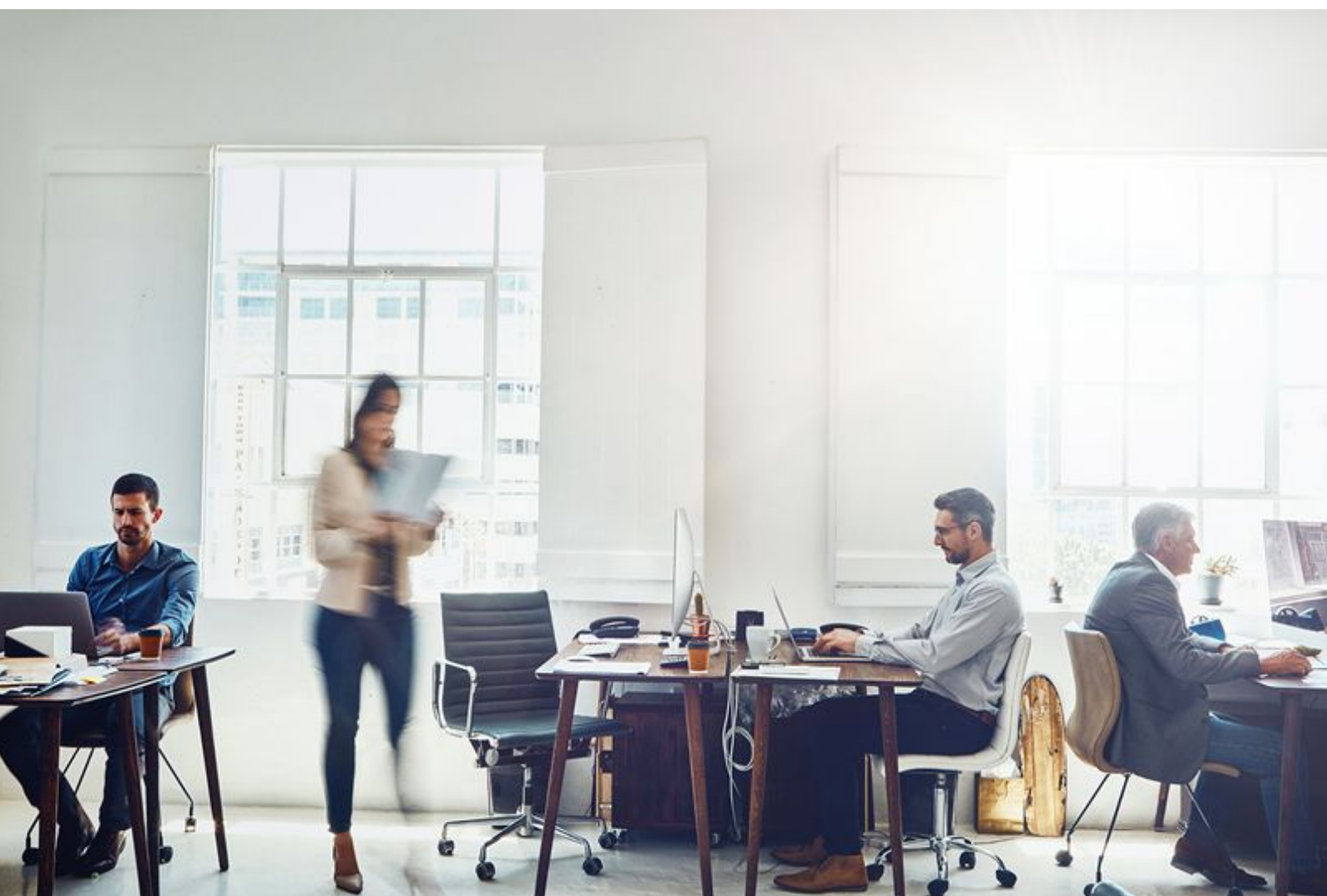


Certification Policy

Website Authentication Certificates

Version: 200205

Classification: Public



Version history

Version	Section and changes	Date of publication
181221	<p>Preparation of a new policy for website authentication certificates, integrated with previous electronic office certification and secure server SSL policies, which may be consulted at http://www.firmaprofesional.com/cps</p> <p>In addition to the integration of these policies, the following modifications have been made:</p> <ul style="list-style-type: none"> ● "2.2 Register Authority (RA)": corrections and clarifications. ● SerialNumber field has been marked as optional, on the basis that OrganizationIdentifier field contains the same information. ● Procedures for domain and organization verification have been updated. ● CAA treatment has been specified. ● Clarification of requirements for high-level Electronic Office certificate key generation. 	21/12/2018
190121	<ul style="list-style-type: none"> ● "4.1.2.3.3. Verification of the applicant operational existence": corrections and clarifications. ● "4.1.2.2.2. Domain name control verification" for OV and "4.1.2.3.4. Domain name control verification" for EV: homogenisation of sections. 	21/01/2019
190305	<ul style="list-style-type: none"> ● Reduced the validity period in Electronic Office Certificates, to 2 years maximum. 	05/03/2019
190507	<ul style="list-style-type: none"> ● "3.3. Multi-domain certificates": corrections and clarifications. ● Added check on the control of multi-domain SSL certificate domains. ● "3.1. Certificates validity period" (exclusively in English version): Corrections. Due to a translation error, the validity of an EV certificates is changed to a period of 2 years maximum. 	07/05/2019
190612	<ul style="list-style-type: none"> ● Added web authentication certificates for payment services 	12/06/2019

	based on the Directive (UE) 2015/2366 on payment services (PSD2).	
190806	<ul style="list-style-type: none"> ● Restructuring of historical version points. ● "4.1.2.2.2. <i>Domain name control verification</i>": indicated that the random code is sent to the domain contact. ● "4.2. <i>Certificate revocation and suspension</i>": included the suspension to explain that is not allowed by this policy. 	06/08/2019
200205	<ul style="list-style-type: none"> ● "4.1.1.4. <i>Application for PSD2 certificates</i>", reformulated the application procedure to homogenize it with that of EV. ● "4.1.2.1. <i>Acceptance of application for Electronic Office Certificates</i>", updated section eliminating parts that do not apply. ● Adaptation of the Policy to the requirements of version 2.7 of the Mozilla Root Store Policy. ● "4.1.2.2.1. <i>Verification of the applicant identity</i>". Elimination of references to obsolete sections 	05/02/2020

Index

1. Introduction	6
1.1. General Description	6
1.2. Identification of the Document	7
1.3. Definitions and acronyms	8
2. Participating Entities	9
2.1. Certification Authorities (CA)	9
2.2. Register Authority (RA)	9
2.3. Applicant	9
2.3.1. Intervening Roles	9
2.4. Subscriber	11
2.5. Third party trusting certificates	11
3. Certificates features	12
3.1. Certificates validity period	12
3.2. Extended Validation Certificates (EV)	12
3.3. Multi-domain certificates	12
3.4. Domain names	13
3.5. Certificate use cases	13
3.5.1. Appropriate use of certificates	13
3.5.2. Non-authorised uses of the certificates	13
3.5.3. Notification of non-authorised uses, complaints and suggestions	13
3.6. Rates	14
4. Operational procedures	15
4.1. Certificate issuance process	15
4.1.1. Application	15
4.1.1.1. Application for Electronic Office Certificates	15

4.1.1.2. Application for OV Certificates	15
4.1.1.3. Application for EV Certificates	16
4.1.1.4. Application for PSD2 certificates	17
4.1.2. Acceptance of the application	17
4.1.2.1. Acceptance of application for Electronic Office Certificates	17
4.1.2.2. Acceptance of application for OV Certificates	18
4.1.2.2.1. Verification of the applicant identity	18
4.1.2.2.2. Domain name control verification	20
4.1.2.3. Acceptance of application for EV Certificates	21
4.1.2.3.1. Verification of the applicant legal existence and identity	21
4.1.2.3.2. Verification of the geographic location where the applicant develops their business	23
4.1.2.3.3. Verification of the applicant operational existence	23
4.1.2.3.4. Domain name control verification	24
4.1.2.3.5. Verification of name, position and authority of the subscriber contract signatory and the certificate approver	24
4.1.2.3.6. Verification of the subscriber contract signature	24
4.1.2.3.7. Verification of the approval for an SSL EV Certificate issuance	25
4.1.2.4. Acceptance of the application for PSD2 certificates	25
4.1.3. Keys generation	25
4.1.4. Processing	25
4.1.5. Certificate issuance	26
4.1.6. Delivery	27
4.2. Certificate revocation and suspension	27
4.3. Certificate renewal	27
4.4. Procedure for problem notification by the subscriber	27
5. Certificate profiles	28

1. Introduction

1.1. General Description

Website authentication certificates are issued to organizations for use with their web servers, in order to guarantee to a person visiting a site that there is an authentic and legitimate entity supporting the existence of that resource. As established in Whereas 67 of Regulation EU 910/2014 of the European Parliament and of the Council of 23 July 2014 regarding electronic identification and trust services for electronic transactions in the internal market, these certificates contribute towards the creation of trust and faith in the performance of mercantile and administrative online operations, since users will trust a website that has been authenticated.

Currently, Firmaprofesional issues four types of Website Authentication Certificates.

- **Electronic Office Certificates**

- Issued to Public Administration Bodies, in accordance with provisions contained within article 38 of Law 40/2015 1st of October of Public Sector Legal Regime.
- Regarded as qualified certificates due to the fact that they comply with the established requirement of annex IV of Regulation EU 910/2014.
- Adhere to the definitions of high and middle assurance levels and certificate profiles established in point 8 of the document "Perfiles de Certificados electrónicos" from Subdirección General de Información, Documentación y Publicaciones of Ministerio de Hacienda y Administraciones Públicas.

- **Organization Validation SSL Certificates (OV):**

- Guarantee that a certain domain has been registered under the name of the organisation identified in the certificate, and that communication between the client's browser and website server is confidential via the use of SSL protocol.
- Adapt to CA/Browser Forum requirements established in document "*Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates*" version in force at the time of publication of this policy.

- **SSL Extended Validation Certificates (EV):**
 - Certificates issued to website servers in accordance with specific criteria of the organisation identity certification.
 - An SSL EV certificate allows browsers that connect to this service, to show an additional level of security.
 - Adapt to CA/Browser Forum requirements established in document “*Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates*” version in force at the time of publication of this policy.
 - These certificates are qualified due to the fact that they comply with requirements established in annex IV of Regulation EU 910/2014.

- **Web authentication certificates for PSD2**
 - Web authentication certificates for payment services.
 - Certificates issued only to payment service providers authorized by the Competent National Authority, in accordance with Directive (EU) 2015/2366 of the european parliament and of the council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Directive PSD2).

Further particular conditions referring to these certificates are explained within this document. This Certification Policy (hereafter “CP”) is subject to compliance with the Certification Practices Statement (hereafter “CPS”) of Firmaprofesional, incorporated herein by reference.

In case of any incompatibility between this document and the requirements published by the CA/Browser Forum, those requirements will have priority over this document.

1.2. Identification of the Document

Name:	Certification Policy for Website Authentication Certificates
Version:	200205
Description:	Certification Policy for Website Authentication Certificates
Date of issue:	05/02/2020

OIDs	1.3.6.1.4.1.13177.10.1.20.1 Electronic Office High-Level 1.3.6.1.4.1.13177.10.1.20.2 Electronic Office Medium-Level 1.3.6.1.4.1.13177.10.1.3.1 SSL OV 1.3.6.1.4.1.13177.10.1.3.10 SSL EV / Qualified / PSD2
Location:	http://www.firmaprofesional.com/cps

This Certification Policy gathers together the following Policies, which are revoked with the publication of this Policy:

- Certification Policy of Electronic Office Certificates (Version 171121). This Policy may be consulted at <https://www.firmaprofesional.com/cps>, in section "Previous Certification Policies and Practices".
- Certification Policy of Secure Web Servers (Version 180719). This Policy may be consulted at <https://www.firmaprofesional.com/cps>, in section "Previous Certification Policies and Practices".

1.3. Definitions and acronyms

Refer to the corresponding section in the Certification Practices Statement of Firmaprofesional (<http://www.firmaprofesional.com/cps>).

2. Participating Entities

2.1. Certification Authorities (CA)

From the date of publication of this Policy, all Website Authentication Certificates are issued by the Subordinate CA “AC Firmaprofesional - INFRAESTRUCTURA”.

2.2. Register Authority (RA)

Management of certificate applications will be performed by Firmaprofesional or by an authorised intermediary.

Management of issuances will be performed solely by Firmaprofesional.

2.3. Applicant

Physical or legal person that requests a certificate.

In general, applications for these certificates made under the name of an organisation will be performed by the person that appears as “Administrative Contact” in the official domain register.

In the case of Electronic Office certificates, these will be requested by administrators, legal representatives and Public Corporation volunteers, empowered to this effect.

In the case of web authentication certificates for PSD2, the applicant will be the legal representative of the payment service provider, which is recorded as such in the Bank of Spain (for Spanish providers) or Competent National Authority.

2.3.1. Intervening Roles

As stipulated within the current in force version of document “*Guidelines For The Issuance And Management Of Extended Validation Certificates*”, issued by CA/Browser Forum, certain roles are established to be executed by distinct persons related to an SSL EV Certificate applicant.

These roles are defined as the following:

1. Certificates petitioner:

An SSL EV Certificate application must be performed by a petitioner authorised by the applicant. The petitioner may be the applicant itself (in cases where this may be a physical person), an employee of the applicant, an agent authorised by the applicant to represent on behalf of, or an employee of a third party (for example, an ISP or a website hosting company). The petitioner will comply with the following function:

- a. Complete and send certification request.

2. Certificate approver:

An SSL EV certificate application must be approved by a person (or persons) authorised by the applicant to do so. An approver may be the applicant itself (in cases where this may be a physical person), an employee of the applicant, an agent authorised by the applicant to represent on behalf of. The approver may accomplish the following functions:

- a. Act as a petitioner, completing and sending certificate applications.
- b. Authorise other employees or third parties to act as petitioners.
- c. Approve certificate requests sent by petitioners.

3. The signatory of the subscriber contract:

In order to request an SSL EV certificate, a subscriber contract must be signed by an authorised signatory. A contract signatory will be a physical person that may be the applicant itself, an employee of the applicant, or an agent authorised by the applicant to represent on behalf of, and that has the authority to sign the subscriber contract on behalf of the applicant. The signatory accomplishes the following function:

- a. Sign the subscriber contract.

4. The applicant representative:

In cases where the CA and the subscriber are affiliated companies, the terms of use

regarding to SSL EV certificates application must be acknowledged and accepted by an applicant authorised representative. This will be a physical person that may be the applicant itself or an agent authorised by the applicant to represent on behalf of, and will have the authority to confirm acknowledgement and acceptance of the terms of use on behalf of the applicant.

2.4. Subscriber

The subscriber of the website authentication certificate will be the Organisation that appears as "Registrant" within the domain official register, or the Administration, Body or Public Law Entity identified in the certificate.

The subscriber of the web authentication certificate PSD2 will be the payment service provider duly authorized and registered in the Public Registry of the Competent National Authority. The subscriber will always be a legal entity comprised, at least, of one of the following categories:

- Account manager
- Payment initiation service provider
- Account information provider
- Issuer of card-based payment instruments

2.5. Third party trusting certificates

These certificates are recognised by Microsoft for all their applications, including Internet Explorer, by Mozilla Foundation, including Firefox, and by Apple, including Safari. Platform @firma, being the validation and electronic signature platform of the Spanish Government, accepts and validates Electronic Office certificates (medium and high-level) and SSL OV certificates.

Third parties trusting these certificates must acknowledge their usage limitations, both quantitative and qualitative, contained within the CPS and this CP.

3. Certificates features

3.1. Certificates validity period

Validity period will be indicated within the certificate, up until a maximum of 2 (two) years for all issued certificates that are described in this Policy.

3.2. Extended Validation Certificates (EV)

SSL EV Web Server Certificates allow browsers that connect to this service to demonstrate an additional level of security than SSL OV Web Server Certificates.

For this purpose, these certificates are issued in accordance with a specific and rigorous verification criteria towards the organisation identified in the certificate. These criteria require a thorough verification of the applicant organisation identity and of the person that submits the application. Almost all of these requirements are covered via electronic signature of an SSL EV Web Server Certificate application, performed with a Corporate Certificate for Legal Representative issued by Firmaprofesional.

3.3. Multi-domain certificates

Multi-domain Web Server Certificates allow the validation of distinct, same-domain URLs with the same certificate.

One way to achieve this is using "Wildcard Characters" for URLs as described within the standard RFC 2818 "HTTP Over TLS".

According to this standard, the character "asterisk" is allowed to be used as a wildcard in a URL. Thus, a certificate with URL "*.domain.com" will be able to be used for any subdomain, like "subdomain1.domain.com", "subdomain2.domain.com", "www.domain.com", etc...

The use of "Wildcards" in SSL Web Server Certificates is supported by all major internet browsers and becomes a very useful tool in cases where there are many subdomains of the same Internet domain and it is necessary to use a unique certificate for all of them.

It is solely permitted to issue wildcard certificates for SSL OV Web Server Certificates.

SSL EV Web Server Certificates and Electronic Office Certificates cannot be wildcard certificates. However, both the OV and EV SSL Web Server certificates and Electronic Office certificates may be multi-domain, protecting several host names through multiple domains with the certificate.

3.4. Domain names

Issuance of certificates for IP addresses or internal Domain Names (private or reserved) is not allowed.

The use of Internationalised domain names (IDN) is not allowed according to this CP. This measure prevents spoofing homograph attacks.

3.5. Certificate use cases

3.5.1. Appropriate use of certificates

Web Server Authentication Certificates may be used for authenticating the identity of a server or an Electronic Office via SSL (or TLS) protocol, and for establishing directly afterwards a secure transmission channel between the server or the Office and the service user.

3.5.2. Non-authorised uses of the certificates

Uses other than those established in this Policy and the Certification Practices Statement are not allowed.

Using this type of certificate for electronic signature of documents is not allowed. Firmaprofesional has other certificate policies appropriate for that purpose.

Uses other than those established in Law 40/2015 of 1st October, of Legal Regime of Public Sector for Electronic Office certificates, are not allowed.

3.5.3. Notification of non-authorised uses, complaints and suggestions

In cases of detection of a non-authorised use of the certificates or having any complaint or suggestion, these must be send to Firmaprofesional via e-mail to the address

soporte@firmaprofesional.com, indicating in the subject whether a “Non-Authorised Use”, a “Complaint” or a “Suggestion”, and providing in writing and with attached documents the relevant information for Firmaprofesional to be able to validate the veracity of the claim.

3.6. Rates

Firmaprofesional is able to establish appropriate rates to subscribers under its criteria, as well as payment methods for each case. For further details about rates and payment conditions of this type of certificates, the Commercial Department of Firmaprofesional should be consulted with.

4. Operational procedures

4.1. Certificate issuance process

Obtention of a certificate must be according to the following steps:

4.1.1. Application

Application process differs between Electronic Office Certificates, SSL OV Certificates and SSL EV Certificates. Details as follows:

4.1.1.1. Application for Electronic Office Certificates

Reference to the Official Journal where the order of that Electronic Office creation appears, must be presented. The order must contain:

- Identification of the Official Journal, article and date of publication
- Electronic Office name
- Electronic Office URL
- Electronic Office holder

Certificate application must be performed by a representative of the Electronic Office holder, duly accredited and authorised for this purpose.

4.1.1.2. Application for OV Certificates

In order to apply for a SSL OV Web Server Certificate, the organisation must be the owner of the domain.

The applicant may perform the application via the following electronic media:

- Firmaprofesional Website.
- E-mail.

- Completing and returning an application form provided by Firmaprofesional.

Firmaprofesional will receive the application and start the verification process.

4.1.1.3. Application for EV Certificates

Obtention of this certificate must follow the following steps:

1. Signature of the subscriber contract and the authorisation letter:

An applicant legal representative must sign a subscriber contract and an authorisation letter. The representative must be empowered to apply for this type of certificate on behalf of the organisation.

In addition, the representative will sign a letter authorising a person (or persons) to execute the role of certificate approver. By means of this role, authorised persons may apply and approve certificate issuance. This letter must include the signature of the authorised persons in addition to the signature of the legal representative. Once this step has been completed, certificates may be requested.

Signature of both documents may be performed in two ways.

- a. Handwritten. In this case, the applicant must send a signed and scanned copy of the contract via e-mail. Firmaprofesional will verify that the contract has been signed by the representative via phone call.
- b. Electronically with a qualified certificate of legal person. In this case, no further verification would be required.

2. Application of certificates:

Performed via a PDF form sent from the e-mail address of one of the certificate approvers. Requesting the issuance implies also approving the certificate issuance on the part of one of the persons referred to in section 2.3.1.

For the application process of Firmaprofesional SSL EV certificates it is necessary to use at least two of the persons mentioned in section 2.3.1.

4.1.1.4. Application for PSD2 certificates

Obtention of this certificate must follow the following steps:

The Payment Services Provider must present the certificate request together with the certificate of being a payment service provider authorized by the competent Authority, which must include the authorization number, the role of the payment service provider and the name of the Competent National Authority.

Qualified web authentication certificates from PSD2 are issued only to legal persons.

The applicant can make the signature of the documentation and the request by the same means allowed for EV certificates, stated in section "4.1.1.3. Application for EV Certificates", the authorization letter not being necessary.

4.1.2. Acceptance of the application

The acceptance process differs between Electronic Office certificates, SSL OV, SSL EV and PSD2. Details are as follows:

4.1.2.1. Acceptance of application for Electronic Office Certificates

These certificates are only issued by the RA of Firmaprofesional..

The Firmaprofesional RA Operator will verify the order of Electronic Office creation as well as the identity of the applicant and their capacity of representation on behalf of the holder.

Where high-level is being applied for, evidence must be provided to prove that the keys generation and custody have been performed in a cryptographic hardware device.

4.1.2.2. Acceptance of application for OV Certificates

Verification process is performed according to stipulations in the current in force version of the document “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”, issued by CA/Browser Forum.

4.1.2.2.1. Verification of the applicant identity

Certificate information will be verified as follows:

1. **In cases where the applicant is an organisation (legal person):** organisation existence, name, address and country are verified following these steps:
 - a. Consultation with official register depending on the type of the organisation. For example, for companies, the consultation will be with the trade register. In cases of public entities, the consultation will be with a public entities register. A signed document issued by an official register 825 days before the issuance of the certificate is also accepted.
 - b. Consultation with a third party database periodically updated and considered a reliable data source. Such a source is understood to be a database used for verifying information about organisations identity, recognised among commercial companies and public administrations as a reliable source and created by a third party different than the applicant. A document or report issued by a reliable source is also valid, like for example, Legal Entity Identifier (LEI).
 - c. A declaration written by a public server, a public notary or a legal firm.

If the applicant wants to incorporate the information of a **registered brand or commercial name** in the certificate, then it is necessary to verify that the applicant has the right to use the brand or the name via one of the following means:

- a. Certificate issued by a governmental entity or consultation with an official register, proving that the applicant has the right to use the brand or the name that will appear in the certificate. In Spain, for example, a search will be performed on the Spanish Patent and Trademark Office Website. It would also be valid if the applicant is able to provide a certificate of this entity.
- b. Consultation with a third party database periodically updated and considered a reliable data source. Such a data source is understood to be a database used for verifying that an organisation has the right to use a brand or a commercial name, and which is recognised among commercial companies and public administrations as a reliable source created by a third party different than the applicant.
A document or report issued by a reliable source will also be considered valid.
- c. A declaration written by a public servant, a public notary or a legal firm, together with documentation accrediting the applicant with having the right to use the brand or the commercial name.

2. **In cases where the applicant is a physical person:** their name, address and country are verified using one of the following means:

- a. DNI, Passport or driving license copy containing a photograph of the face of the applicant. Via this means the name and the address of the applicant will be verified.
- b. If the location requested to be included in the certificate is not the same as appearing in the submitted DNI, passport or driving license, the applicant may

provide an amenity bill (e.g. water or electricity) or a bank statement confirming the applicant is associated to the location requested to be included in the certificate.

4.1.2.2.2. Domain name control verification

Prior to the SSL Certificate issuance, Firmaprofesional will verify that the applicant has control over the domain; if the request is carried out for a multidomain SSL certificate, Firmaprofesional will verify that all the domains added to the SAN (Subject Alternative Name) belong to the same organization. The verification will be carried out using at least one of the following methods:

1. A unique and random code is sent to the domain contact via e-mail, fax, SMS or ordinary mail. Any person within the organisation may reply via any of these media, indicating the random code. The most common case being via e-mail reply.

In order to send the random code, Firmaprofesional will use the e-mail address, fax number, phone number or postal address that appears in the result of the search performed in the Whois service.
2. Phone call to the domain name administrative or technical contact identified via consultation with the corresponding Whois service. The fact that the applicant has requested a certificate for the domain name is confirmed in this phone call, which is recorded and stored by Firmaprofesional.
3. E-mail sent to one or more of the following addresses: "admin", "administrator", "webmaster", "hostmaster" o "postmaster", followed by the symbol "@" and the name of the domain. This e-mail includes a random and unique code. Any person from the applicant organisation replying this e-mail must indicate the random code.
4. The applicant makes a change in the domain DNS register for which requests an SSL certificate. Firmaprofesional indicates a random and unique code. The applicant

must add the random code in a field named CNAME, TXT or CAA in their DNS register.
 Once the change is made by the applicant, Firmaprofesional verifies it.

4.1.2.3. Acceptance of application for EV Certificates

Verification requirements for Firmaprofesional SSL EV Web Server Certificates issuance are as follows:

4.1.2.3.1. Verification of the applicant legal existence and identity

Type of entity	Aspects to verify	Verification methods - one of the following options	Evidence
Private organisation (non-governmental entities whose creation was via an incorporation act in a legal register)	<ul style="list-style-type: none"> - Legal existence - Name of the organisation - Register number or VAT - Official Register 	1) Online consultation with: <ul style="list-style-type: none"> - Trade Register. - National Chamber of Commerce. - Or Legal Entity Identifier (LEI). 2) Certificate or document issued two years before the SSL Certificate issuance, by the Trade Register or equivalent, LEI or Chamber Commerce two years before the SSL Certificate issuance	Copy of the consultation, certificate or document issued.
Public Organisation or Governmental Organisation	<ul style="list-style-type: none"> - Legal existence - Name of the organisation - Register number or VAT 	1) Consultation with the official register 2) Consultation with LEI. 3) Certificate or document issued two years before the SSL Certificate issuance, by the Trade Register or LEI.	Copy of the consultation, certificate or document issued.

<p>Business Entity / Commercial Entity (Any entity that is not a private organisation, public entity or non-commercial entity)</p>	<ul style="list-style-type: none"> - Legal existence - Name of the organisation - Register number or VAT 	<p>1) For Professional Associations: Creation bylaws, their publication in BOE and VAT card, or LEI.</p> <p>2) For others: Consultation with public official register or LEI.</p> <p>3) Certificate or document issued two years before the SSL Certificate issuance, by the Trade Register or LEI.</p>	<p>For Associations: - Bylaws copy -BOE publication copy - VAT copy - or LEI - Certificate or document issue copy.</p> <p>For others: - Consultation copy. -or LEI. - Certificate or document issued.</p>
	<ul style="list-style-type: none"> - Representative 	<p>Official document (record) of appointment, either of the General Meeting of the entity, of the public registry or power of attorney</p>	<p>Copy of the Official document (record) or power of attorney</p>
<p>Non-Commercial Entities (International Organisation)</p>	<ul style="list-style-type: none"> - Legal existence - Name of the organisation - Register number or VAT 	<p>1) Constitution document.</p> <p>2) LEI.</p>	<p>-Constitution copy. - or LEI.</p>
<p>Registered brands or commercial names (if an entity wants the SSL EV Certificate to include its commercial name or registered brand). Its use is limited to fields where this information may appear</p>	<ul style="list-style-type: none"> - The applicant has registered the commercial name or the brand.. - Registered brand or commercial name validity use. 	<p>1) Online Consultation with national official register.</p> <p>2) Online consultation with international official register.</p> <p>3) Certificate or document issued two years before the SSL Certificate issuance, by the Trade Register or LEI.</p>	<p>Copy of the consultation, certificate or document issued.</p>

4.1.2.3.2. Verification of the geographic location where the applicant develops their business

Type of entity	Aspects to verify	Verification methods - one of the following options	Evidence
For all types of organisations	- Geographic location where the applicant develops their business.	1) If the geographic location of the applicant appears in one of the methods mentioned in section "Verification of the applicant legal existence and identity", then no additional verifications are needed. 2) Consultation with a reliable database. For example Legal Entity Identifier (LEI). 3) Notarial deed that certifies the geographic location.	Evidences mentioned in section "Verification of the applicant legal existence and identity", reliable database consultation copy or notarial deed copy.

4.1.2.3.3. Verification of the applicant operational existence

Type of entity	Aspects to verify	Verification methods - one of the following options	Evidence
For all types of organisation	- Operational existence of the organisation	All methods described in sections "Verification of the applicant legal existence and identity" and "Verification of the geographic location where the applicant develops their business", verify that the organisation has an active status. If this was not possible, it would be necessary an online consultation with a reliable database like Legal Entity Identifier (LEI)	Evidences contained in section "Verification of the applicant legal existence and identity", copy of consultation with the reliable database.

4.1.2.3.4. Domain name control verification

For EV certificates, Firmaprofesional will follow the same method for domain name control verification than for OV certificates. For further information, section "4.1.2.2.2. Domain name control verification" of this document may be consulted.

4.1.2.3.5. Verification of name, position and authority of the subscriber contract signatory and the certificate approver

The applicant must sign a subscriber contract and send an scanned copy to Firmaprofesional. The contract establishes that the applicant may request SSL EV Certificates from Firmaprofesional for domains under their control and that they are empowered to use.

The contract must be signed by a person who acts as the subscriber contract signatory according to roles definition included in section 4.1.1.3.1 of this Policy.

Includes an affidavit, where is recognised that the signatory is authorised to act on behalf of the applicant for requesting an SSL EV Certificate to Firmaprofesional, and to use and secure the issued certificate. Thus, the empowerment of the subscriber contract signatory is verified.

The contract and affidavit shall be accompanied by an authorisation letter, whereby the applicant authorises other persons to execute the roles described in section 4.1.1.3.1 of this Policy. This letter must include the signatures of each authorised persons, aside from the signature of the subscriber contract signatory. Thus, the name, position, office and the approver authority are verified.

4.1.2.3.6. Verification of the subscriber contract signature

Firmaprofesional uses one of the following methods to verify the subscriber contract signature:

1. Via phone call to the applicant and questionnaire to the subscriber contract signatory. This call will be recorded and stored as evidence.

2. If the contract is signed with a legal representative certificate of the applicant organisation, it is stored as evidence and no additional verifications are needed.

4.1.2.3.7. Verification of the approval for an SSL EV Certificate issuance

In order to issue an SSL EV Certificate, the authorised certificate approver, via authorisation letter (containing their e-mail address) must send the certificate application from their e-mail. By this means, the approver would be already authorising the certificate issuance.

4.1.2.4. Acceptance of the application for PSD2 certificates

To verify the information of the certificate application, Firmaprofesional must validate this information comparing it against the Public Registry of the Competent National Authority (the public registry of the Bank of Spain or the public registry of the European Banking Authority-EBA, among others).

4.1.3. Keys generation

Signature keys will be generated within the applicant systems using their own compatible applications with the PKI standards. Generally, server applications that may be configured with SSL protocol, like IIS of Microsoft, include tools for generating keys and certificate requests.

Keys must be RSA with a minimum length of 2.048 bits.

4.1.4. Processing

In Electronic Office Certificate cases, the RA Operator will validate the veracity and accuracy of the applicant and electronic office data, as well as that the applicant has the private key associated to the public key included in the certificate application. The RA Operator will generate the application in a standard format and will send it to Firmaprofesional.

In order to process **SSL OV, SSL EV and PSD2 certificates**, the applicant will deliver to Firmaprofesional, directly or via authorised intermediary, a certificate application in PKCS#10 format.

Firmaprofesional will perform the technical validation of the PKCS#10 request and contained data.

4.1.5. Certificate issuance

Previous to Electronic Office Certificates issuance, the RA Operator will generate the certificate request in a standard format and will send it to Firmaprofesional.

Firmaprofesional will validate the integrity of the applications and that it has been generated by a RA Operator duly authorised. After this validation, the certificate will be issued.

In cases where Firmaprofesional receives a guarantee of the requirements compliance to consider that the certificate has High-level security according to Certificate Profiles document done by the Spain Government, the certificate will be issued with the corresponding OID.

Previous to SSL OV, SSL EV and PSD2 Certificates issuance, the existence of CAA register for every DNS name of extensions CN and subjectAltName of the certificate. In case that the certificate is issued, the validation will be performed before the CAA register TTL. Firmaprofesional processes tag "issue" and "issuewild". The CAA register that identifies those domains whose issuance is authorised by Firmaprofesional is "firmaprofesional.com".

If the application is electronically signed via a Firmaprofesional Corporate Certificate of Legal Representative, a SSL EV Web Server Certificate will be issued; in other cases, a SSL OV Web Server Certificate will be issued.

Additionally, the SSL EV Web Server Certificate issuance requires the approval of two persons: the RA Operator in charge of the application management, and the Administrator of the Technical Department in charge of the certificate issuance. The same requirement is needed for the issuance of a PSD2 Certificate.

4.1.6. Delivery

Firmaprofesional will deliver the certificate to the applicant allowing for secure download from the Internet.

Electronic Office Certificates must be formally accepted by the applicant, leaving documented evidence in the hands of the RA.

4.2. Certificate revocation and suspension

The suspension of any of the types of certificates contemplated in this policy is not allowed.

The revocation is performed as specified in the Certification Practice Statement (CPS).

4.3. Certificate renewal

Same steps than a new certificate issuance must be followed (4.1 Certificate Issuance Process).

4.4. Procedure for problem notification by the subscriber

If the subscriber of Website authentication certificates detects any problem with the certificate, they will be able to notify such via e-mail to soporte@firmaprofesional.com.

Any e-mail received in this address enters into the Customer Service System of Firmaprofesional.

In case of changes in relevant information on PSD2 of the payment service provider that may affect the validity of the certificate, the Bank of Spain or Competent National Authority will communicate it through the account soporte@firmaprofesional.com

5. Certificate profiles

In accordance to prescriptions contained in this Certification Policy, the following certificates are issued with their associated OID:

Type of Certificate	OID
Electronic Office High-Level	1.3.6.1.4.1.13177.10.1.20.1
Electronic Office Medium-Level	1.3.6.1.4.1.13177.10.1.20.2
SSL OV	1.3.6.1.4.1.13177.10.1.3.1
SSL EV / Qualified and PSD2	1.3.6.1.4.1.13177.10.1.3.10

Extensions used for every type of certificate issued under this policy, will be published in the document "Certificate Profiles" on the Firmaprofesional website (<http://www.firmaprofesional.com/cps>).