3.2 Enrollment identity validation

3.2.1 Proof of possession of the private key

When the CA does not generate the server keys, CA verifies that the subscriber owns the private key related to the one present in the future certificate. This verification can be done with a "certificate signing request" in PKCS10 format by challenging the proof of possession.

3.2.2 Organization identity validation

The Registration Authority verifies the organization identity, the legal representative identity and identity of all persons designated by the representative, directly or indirectly, to represent the organization to the CA or the RA. The legal representative and these persons are the certificate "agents".

In lack of designation, the legal representative is the unique certificate agent.

At the time of the registration, the organization must bring the proof of its existence, the proof of the identity of its legal representative as well as the mandate chain conferring the power to the certificate agents.

The CA or the RA archives all pertinent documents relating to this recording.

The CPS defines the documents to provide and the process used by the RA.

The RA verifies that the request contains the following documents:

- A written request of certificate, signed, and dated back to less than 3 months, by a legal representative of the entity or by the certificate agent
- A signed mandate, and dated back to less than 3 months, by a legal representative of the organization or by the certificate agent designating the future holder to which the certificate must be delivered. This mandate must be signed for acceptance by the future certificate holder
- A copy of the status of the organization, in course of validity, carrying signature of its representatives, or for an association a verbal process of the general assembly carrying the signature of its representatives,
- A document, valid at the recording, carrying the number SIREN of the organization (k-bis extract or a situation notice from the SIRENE register justifying the registration number) or, another valid piece testifying the unique identification of the company that will figure in the certificate or, for the administrations a valid document at the recording, carrying delegation of responsible authority of the administrative structure.

The RA preserves the documents received for the recording of the holder, examines the given pieces and documents with a reasonable care and verifies if they appear to be conformant and valid.

3.2.3 Issued identity validation

The certificate must always have the name of the organization and eventually all complementary information helping to easily identify the holder.

For all organization certificate requests, the document must be signed by the certificate agent, and the sent to Certinomis.

The CPS defines the documents to provide and the process used by the RA.

3.2.3.1 Holder enrollment process

The identification of the future holder (person) representing an entity requires, first, identification of the entity and, secondly, the identification of the individual.
The identification of the entity is performed under the terms of Article 3.2.2.

The RA verifies the photocopy of at least one piece of official identification of valid recipient containing a photograph and signature, preceded by the words "certified true copy of the original", dated within three (3) months from the date of filing of documents deemed to be the date in the postmark.

The RA maintains the documents received for registration of the beneficiary, examines the evidence and documents provided with reasonable care and checks whether or not present the appearance of compliance and validity.

3.2.3.1 Certificate agent enrollment process

The RA has to register the certificate agent in order to:

- Use this registration to identify the organization of the certificate request submitted by the certificate agent.
- Optionally issue a certificate used by the certificate agent in order to sign and submit certificate request in an electronic way

The identification of the future certificate agent representing an organization requires, in one hand, the identification of the organization, on the other hand, the identification of the person.

The organization identification is done as described in chapter 3.2.2

The RA verifies that the application contains the following parts:

- A warrant signed and dated within 3 months by a legal representative of the entity designating the certificate agent. This warrant must be signed by the certificate agent for acceptance
- A commitment signed and dated within 3 months of the certificate agent, with HQ, to perform properly and independently controls the records of applicants,
- A commitment signed and dated within 3 months of the certificate agent to report to the RA his departure from the organization,
- A formal identity document valid certificate agent with a photo ID (such as national identity card, passport or stay), which is presented to RA which retains a copy.

The RA verifies the photocopy of at least one official ID of the recipient being validity with his photo and signature, preceded by the words "certified copy true to the original "dated less than three (3) months from the date of filing of documents deemed to be the date in the postmark.

The RA maintains the documents received for registration of the beneficiary, and examines parts documents provided with reasonable care and checks whether or not present the appearance of compliance and validity.

<u>3.2.3.3 Device enrollment process</u>

The identification of the future device (or application) representing a organization needs, on one hand, the identification of this entity and, on the other hand, the identification of the physical person in charge of the device and at last the identity of the device.

The identification of the entity and person in charge of the device is realized following the disposals of the item 3.2.3.1 and if the entity designates a certificate agent, following disposals of the item 3.2.3.2.

RA verifies that the requester is authorized by his organization to receive certificates for the device or the application. The person or the organization that presents a request must establish the proof of his right of usage on the device or the application that will have the requested certificate. In particular in the case of a web server, the person will have to establish the proof that the domain name belongs to him.

RA verifies that the request contains the following documents:

- A written request of certificate, dated back to less than 3 months, signed by a legal representative of the entity or by the certificate agent, containing the server FQDN.
- A signed mandate, and dated back to less than 3 months, by a legal representative of the organization or by the certificate agent designating the

future holder to which the certificate must be delivered. This mandate must be signed for acceptance by the future certificate holder.
- A proof of possession by the entity of the domain name corresponding to the FQDN of the server.

The RA preserves the documents received for the recording of the holder, examines the given pieces and documents with a reasonable care and verifies if they appear to be conformant and valid.

3.2.3.4 Enrollment of a new certificate manager for an existing certificate

In case of a change of the “server certificate manager” during the validity of the server certificate, the new certificate manager must be registered as a replacement of the previous one.

The identification of the future certificate manager representing an organization requires, in one hand, the verification of the authorization to represents the organization, on the other hand, the verification of the authorization to manage server certificates for this organization.

The RA verifies that the application contains the following parts:

- A warrant signed and dated within 3 months by a certificate agent of the entity designating the certificate manager. This warrant must be signed by the certificate manager for acceptance
- A copy of the status of the organization, in course of validity, carrying signature of its representatives, or for an association a verbal process of the general assembly carrying the signature of its representatives,
- A formal identity document valid certificate manager with a photo ID (such as national identity card, passport or stay), which is presented to RA which retains a copy.

The RA verifies the photocopy of at least one official ID of the recipient being validity with his photo and signature, preceded by the words "certified copy true to the original "dated less than three (3) months from the date of filing of documents deemed to be the date in the postmark.

The RA maintains the documents received for registration of the certificate manager, and examines parts documents provided with reasonable care and checks whether or not present the appearance of compliance and validity.

3.2.4 Unverified information

Certificates issued by this CP doesn’t content any unverified information.

3.2.5 Verification of the authority of the subscriber

This step is done during the validation of the person identity (directly by the RA or by the certificate agent).

3.2.6 Interoperability criteria

No interoperability with other CA is planned.