place of Business.

(2) Acceptable Methods of Verification To verify the address of Applicant's Place of Business:

(A) For Applicants whose Place of Business is in the same country as Applicant's Jurisdiction of Incorporation or Registration:

(1) For Applicants whose Place of Business is in the same country as Applicant's Jurisdiction of Incorporation or Registration:

(1) For Applicants listed at the same Place of Business address in the current version of either at least one Qualified Independent Information Source or a Qualified Governmental Tax InformationSource, the CA MUST confirm that Applicant's address as listed in the EV Certificate Request is a valid business address for Applicant or a Parent/Subsidiary Company by reference to such Qualified Independent Information Sources or a Qualified Governmental Tax Information Source, and MAY rely on Applicant's representation that such address is its Place of Business;

(2) For Applicants who are not listed at the same Place of Business address in the current version of either at least one Qualified Independent Information Source or a Qualified Governmental Tax Information Source, the CA MUST confirm that the address provided by Applicant in the EV Certificate Request is in fact Applicant's or a Parent/Subsidiary Company's business address, by obtaining documentation of a site visit to the business address, which MUST be performed by a reliable individual or firm. The documentation of the site visit MUST:

(a) Verify that Applicant's business is located at the exact address stated in the EV Certificate Request (e.g., via permanent signage, employee confirmation, etc.);

(b) Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location;

(c) Indicate whether there is a permanent sign (that cannot be moved) that identifies Applicant;

(d) Indicate whether there is evidence that Applicant is conducting ongoing business activities at the site (e.g., that it is not just a mail drop, P.O. box, etc.); and

(e) Include one or more photos of (i) the exterior of the site (showing signage indicating Applicant's name, if present, and showing the street address if possible), and (ii) the interior reception area or workspace

(3) For all Applicants, the CA MAY alternatively rely on a Verified Legal Opinion or a Verified Accountant Letter that indicates the address of Applicant's or a Parent/Subsidiary Company's Place of Business and that business operations are conducted there.

(4) For Government Entity Applicants, the CA MAY rely on the address contained in the records of the QGIS in Applicant's Jurisdiction.

(B) For Applicants whose Place of Business is not in the same country as Applicant's Jurisdiction of Incorporation or Registration, the CA MUST rely on a Verified Legal Opinion that indicates the address of Applicant's Place of Business and that business operations are conducted there.

(b) Telephone Number for Applicant's Place of Business

(1) Verification Requirements To further verify Applicant's physical existence and business presence, as well as to assist in confirming other verification requirements, the CA MUST verify that the telephone number provided by Applicant is a main phone number for Applicant's Place of Business.

(2) Acceptable Methods of Verification To verify Applicant's telephone number, the CA MUST perform A and one of B, C, or D as listed below:

(A) Confirm Applicant's telephone number by calling it and obtaining an affirmative response sufficient to enable a reasonable person to conclude that Applicant is reachable by telephone at the number dialed; and

(B) Confirm that the telephone number provided by Applicant is listed as Applicant's or Parent/Subsidiary Company's telephone number for the verified address of its Place of Business in records provided by the applicable phone company, or, alternatively, in either at least one (1) Qualified Independent Information Source or a Qualified Governmental Tax Information Source; *or*

(C) During a site visit, the person who is conducting the site visit MUST confirm Applicant's or Parent/Subsidiary Company's main telephone number by calling it and obtaining an affirmative response sufficient to enable a reasonable person to conclude that Applicant is reachable by telephone at the number dialed. The CA MUST also confirm that Applicant's main telephone number is not a mobile phone; *or*

(D) Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that Applicant's telephone number, as provided, is a main phone number for Applicant's Place of Business.

(E) For Government Entity Applicants, the CA MAY rely on the telephone number contained in the records of the QGIS in Applicant's Jurisdiction.

17. Verification of Applicant's Operational Existence

(a) Verification Requirements If Applicant has been in existence for less than three years, as indicated by the records of the Incorporating Agency or Registration Agency, and is not listed in either the current version of one Qualified Independent Information Source or a Qualified Governmental Tax Information Source, the CA MUST verify that Applicant has the ability to engage in business.

(b) Acceptable Methods of Verification To verify Applicant's operational existence, the CA MUST perform one of the following:

(1) Verify Applicant has an active current Demand Deposit Account with a Regulated Financial Institution. The CA MUST receive authenticated documentation directly from a Regulated Financial Institution verifying that Applicant has an active current Demand Deposit Account with the institution.

(2) Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that Applicant has an active current Demand Deposit Account with a Regulated Financial Institution;

18. Verification of Applicant's Domain Name

(a) Verification Requirements To verify Applicant's registration, or exclusive control, of the domain name(s) to be listed in the EV Certificate, the CA MUST verify that each such domain name satisfies the following requirements:

(1) The domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN)-approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA);

(2) Domain registration information in the WHOIS database SHOULD be public and SHOULD show the name, physical address, and administrative contact information for the organization.

For Government Entity Applicants, the CA MAY rely on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name.

(3) Applicant:

(A) is the registered holder of the domain name; or

(B) has been granted the exclusive right to use the domain name by the registered holder of the domain name;

(4) Applicant is aware of its registration or exclusive control of the domain name;

(b) Acceptable Methods of Verification

(1) Applicant as Registered Holder Acceptable methods by which the CA MAY verify that Applicant is the registered holder of the domain name include the following:

(A) Performing a WHOIS inquiry on the Internet for the domain name supplied by Applicant, and obtaining a response indicating that Applicant or a Parent/Subsidiary Company is the entity registered to the domain name; or

(B) Communicating with the contact listed on the WHOIS record to confirm that Applicant is the registered holder of the domain name and having the contact update the WHOIS records to reflect the proper domain name registration. Confirmation that the registered owner of the domain name is a Parent/Subsidiary Company of Applicant, or a registered trading name of Applicant is sufficient to establish that Applicant is the registered owner of the domain name;

(C) In cases where domain registration information is private, and the domain registrar offers services to forward communication to the registered domain holder, the CA MAY contact Applicant through the domain registrar by e-mail or paper mail.

(2) Applicant's Exclusive Right to Use In cases where Applicant is not the registered holder of the domain name, the CA MUST verify Applicant's exclusive right to use the domain name(s).

(A) In cases where the registered domain holder can be contacted using information obtained from WHOIS, or through the domain registrar, the CA MUST obtain positive confirmation from the registered domain holder by paper mail, e-mail, telephone, or facsimile that Applicant has been granted the exclusive right to use the requested Fully Qualified Domain Name (FQDN).

If the Top-Level Domain is a generic top-level domain (gTLD) such as .com, .net, or .org in accordance with RFC 1591, the CA MUST obtain positive confirmation from the second-level domain registration holder. For example, if the requested FQDN is www1.www.example.com, the CA MUST obtain positive confirmation from the domain holder of example.com.

If the Top-Level Domain is a 2 letter Country Code Top-Level Domain (ccTLD), the CA MUST obtain positive confirmation from the domain holder at the appropriate domain level, based on the rules of the ccTLD. For example, if the requested FQDN is www.mysite.users.internet.co.uk, the CA MUST obtain positive confirmation from the domain holder of internet.co.uk.

In addition, the CA MUST verify Applicant's exclusive right to use the domain name using one of the following methods:

(1) Relying on a Verified Legal Opinion to the effect that Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet; or

(2) Relying on a representation from the Contract Signer, or the Certificate Approver, if expressly so authorized in a mutually-agreed upon contract.

(B) In cases where the registered domain holder cannot be contacted, the CA MUST:
(1) Rely on a Verified Legal Opinion to the effect that Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet, and
(2) Rely on a representation from the Contract Signer, or the Certificate Approver, if expressly so authorized in a mutually-agreed-upon contract, coupled with a practical demonstration by Applicant establishing that it controls the domain name by making an agreedupon change in information found online on a web page identified by a uniform resource identifier containing Applicant's FQDN;
(3) Knowledge Acceptable methods by which the CA MAY verify Applicant is aware that it has exclusive control of the domain name include the following:
(A) Relying on a Verified Legal Opinion to the effect that Applicant is aware that it has exclusive control of the domain name; or
(B) Obtaining a confirmation from the Contract Signer or Certificate Approver verifying that Applicant is aware that it has exclusive control of the domain name.
(4) Mixed Character Set Domain Names EV Certificates MAY include domain names containing mixed character sets only in compliance with the rules set forth by the domain registrar. The CA MUST visually compare any domain names with mixed character sets with known high risk domains. If a similarity is found then the EV Certificate Request MUST be flagged as High Risk. The CA must perform reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that Applicant and the target in question are the same organization.

19. Verification of Name, Title, and Authority of Contract Signer and Certificate Approver

(a) Verification Requirements For both the Contract Signer and the Certificate Approver, the CA MUST verify the following:
(1) Name, Title and Agency The CA MUST verify the name and title of the Contract Signer and the Certificate Approver, as applicable. The CA MUST also verify that the Contract Signer and the Certificate Approver are agents representing Applicant.
(2) Authorization of Contract Signer The CA MUST verify, through a source other than the Contract Signer, that the Contract Signer is expressly authorized by Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of Applicant, including a contract that designates one or more Certificate Approvers on behalf of Applicant ("Signing Authority").
(3) Authorization of Certificate Approver The CA MUST verify, through a source other than the Certificate Approver, that the Certificate Approver is expressly authorized by Applicant to do the following, as of the date of the EV Certificate Request ("EV Authority"):
(a) Submit, and, if applicable, authorize a Certificate Requester to submit, the EV Certificate Request on behalf of Applicant; and
(b) Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from Applicant by the CA for issuance of the EV Certificate; and
(c) Approve EV Certificate Requests submitted by a Certificate Requester.

(b) Acceptable Methods of Verification – Name, Title and Agency Acceptable methods of verification of the name, title, and agency status of the Contract Signer and the Certificate Approver include:
(1) Name and Title The CA MAY verify the name and title of the Contract Signer and the Certificate Approver by any appropriate method designed to provide reasonable assurance that a person claiming to act in such a role is in fact the named person designated to act in such role**.**
(2) Agency The CA MAY verify agency of the Contract Signer and the Certificate Approver by:
(A) Contacting Applicant's Human Resources Department by phone or mail (at the phone number or address for Applicant's Place of Business, verified in accordance with these Guidelines) and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee; or
(B) Obtaining an Independent Confirmation From Applicant, or a Verified Legal Opinion (as described in Section 22 (a)), or a Verified Accountant Letter (as described in Section 22 (b)) verifying that the Contract Signer and/or the Certificate Approver, as applicable, is either an employee or has otherwise been appointed as an agent of Applicant.
The CA MAY also verify the agency of the Certificate Approver via a certification from the Contract Signer (including in a contract between the CA and Applicant signed by the Contract Signer), provided that the employment or agency status and Signing Authority of the Contract Signer has been verified.
(c) Acceptable Methods of Verification - Authorization Acceptable methods of verification of the Signing Authority of the Contract Signer, and the EV Authority of the Certificate Approver, as applicable, include:

(1) Legal Opinion The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by reliance on a Verified Legal Opinion (as described in Section 22 (a));
(2) Accountant Letter The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by reliance on a Verified Accountant Letter (as described in Section 22(b));
(3) Corporate Resolution The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by reliance on a properly authenticated corporate resolution that confirms that the person has been granted such Signing Authority, provided that such resolution is (1)
certified by the appropriate corporate officer (e.g., secretary), and (2) the CA can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification.
(4) Independent Confirmation from Applicant The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by obtaining an Independent Confirmation from Applicant.
(5) Contract between CA and Applicant The EV Authority of the Certificate Approver MAY be verified by reliance on a contract between the CA and Applicant that designates the Certificate Approver with such EV Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified.
(6) Prior Equivalent Authority The signing authority of the Contract Signer, and/or the EV authority of the Certificate Approver, MAY be verified by relying on a demonstration of Prior Equivalent Authority.
(A) Prior Equivalent Authority of a Contract Signer MAY be relied upon for confirmation or verification of the signing authority of the Contract Signer when the Contract Signer has executed a binding contract between the CA and the Applicant with a legally valid and enforceable seal or handwritten signature and only when the contract was executed more than 90 days prior to the EV certificate application. The CA MUST record sufficient details of the previous agreement to correctly identify it and associate it with the EV application. Such details MAY include any of the following:
(1) Agreement title
(2) Date of Contract Signer's signature
(3) Contract reference number
(4) Filing location
(B) Prior Equivalent Authority of a Certificate Approver MAY be relied upon for confirmation or verification of the EV authority of the Certificate Approver when the Certificate Approver has performed one or more of the following:
(1) Under contract to the CA, has served (or is serving) as an Enterprise RA for the Applicant
(2) Has participated in the approval of one or more EV certificates issued by the CA, which are currently in use on public servers operated by the Applicant. In this case the CA MUST have contacted the Certificate Approver by phone at a previously validated phone number or have accepted a signed and notarized letter approving the certificate request.
(d) Pre-Authorized Certificate Approver Where the CA and Applicant contemplate the submission of multiple future EV Certificate Requests, then, after the CA:
(1) Has verified the name and title of the Contract Signer and that he/she is an employee or agent of Applicant, and
(2) Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in the preceding Subsection (c).
The CA and Applicant MAY enter into a written agreement, signed by the Contract Signer on behalf of Applicant, whereby, for a specified term, Applicant expressly authorizes one or more Certificate Approver(s) designated in such agreement to exercise EV Authority with respect to each future EV Certificate Application submitted on behalf of Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s). Such an agreement MUST provide that Applicant shall be obligated under the Subscriber Agreement for all EV Certificates issued at the request of, or approved by, such Certificate Approver(s) until such EV Authority is revoked, and MUST include mutually agreed-upon provisions for (i) authenticating the Certificate Approver when EV Certificate Requests are approved, (ii) periodic reconfirmation of the EV Authority of the Certificate Approver, (iii) secure procedures by which Applicant can notify the CA that the EV Authority of any such Certificate Approver is revoked, and (iv) such other appropriate precautions as are reasonably necessary.

20. Verification of Signature on Subscriber Agreement and EV Certificate Requests

Both the Subscriber Agreement and each EV Certificate Request MUST be signed.
The Subscriber Agreement MUST be signed by an authorized Contract Signer. The EV Certificate Request MUST be signed by the Certificate Requester submitting the document. If the Certificate requester is not also an authorized Certificate Approver, then an authorized Certificate Approver MUST independently approve the EV Certificate Request. In all cases, the signature MUST be a legally valid and enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or EV Certificate Request), or a legally valid and enforceable

electronic signature (for an electronic Subscriber Agreement and/or EV Certificate Request), that binds Applicant to the terms of each respective document.

(a) Verification Requirements

(1) Signature The CA MUST authenticate the signature of the Contract Signer on the Subscriber Agreement and the signature of the Certificate Requester on each EV Certificate Request in a manner that makes it reasonably certain that the person named as the signer in the applicable document is, in fact, the
person who signed the document on behalf of Applicant.

(2) Approval Alternative In cases where an EV Certificate Request is signed and submitted by a Certificate Requester who does not also function as a Certificate Approver, approval and adoption of the EV Certificate Request by a Certificate Approver in accordance with the requirements of Section 21 can substitute for authentication of the signature of the Certificate Requester on such EV Certificate Request.

(b) Acceptable Methods of Signature Verification Acceptable methods of authenticating the signature of the Certificate Requester or Contract Signer include:

(1) A phone call to Applicant's or Agent's phone number, as verified in accordance with these Guidelines, asking to speak to the Certificate Requester or Contract Signer, as applicable, followed by a response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of Applicant.

(2) A letter mailed to Applicant's or Agent's address, as verified through independent means in accordance with these Guidelines, for the attention of the Certificate Requester or Contract Signer, as applicable, followed by a phone or mail response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of Applicant.

(3) Use of a signature process that establishes the name and title of the signer in a secure manner, such as through use of an appropriately secure login process that identifies the signer before signing, or through use of a digital signature made with reference to an appropriately verified certificate.

(4) Notarization by a notary, provided that the CA independently verifies that such notary is a legally qualified notary in the jurisdiction of the Certificate Requester or Contract Signer;

21. Verification of Approval of EV Certificate Request

(a) Verification Requirements In cases where an EV Certificate Request is submitted by a Certificate Requester, before the CA MAY issue the requested EV Certificate, the CA MUST verify that an authorized Certificate Approver reviewed and approved the EV Certificate Request.

(b) Acceptable Methods of Verification Acceptable methods of verifying the Certificate Approver's approval of an EV Certificate Request include:

(1) Contacting the Certificate Approver by phone or mail at a verified phone number or address for Applicant and obtaining oral or written confirmation that the Certificate Approver has reviewed and approved the EV Certificate Request;

(2) Notifying the Certificate Approver that one or more new EV Certificate Requests are available for review and approval at a designated access controlled and secure website, followed by a login by, and an indication of approval from, the Certificate Approver in the manner required by the website; or

(3) Verifying the signature of the Certificate Requester on the EV Certificate Request in accordance with Section 20 of these Guidelines.

22. Verification of Certain Information Sources

(a) Verified Legal Opinion

(1) Verification Requirements Before relying on any legal opinion submitted to the CA, the CA MUST verify that such legal opinion meets the following requirements ("Verified Legal Opinion"):

(A) Status of Author The CA MUST verify that the legal opinion is authored by an independent legal practitioner retained by and representing Applicant (or an in-house legal practitioner employed by Applicant) (Legal Practitioner) who is either:

(i) A lawyer (or solicitor, barrister, advocate, or equivalent) licensed to practice law in the country of Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where Applicant maintains an office or physical facility; or

(ii) A notary that is a member of the International Union of Latin Notaries, and is licensed to practice in the country of Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where Applicant maintains an office or physical facility (and that such jurisdiction recognizes the role of the Latin Notary).

(B) Basis of Opinion The CA MUST verify that the Legal Practitioner is acting on behalf of Applicant and that the conclusions of the Verified Legal Opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the Legal Practitioner's professional judgment and expertise.

(C) Authenticity The CA MUST confirm the authenticity of the Verified Legal Opinion.

(2) Acceptable Methods of Verification Acceptable methods of establishing the foregoing requirements for a Verified Legal Opinion are:
(A) Status of Author The CA MUST verify the professional status of the author of the legal opinion by directly contacting the authority responsible for registering or licensing such Legal Practitioner(s) in the applicable jurisdiction.
(B) Basis of Opinion The text of the legal opinion MUST make it clear that the Legal Practitioner is acting on behalf of Applicant and that the conclusions of the legal opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The legal opinion MAY also include disclaimers and other limitations customary in the Legal Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Legal Practitioner, should the legal opinion prove to be erroneous. An acceptable form of legal opinion is attached as Appendix D.
(C) Authenticity To confirm the authenticity of the legal opinion, the CA MUST make a telephone call or send a copy of the legal opinion back to the Legal Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Legal Practitioner listed with the authority responsible for registering or licensing such Legal Practitioner, and obtain confirmation from the Legal Practitioner or the Legal Practitioner's assistant that the legal opinion is authentic. If a phone number is not available from the licensing authority, the CA MAY use the number listed for the Legal Practitioner in records provided by the applicable phone company, a QGIS, or a QIIS.
In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by the CA in Section 22(a)(2)(A), no further verification of authenticity is required.

(b) Verified Accountant Letter

(1) Verification Requirements Before relying on any accountant letter submitted to the CA, the CA MUST verify that such accountant letter meets the following requirements ("Verified Accountant Letter"):
(A) Status of Author The CA MUST verify that the accountant letter is authored by an independent professional accountant retained by and representing Applicant (or an in-house professional accountant employed by Applicant) (Accounting Practitioner) who is a certified public accountant, chartered accountant, or equivalent licensed by a full member of the International Federation of Accountants (IFAC) to practice accounting in the country of Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where Applicant maintains an office or physical facility;
(B) Basis of Opinion The CA MUST verify that the Accounting Practitioner is acting on behalf of Applicant and that the conclusions of the Verified Accountant Letter are based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the Accounting Practitioner's professional judgment and expertise.
(C) Authenticity The CA MUST confirm the authenticity of the Verified Accountant Letter. (2) Acceptable Methods of Verification Acceptable methods of establishing the foregoing requirements for a Verified Accountant Letter are:
(A) Status of Author The CA MUST verify the professional status of the author of the accountant letter by directly contacting the authority responsible for registering or licensing such Accounting Practitioners in the applicable jurisdiction.
(B) Basis of Opinion The text of the accountant letter MUST make clear that the Accounting Practitioner is acting on behalf of Applicant and that the information in the accountant letter is based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The accountant letter MAY also include disclaimers and other limitations customary in the Accounting Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Accounting Practitioner, should the accountant letter prove to be erroneous. Acceptable forms of accountant letter are attached as Appendix E.
(C) Authenticity To confirm the authenticity of the accountant's opinion, the CA MUST make a telephone call or send a copy of the accountant letter back to the Accounting Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Accounting Practitioner listed with the authority responsible for registering or licensing such Accounting Practitioners and obtain confirmation from the Accounting Practitioner or the Accounting Practitioner's assistant that the accountant letter is authentic. If a phone number is not available from the licensing authority, the CA MAY use the number listed for the Accountant in records provided by the applicable phone company, a QGIS, or a QIIS.
In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by the CA in Section 22(b)(2)(A), no further verification of authenticity is required.

(c) Face-to-face Validation

(1) Verification Requirements Before relying on any face-to-face vetting documents submitted to the CA, the CA MUST verify that the Third-Party Validator meets the following requirements:

(A) Qualification of Third-Party Validator The CA MUST independently verify that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in Applicant's jurisdiction), Lawyer, or Accountant in the jurisdiction of the individual's residency;
(B) Document chain of custody The CA MUST verify that the Third-Party Validator viewed the Vetting Documents in a face-to-face meeting with the individual being validated
(C) Verification of Attestation If the Third-Party Validator is not a Latin Notary, then the CA MUST confirm the authenticity of the attestation and vetting documents.
(2) Acceptable Methods of Verification Acceptable methods of establishing the foregoing requirements for vetting documents are:
(A) Qualification of Third-Party Validator The CA MUST verify the professional status of the Third-Party Validator by directly contacting the authority responsible for registering or licensing such Third-Party Validators in the applicable jurisdiction.
(B) Document Chain of Custody The Third-Party Validator MUST submit a statement to the CA which attests that they obtained the Vetting Documents submitted to the CA for the individual during a face-to-face meeting with the individual.
(C) Verification of Attestation If the Third-Party Validator is not a Latin Notary, then the CA MUST confirm the authenticity of the vetting documents received from the Third-Party Validator. The CA MUST make a telephone call to the Third-Party Validator and obtain confirmation from them or their assistant that they performed the face-to-face validation. The CA MAY rely upon self-reported information obtained from the Third-Party Validator for the sole purpose of performing this verification process. In circumstances where the attestation is digitally signed, in a manner that confirms the authenticity of the documents,and the identity of the signer as verified by the CA in Section 22(c)(2)(A), no further verification of authenticity is required.
(d) Independent Confirmation From Applicant An "Independent Confirmation From Applicant" is a confirmation of a particular fact (e.g., knowledge of its exclusive control of a domain name, confirmation of the employee or agency status of a Contract Signer or Certificate Approver, confirmation of the EV
Authority of a Certificate Approver, etc.) that is:
(i) Received by the CA from a person employed by Applicant (other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact ("Confirming Person"), and who represents that he/she has confirmed such fact;
(ii) Received by the CA in a manner that authenticates and verifies the source of the confirmation; and
(iii)Binding on Applicant. An Independent Confirmation from Applicant MAY be obtained via the following procedure:
(1) Confirmation Request The CA MUST initiate an appropriate out-of-band communication requesting verification or confirmation of the particular fact at issue ("Confirmation Request") as follows:
(A) Addressee The Confirmation Request MUST be directed to:
(i) A position within Applicant's organization that qualifies as a Confirming Person (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) and is identified by name and title in a current Qualified Government Information Source (e.g., an SEC filing), a Qualified Independent Information Source, a Qualified Government Tax Information Source, a Verified Legal Opinion, a Verified Accountant Letter, or by contacting Applicant's Human Resources Department by phone or mail (at the phone number or address for Applicant's Place of Business, verified in accordance with these Guidelines); or
(ii) Applicant's Registered Agent or Registered Office in the Jurisdiction of Incorporation as listed in the official records of the Incorporating Agency, with instructions that it be forwarded to an appropriate Confirming Person; or
(iii)A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting Applicant's Human Resources Department by phone or mail (at the phone number or address for Applicant's Place of Business, verified in accordance with these Guidelines).
(B) Means of Communication The Confirmation Request MUST be directed to the Confirming Person in a manner reasonably likely to reach such person. The following options are acceptable:
(i) By paper mail addressed to the Confirming Person at:
(a) The address of Applicant's Place of Business as verified by the CA in accordance with these Guidelines; or
(b) The business address for such Confirming Person specified in a current Qualified Government Information Source (e.g., an SEC filing), a Qualified Independent Information Source, a Qualified Government Tax Information Source, a Verified Legal Opinion, or a Verified Accountant Letter; or
(c) The address of Applicant's Registered Agent or Registered Office listed in the official records of the Jurisdiction of Incorporation; or
(ii) By e-mail addressed to the Confirming Person at the business e-mail address for such person listed in a current Qualified Government Information Source, a Qualified Government Tax Information Source, a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant Letter; or

(iii)By telephone call to the Confirming Person, where such person is contacted by calling the main phone number of Applicant's Place of Business (verified in accordance with these Guidelines) and asking to speak to such person, and a person taking the call identifies himself as such person; or
(iv) By facsimile to the Confirming Person at the Place of Business. The facsimile number must be listed in a current Qualified Government Information Source, a Qualified Independent Information Source, a Qualified Government Tax Information Source, a Verified Legal Opinion, or a Verified Accountant Letter. The cover page must be clearly addressed to the Confirming Person.
(2) Confirmation Response The CA MUST receive a response to the Confirmation Request from a Confirming Person that confirms the particular fact at issue. Such response MAY be provided to the CA by telephone, by email, or by paper mail, so long as the CA can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.
(e) Qualified Independent Information Sources (QIIS) A regularly-updated and current publicly available database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information. A commercial database is a QIIS if the following are true:
(1) data it contains that will be relied upon has been independently verified by other independent information sources;
(2) the database distinguishes between self-reported data and data reported by independent information sources;
(3) the database provider identifies how frequently they update the information in their database;
(4) changes in the data that will be relied upon will be reflected in the database in no more than 12 months; and
(5) the database provider uses authoritative sources independent of the subject, or multiple corroborated sources, to which the data pertains. Databases in which the CA or its owners or affiliated companies maintain a controlling interest, or in which any Registration Authorities (RAs) or subcontractors to whom the CA has outsourced any portion of the vetting process (or their owners or affiliated companies) maintain any ownership or beneficial interest do not qualify as a QIIS. The CA SHOULD check the accuracy of the database and ensure its data is acceptable.
(f) Qualified Government Information Source (QGIS) A regularly-updated and current publicly available database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided they are maintained by a Government Entity, the reporting of data is required by law and false or misleading reporting is punishable with criminal or civil penalties. Nothing in these Guidelines shall prohibit the use of third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity.
(g) Qualified Government Tax Information Source (QGTIS) A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities or Individuals (e.g. the I.R.S. in the United States).

23. Other Verification Requirements

(a) High Risk Status

(1) Verification Requirements The CA MUST seek to identify Applicants likely to be at a high risk of being targeted for fraudulent attacks ("High Risk Applicants"), and conduct such additional verification activity and take such additional precautions as are reasonably necessary to ensure that such Applicants are properly verified under these Guidelines.
(2) Acceptable Methods of Verification The CA MAY identify High Risk Applicants by checking appropriate lists of organization names that are most commonly targeted in phishing and other fraudulent schemes, and automatically flagging EV Certificate Requests from Applicants named on these lists for further scrutiny before issuance. Examples of such lists include:
(A) Lists of phishing targets published by the Anti-Phishing Work Group (APWG); and
(B) Internal databases maintained by the CA that include previously revoked EV Certificates and previously rejected EV Certificate Requests due to suspected phishing or other fraudulent usage.
The information SHOULD then be used to flag suspicious new EV Certificate Requests. If an Applicant is flagged as a High Risk Applicant, the CA MUST perform reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that Applicant and the target in question are the same organization.

(b) Denied Lists and Other Legal Black Lists

(1) Verification Requirements The CA MUST verify whether Applicant, the Contract Signer, the Certificate Approver, Applicant's Jurisdiction of Incorporation, Registration, or Place of Business:
(a) Is identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of the CA's jurisdiction(s) of operation; or
(b) Has its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of the CA's jurisdiction prohibit doing business.

The CA SHOULD NOT issue any EV Certificate to Applicant if either Applicant, the Contract Signer, or Certificate Approver or if Applicant's Jurisdiction of Incorporation or Registration or Place of Business is on any such list.
(2) Acceptable Methods of Verification
The CA MUST take reasonable steps to verify with the following lists and regulations:
If the CA has operations in the U.S., the CA MUST take reasonable steps to verify with the following US Government denied lists and regulations:
(A) BIS Denied Persons List - http://www.bis.doc.gov/dpl/thedeniallist.asp
(B) BIS Denied Entities List - http://www.bis.doc.gov/Entities/Default.htm
(C) US Treasury Department List of Specially Designated Nationals and Blocked Persons - http://www.treas.gov/ofac/t11sdn.pdf
(D) US Government export regulations
(3) If the CA has operations in any other country, the CA SHOULD take reasonable steps to verify with all equivalent denied lists and export regulations (if any) in such other country.

24. Final Cross-Correlation and Due Diligence

Except for EV Subscriber Certificates approved by an Enterprise RA:
(a) The results of the verification processes and procedures outlined in these Guidelines are intended to be viewed both individually and as a group. Thus, after all of the verification processes and procedures are completed, the CA MUST have a person who is not responsible for the collection of information review all of the information and documentation assembled in support of the EV Certificate application and look for discrepancies or other details requiring further explanation.
(b) The CA MUST obtain and document further explanation or clarification from Applicant, Certificate Approver, Certificate Requester, Qualified Independent Information Sources, and/or other sources of information, as necessary, to resolve the discrepancies or details requiring further explanation.
(c) The CA MUST refrain from issuing an EV Certificate until the entire corpus of information and documentation assembled in support of the EV Certificate is such that issuance of the EV Certificate will not communicate inaccurate factual information that the CA knows, or the exercise of due diligence should discover, from the assembled information and documentation. If satisfactory explanation and/or additional documentation are not received within a reasonable time, the CA SHOULD decline the EV Certificate Request and notify Applicant accordingly.
(d) In the case where some or all of the documentation used to support the application is in a language other than the CA's normal operating language, the CA or its Affiliate MUST perform the requirements of this Final Cross-Correlation and Due Diligence section using employees under its control and having appropriate training, experience, and judgment in confirming organizational identification and authorization and fulfilling all qualification requirements contained in Section 29 of these Guidelines. When employees under the control of the CA do not possess the language skills necessary to perform the Final Cross-Correlation and Due Diligence a CA MAY:
(i) Rely on language translations of the relevant portions of the documentation, provided that the translations are received from a Translator; or (ii) When the CA has utilized the services of a RA, the CA MAY rely on the language skills of the RA to perform the Final Cross-Correlation and Due Diligence, provided the RA complies with Sections 24 (a)(b) and (c) above.
Notwithstanding the foregoing, prior to issuing the EV Certificate, the CA MUST review the work completed by the RA and determine that all requirements have been met; or
(iii) When the CA has utilized the services of a RA, the CA MAY rely on the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with this Section 24 and is subjected to the Audit Requirements of Sections 35 (b) and (c).
Furthermore, in the case of Enterprise EV Certificates to be issued in compliance with the requirements of Section 30 of these Guidelines, the Enterprise RA MAY perform the requirements of this Final Cross-Correlation and Due Diligence section.

25. Certificate Renewal Verification Requirements

Before renewing an EV Certificate, the CA MUST perform all authentication and verification tasks required by these Guidelines to ensure that the renewal request is properly authorized by Applicant and that the information in the EV Certificate is still accurate and valid.