**3.2.2** Identity authentication of an organization

This section contains requirements for checking the identity of an organization.

3.2.2.1 Certification Entities linked to CATCert managed by third party

The Root Certification Entity has to authenticate, previously to issue and deliver any certificate of Certification Entity linked to CATCert, the Certification Entity identity and all the required data established on the corresponding section.

In order to fulfill this, the Certification Entity can use the next methods:

1. Getting the information about the organization from an external supplier of services.
2. Checking the presented documentation by the applicant. In this case it is required the physical presence of the person in charge of the future Certification Entity.

3.2.2.2 Registration Entities

The Certification Entity has to authenticate, previously to issue and deliver any operator’s certificate, for any of the Registration Entity members, the Registration Entity identity and the operator identity, as established on the corresponding section for organization certificates.

In order to fulfill this, the Certification Entity can use the next methods:

1. Getting the information about the organization from an external supplier of services.
2. Checking the presented documentation by the applicant. In this case it is required the physical presence of the person in charge of the future Registration Entity.

3.2.2.3 Certificate subscribers

3.2.2.3.1 Requirements for class 1 certificates

It is not required to carry out an authentication procedure of the titular organization of the certificate for class 1 certificates, because these are corporative certificates where the subscriber organization of the certificate is the same than the Registration Entity.

3.2.2.3.2 Requirements for class 2 certificates

The Certification Entity has to authenticate, previously to issue and deliver any organization certificate of class 2, the subscriber identity and all the required data established on the corresponding section for organization certificates.

The Certification Entity can use the Registration Entities for fulfill this task.

In order to fulfill this, the Certification Entity or the Registration Entity can use the next methods:

1. Getting the information about the organization from an external supplier of services. The Certification Entity previously will have to approve the external supplier.
2. Checking the presented documentation by the applicant about:
	1. Organization complete legal name
	2. Organization legal status
	3. Identification fiscal number
	4. Data of registry identification

Additionally to the required checking of the organization in charge of the secure server, it will be checked:

1. The existence of the server
2. The legal ownership of the domain
3. The organization authorization of issuing the server certificate.

**3.2.3** Identity authentication of a physical person

This section contains requirements for checking the identity of a physical person identified in a certificate.

3.2.3.1 Identification elements required

The Certification Entity will establish the amount ant types of necessary documents to prove the key owner identity, being able to use the following:

1. National Identity Document (DNI) or, Foreigner Identity Number (NIE) or, in an equivalent way, the renewal receipt more another identity document with photography.
2. Passport
3. Any other document accepted by the Spanish law, whenever it contains at least the following information:
	1. Name and Surnames
	2. Birth data and place
	3. Identity number legally recognized
	4. Other personal attributes that have to figure in the certificate

3.2.3.2 Validation of the identification elements

3.2.3.2.1 Requirements for Class 1 certificates

The identification information of key owners of class 1 certificates will be validated comparing the request with the internal registry of the Registration Entity, it has to warrantee the correctness of the information to certify. A human resources corporative supplier can take care of this task.

3.2.3.2.2 Requirements for Class 2 certificates

The identification information of individual certificates of subscribers, as well as of key owners of organization certificates, is carried out contrasting the requested information with the delivered documentation, electronically or in physical support.

3.2.3.3 Need of physical presence

The identification of a physical personal who has to obtain a recognized certificate can be done:

* Through his physical presence in front of the person in charge to verify his identity.
* Through the procedure established by de administrative law, when the physical presence is done in front of Public Administrations.

3.2.3.1 Requirements for CPSR and CESR (physical person and corporate body)

Previously to issue and deliver any CPSR or CESR certificate, the Certification Entity will have to carry out the subscriber identity of individual certificates or the key owner through the physical presence of him (directly or indirectly).

Meanwhile this stage it will be validated the person identity.

3.2.3.4 Link between the physical person and the organization

3.2.3.4.1 Requirements for Class 1 certificates

Since the certificates are corporative, where the Registration entity and the Subscriber Entity are the same, it is not necessary to get any specific documental accreditation about the link between the key owner and the Registry Entity, it will be use the internal registries of the institution.

3.2.3.4.2 Requirements for Class 2 certificates

When organization certificates are issued, the Certification Entity has to get a documental accreditation of the link between the physical person and the organization through any media admitted by the Spanish law.

The Certification Entity can use the Registration Entities for doing this task.