

Translation of section 3.1.8 of the updated CPS

http://www.camerfirma.com/mod_web/usuarios/politicas/CPS_V_3_2_1.pdf

Which is available from Camerfirma's Policy Repository: <http://policy.camerfirma.com/>

3.1.8 Authentication of the identity of an individual, organization, and their relationship.

The verification of the identity certificate does not differentiate between different hierarchies, but that is associated with the type of certificate issued.

To make a correct identification of the subscriber's identity, AC Camerfirma through the RA requires:

Certificates Recognized:

- Identification of Applicant:

The physical Impartiality of the Applicant, or representative of the applicant if this is a legal entity and the presentation of his paper National identity card, residence card or passport.

- Identification of the entity:

It requires the identification of the entity, for which the RA require relevant documentation according to the type of entity. This information varies depending on the type of entity and is included in the RA Manuals and operating in Camerfirma Web.

- Identification of representation:

For certificates of empowerment and representation requires documentation on the ability of representation of Signer / Subscriber regarding the entity, by delivery of notarial deeds demonstrate their performance.

There will be a certificate issued by the commercial register with less than 10 days old. The RA may also have electronic means for the online consultation of the state representation of the applicant.

Certificates of seizing the different powers are described in a table of entries, which are incorporated in the certificate of two ways: one placed in the Title field (TITLE) specify the details of representation, and two by a field link STATEMENT USER (USER NOTICE) to scripts scanned and signed by the RA operator.

To link certificates must be presented in a authorization signed by a representative of the company.

In the Certificates of legal person, in which the Signer / Subscriber and Applicant are different, it must be demonstrated documentary evidence that the Applicant has sufficient powers to perform the license application on behalf of the signer / subscriber through the presentation of a certificate of public records not exceeding 10 days or through online consultation launched by the RA itself data from public records.

In public employment certificates are not required documentation proving the existence of government, agency or public entity, since that identity is part of the field Corporate General Administration of the State or other of the AAPP State. It requires documentation of identity of the person who acts as responsible, on behalf of the Public Administration, or body public entity. Applicant / person responsible will be identified before the RA with your ID and a document certifying their membership as Public Administration employee, agency or body under public stating also the NIF of it.

Technical Certificates:

For secure server certificates OV (Organization Validation) the following is checked:

1. The existence of the entity through access to public records

(www.registradores.org; www.rmc.es) Camerdata (www.camerdata.es) or databases of the tax office (www.aeat.es).

2. The existence of the domain and the right to use it by the Subscriber is checked by accessing databases of Internet domains:

- <http://reports.internic.net>
- <http://www.networksolutions.com>
- <http://en.gandi.net>
- <http://www.interdomain.es>
- <https://www.nic.es/> (. S)
- <http://www.eurid.eu/> (. Eu)
- <http://www.nic.coop/whoissearch.aspx> (. Coop)
- <http://www.nominalia.com/>
- <http://www.arsys.es/>

3. The control of the domain by the subscriber, checking that data received by consulting the databases of Internet domains are clearly consistent with the data presented in the entity application.

These certificates are delivered via email to the administrative and technical contacts that appear in the domain databases.

In the electronic seal certificates are supported documentary business by querying the existence of the company / entity, either in the bases AEAT data of Camerdata or public records, such as in the issuance of secure server certificates OV previously seen. The email Applicant must come from an email address whose domain is associated with the company or organization that has made the request.

The certificate will be delivered in this e-mail. The activation code If delivered a PKCS12 format file by phone. The phone will be located by accessing the telephone consultation service [https: // www.paginasamarillas.es](https://www.paginasamarillas.es) or by calling location services phones. This information will be reflected in the record of issuance of certificate.

In the field owner of the company stamp certificates can show: company name, the name of the application for which was generated certificate or an internal reference. Camerfirma not perform any verification on these data.

In the code-signing certificates, it's the same test that the issuance of the Certificate of electronic seal.

The encryption certificates will be issued on a telematics using a valid qualified certificate.

It is possible under this CPS establish encryption certificates emissions processes batch. In these cases, verification of identity can be performed in Non processes delivering a RA or Camerfirma, a document with the applicant's identity and its relationship to an entity. This process face is made only when the certificate allows the exclusive use of encryption.

Secure Server Certificates (EV) "extended validation" follow the guidelines of the "CA / Browser Forum for Issuance and Management Guidelines of extended validation certificates," and shall also follow the same procedures as for a secure server OV certificate, ie:

1. The standing physical Signer / Subscriber, or a representative of Applicant if it is a legal person and the presentation of an ID card.
2. Identification of the entity for which required documentation RA relevant depending on the type of entity.
3. Presentation of an authorization signed by a representative of the entity to act as the Applicant.

In addition, the RA shall ensure:

4. The existence of the entity:

- With access to public records (www.registradores.org; www.rmc.es) Camerdata (www.camerdata.es) or databases Tax Agency (www.aeat.es). If the operator RA need further information incorporated in the organization the certificate, you will have access to a database management business risk as e-Informa <http://www.einforma.com>. This database provides information from both commercial register companies and their representatives incorporating information from risk.
- A finding that the data or documents provided are not older than 1 year.
- Consultation of the minimum of legal existence of the organization of 1 year.
- You can not issue certificates to companies in countries eradicated where there is a government ban to do business.

5. The existence of the domain and the right to use thereof by the Subscriber checks by accessing databases of Internet domains:

- <http://reports.internic.net>
- <http://www.networksolutions.com>
- <http://en.gandi.net>
- <http://www.interdomain.es>
- [https: // www.nic.es/](https://www.nic.es/) (. S)
- <http://www.eurid.eu/> (. Eu)
- <http://www.nic.coop/whoissearch.aspx> (. Coop)

- <http://www.nominalia.com/>
- <http://www.arsys.es/>

6. The entity controls the Internet domain for which issued the certificate. This means that the entity described in the service of access to basic Internet domain data is clearly identified and consistent with entity represented by the applicant.

Guides issuing EV certificates require the differentiation of different organization (Private, Government, Business). In these cases, the applicant mark in the application document the type of entity to which it belongs. The registration authority shall verify its compliance and validate the certificate that incorporate such information as defined in emission Guides reference.

Each type of entity must submit appropriate documentation as to prove its legal existence, as indicated in the website Camerfirma.

Marked as EV certificates are checked monthly by an auditor which they will ensure the correct issue and the existence of documentation has provided the basis for their issuance.

In the electronic Site Certificates for public administration and e-Seal for automated performance will require the assistance to the applicant's physical. This must go, always Camerfirma instance, the corresponding RA where there will be checking the documentation of data contained in the application form.

See licenses to carry out the same electronic checks that the issuance of a secure server certificate already described EV above.

For the issuance of Certificates of electronic seal for action carry out the same automated checks for a Certificate of business electronic seal and above.