2.1 Enrollment identity validation

2.1.1 Person identity validation

Each person named in an application file, it makes the applicant's behalf or on behalf of his company, must provide proof of its existence. This evidence takes the form of a valid official identity document.

A list of documents accepted subject to the additional sheet:
[FC_AE_OPC_JUSTIFS]

2.1.2 Organization identity validation

In a license application, the organization must provide evidence of its existence, the proof of the identity of his legal representative and the chain of giving their power to agents to certification.

2.1.2.1 Existence of the organization

In principle, the organization must provide proof of his existence and his identification number (unique registration number and identified with a commercial register or any other official list and update.)
This evidence takes the form of a supporting document. In the most common case, this is a K-Bis issued by the registries of commercial courts of the company's headquarters, in the case of a company.

A list of documents accepted subject to the additional sheet:
[FC_AE_OPC_JUSTIFS]

2.1.3 Server identity

In this section there is two processes depending of the usage of the certificate.

2.1.3.1 Registering a FQDN

The certificate’s common name (CN) must be a FQDN. (Fully Qualified Domain Name). A FQDN starts with a hostname (www, ftp…) and ends with an extension (.com, .eu, .fr, .org etc.). This is the internet address to access to the server, with no directory or files (not a full URL)

ex. : www.certinomis.com , www.test-certinomis.com are FQDN.
On the other hand, www.certinomis.com/faq is not acceptable (directory).

The following chars are forbidden within a FQDN : slash(/), comma(,) spaces (and other like tab). Dash(-) and dot (.) are accepted.

The operator (RA) must verify:

- The link between the organization and the domain name to certify.
- If necessary, ask complements

The ownership of the domain name, on these internet web sites:

http://www.networksolutions.com/whois/index.jhtml. (domains .com, ..org, .net)
http://www.afnic.fr/outils/whois (domains .fr)
http://www.eurid.eu (domains .eu)
http://www.norid.no/domenenavnbaser/domreg.html (other countries)

If the identified organization is not the owner of the domain, the recorded owner of the domain must provide an authorization of usage of domain name to the identified organization.
The domain's contact information must be up-to-date. If not the domain owner must update them. When done, he must notify the operator for checking the domain name recording and then the operator can validate the certificate request.
In addition, if the request is done under the form of a request accompanied with a CSR, this one is checked by the back office tool in order to verify the proof of possession of the private key.

2.1.3.2 Registering a trademark

The operator (RA) must verify:

- The link between the organization and trademark to certify.
- If necessary, ask complements

To check the owner of a French or European trademark, the operator (RA) must connect to the INPI web site : http://www.inpi.fr/

If the subscriber is not owner of the trademark, the owner, must provide an authorization of use by the subscriber of this trademark.

2.1.3.3 SSL certificate

The oprator (RA) must verify:

- The link between the organization and the requested FQDN
- If necessary, ask complements

In order to verify the operator must phone to the technical contact to validate the FQDN, by following the complementary process describe in 3.4.4

2.1.3.4 Signing certificate

The certificate common name (CN) must contain the identity and the usage of the certificate. The identity must be:

- Either the registered organization name

- Or a trademark of the organization (a proof of this possession must be provided).

The usage of the certificate must be separated of the identity with a dash character.
Ex: Certinomis – Electronic Invoices

2.1.4 Authorization verification

2.1.4.1 Document giving evidence of legal representative's quality

Only the legal representative of an organization can request electronic certificate containing the name of this organization. This, it is needed a document giving evidence of the legal representative's quality.

A list of documents accepted subject to the additional sheet:
[FC_AE_OPC_JUSTIFS]

2.1.4.2 Mandate, internal power, chain of power

If the legal representative chooses to enroll a certificate agent or a certificate manager, a mandate or a proxy must be used. Mandate can be:

- Either fill the document "Certificate Agent enrollment" given by Certinomis is each request for organization certificate or server certificate, without any changes.
- Or provide an internal organization document giving power to the mandated person. The scope of this mandate must include at least the same scope as the one described in the Certinomis one.
  For a town council, for instance, this document can be a copy of the minutes / the debate leading to the election of the Mayor, the Chairman, etc.

[…]

3 Request forms

3.1 Enrollment forms

3.1.2 "1 star certificates"

[SERVER]
An authorization to issue a certificate that includes:
the name and identification number of the organization, the full name of the technical contact, the server name.

A proxy of the legal representative (present conditional)

This must be informed if the designated certificate agent is not the legal representative of the entity he represents. This form contains the name, business contact of the legal representative's name, identification number of the organization, and remembers: the full name and address of the representative professional certification.
This document states explicitly the role and powers of attorney submitted to management certification certificate requests on behalf of the organization.

This document is optional if the legal representative of the company is only mandatory for certification. May be replaced by any document or power of attorney within the organization to the extent the powers are set out at least equivalent to the powers set out in the Document record type.

A warrant, dated within 3 months, appointing the future server manager as eligible to be server manager for the computer server which the server certificate must be issued. This warrant must be signed by a legal representative of the entity or the certificate agent and co-signed for acceptance by the future server manager,

A request form that includes:

- The information contained in the CSR (Certificate Signing Request, or certificate signing request). The CSR is generated by the client on the server before being pasted on the forms certificate application online.

A customer agreement signed and dated or a reference to a contract with the customer agreement.

A customer's purchase order or an order of service partners (depending on the billing).

The file also includes documents requested to verify the information given on this application.

[…]

3.4 COMPLEMENTARY(ADDITIONAL) CHECKS

3.4.1 Signature verifications

[…]

3.4.2 Check of the coherence and the comprehensiveness

[…]

3.4.3 Holder and server manager email addresses

[…]

3.4.4 Phone verifications

The goal of telephone verification procedure is to check:

- The provided contact works in the corporation that did the request.
- He agrees the certificate request
- He confirms the FQDN value
- He is authorized to do a certificate request, to receive it and to install it.

This verification must be carried out by a strictly different person of the person that carried out the preceding verifications.

3.4.4.1 Phone verifications: reachable contact

The verification of the number of telephone can be done on the following official sites:

- www.verif.com
- www.pagesjaunes.com

Or by the telephone services (118 008, 118 712, 118 000, 118 218 etc.).

If the number of seized telephone is a number of cellular telephone: the technical contact must produce a right proof indicating the link between this number and the corporation (telephone bill with the name of the Organization for example).

At the time of the telephone call, the RA operator puts a number of questions to validate the certificate request:

- If you obtain all the responses to your questions, you can validate this step of verification and emit the certificate
- If certain information is lacking or erroneous, you must indicate to the customer the elements to provide in order to rectify his request.

There is a calling script in annex 2.2

Specific case (revocation request): A specific phone check is done by the RA operator in case of revocation request from FQDN administration contact.
In order not to revoke arbitrarily, the RA operator checks the validity of the revocation request by a phone call to the administrative contact of the domain.
If the contact confirms the revocation request and gives motivation for, then the RA operator revokes the certificate.

3.4.4.2 Phone Verifications : UNreachable contact

The phone verification may fail:

- the person is unreachable
- the person has neither vocal messaging system nor personal assistant to deliver a message
- the contacted person is not the one who made the certificate request

- the technical contact is not granted to ask for certificate

In all cases, if you have to let a message, in order to be phoned back, don't forget to:

- tell the goal of the phone call
- tell that it is "urgent" (without phone call verification, the SSL certificate e will not be issued)
- let your information contact and to precise the opening hours of Certinomis office.

The maximum phone try to reach the person to do the phone verifications is 3.
After 3 failed phone call, send an email. After 24H, the certificate e request is in stand-by (the certificate is not issued) until the person call back.

There is an email template in annex.

3.4.5 Order form

[…]