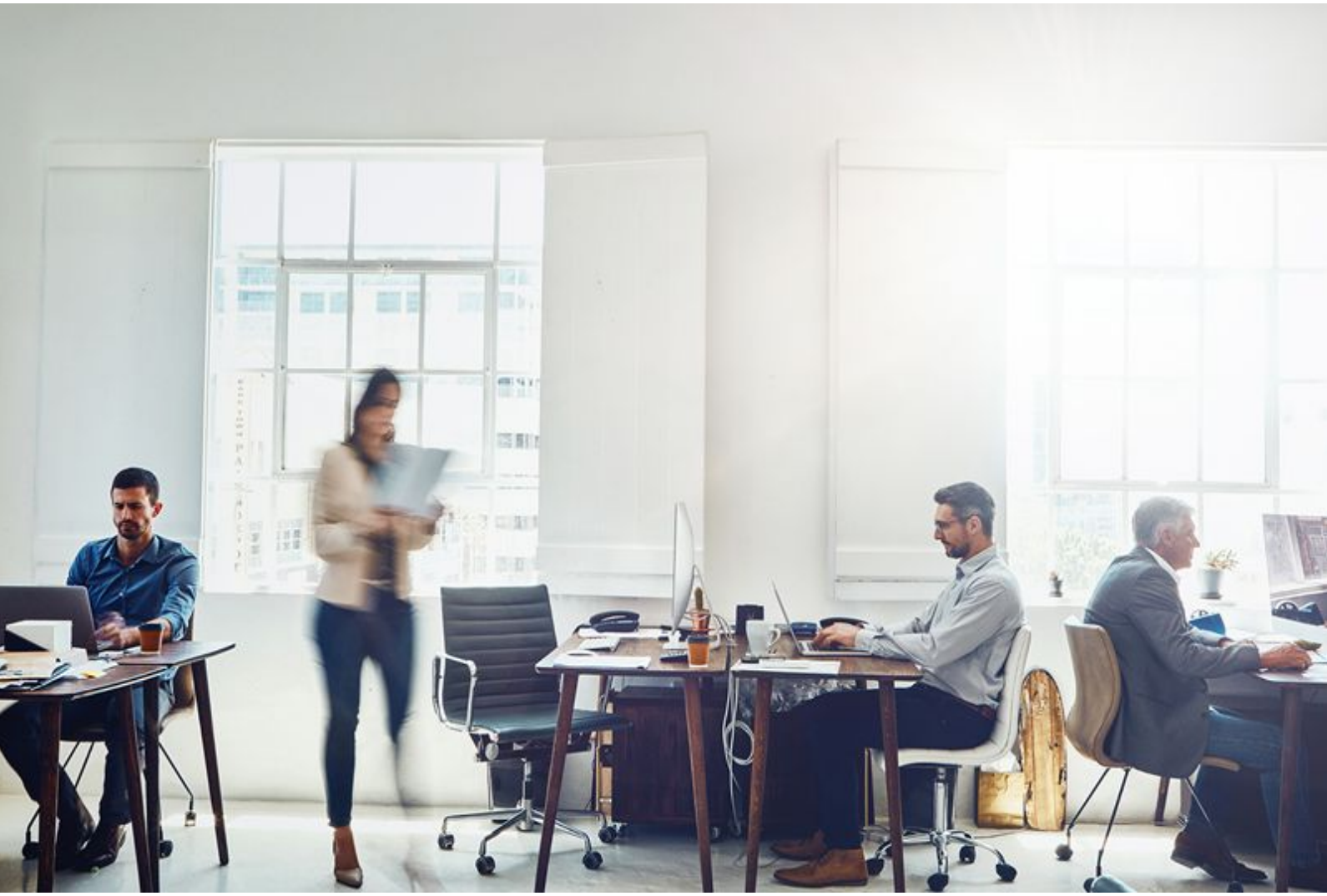
Certification Policy

Website Authentication Certificates

Version: 210217

Classification: Public



BARCELONA
EDIF. ESADECREAPOLIS
AV. TORRE BLANCA, 57 - LOCAL M2
08173 SANT CUGAT DEL VALLÈS
+34 934 774 245

MADRID
VELÁZQUEZ 59, 1º CTRO.-IZDA.
28001 MADRID
+34 915 762 181

WWW.FIRMAPROFESIONAL.COM

Version history

Version	Section and changes	Date of publication
181221	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 In addition to the integration of these policies, the following modifications have been made: • "*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	• "*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	• Reduced the validity period in Electronic Office Certificates, to 2 years maximum.	05/03/2019
190507	• "*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	• Added web authentication certificates for payment services	12/06/2019

	based on the Directive (UE) 2015/2366 on payment services (PSD2).	
190806	• Restructuring of historical version points. • "*4.1.2.2.2. Domain name control verification*": indicated that the random code is sent to the domain contact. • "*4.2. Certificate revocation and suspension*": included the suspension to explain that is not allowed by this policy.	06/08/2019
200205	• "*4.1.1.4. Application for PSD2 certificates*", reformulated the application procedure to homogenize it with that of EV. • "*4.1.2.1. Acceptance of application for Electronic Office Certificates*", 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. Verification of the applicant identity*". Elimination of references to obsolete sections	05/02/2020
200806	• Extension of the verification mechanisms of the legal existence and identity of the applicant in the section 4.1.2.3.1. Verification of the applicant legal existence and identity. • New section 4.1.2.1.1 Domain name control verification	06/08/2020
200901	• Reduced the maximum validity of the Certificates to 1 year.	01/09/2020
201001	• Added reference about verification sources registry table in section 3.2	01/10/2020
210217	• Adaptation to the new Law 6/2020, regulating certain aspects of electronic trust services. • Adaptation to RFC3647	17/02/2021

Index

1. Introduction

1.1. Summary

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:	210217
Description:	Certification Policy for Website Authentication Certificates
Date of issue:	17/02/2021

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. Participating Entities

1.3.1. Certification Authorities (CA)

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

1.3.2. Register Authority (RA)

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

Issuance management will be performed solely by Firmaprofesional.

1.3.3. 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

1.3.3.1. 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.

1.3.3.2. 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 petitionary:**

   An SSL EV Certificate application must be performed by a petitionary authorised by the applicant. The petitionary 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 of behalf of, or an employee of a third party (for example, an ISP or a website hosting company). The petitionary 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 petitionary, completing and sending certificate applications.
   b. Authorise other employees or third parties to act as petitionaries.
   c. Approve certificate requests sent by petitionaries.

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 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.

1.3.4. 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.

1.3.5 Other participants

No stipulation.

1.4 Use of the Certificates

1.4.1 Appropriate uses of certificates

Website Authentication Certificates can be used to authenticate the identity of a server or an Electronic Office using the SSL (or TLS) protocol and then establish a secure transmission channel between the server or the Office and the user of the service.

1.4.1.1. Certificates validity period

Validity period will be indicated within the certificate, up to a maximum of 1 (one) year for all issued certificates that are described in this Policy.

1.4.1.2. 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.

The list of Incorporating Agencies or Registry Agencies is published in the repository of the Firmaprofesional website (www.firmaprofesional.com), in the section "Verification Sources".

1.4.1.3. 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.

1.4.1.4. 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.

1.4.2. 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.

1.4.2.1. 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.

1.5 Policy Administration

As stated in the current Certification Practices Statement of Firmaprofesional.

1.5.1 Organization managing the document

As stated in the current Certification Practices Statement of Firmaprofesional.

1.5.2 Contact person

As stated in the current Certification Practices Statement of Firmaprofesional.

1.5.3 Person who determines the suitability of the CP for the policy

As stated in the current Certification Practices Statement of Firmaprofesional.

1.5.4 CP approval procedure

As stated in the current Certification Practices Statement of Firmaprofesional.

1.6 Definitions and acronyms

As stated in the Firmaprofesional Certification Practices Statement (http://www.firmaprofesional.com/cps).

2. Repositories and Publication of Information

2.1 Repositories

As stated in the current Certification Practices Statement of Firmaprofesional.

2.2 Publication of certification information

As stated in the current Certification Practices Statement of Firmaprofesional.

2.3 Time or frequency of publication

As stated in the current Certification Practices Statement of Firmaprofesional.

2.4 Access control to repositories

As stated in the current Certification Practices Statement of Firmaprofesional.

3. Identification and Authentication

3.1 Appoint

As stated in the current Certification Practices Statement of Firmaprofesional.

3.1.1 Types of names

As stated in the current Certification Practices Statement of Firmaprofesional.

3.1.2 Need for names to be meaningful

As stated in the current Certification Practices Statement of Firmaprofesional.

3.1.3 Anonymity or pseudonymity of subscribers

As stated in the current Certification Practices Statement of Firmaprofesional.

3.1.4 Rules for interpreting various forms of names

As stated in the current Certification Practices Statement of Firmaprofesional.

3.1.5 Uniqueness of names

As stated in the current Certification Practices Statement of Firmaprofesional.

3.1.6 Recognition, authentication and function of marks

As stated in the current Certification Practices Statement of Firmaprofesional.

3.2 Initial identity validation

The list of Incorporating Agencies or Registry Agencies is published in the repository of the Firmaprofesional website (www.firmaprofesional.com), in the "Verification Sources" section.

The following steps are followed to verify the certificate information:

1. If the applicant is an organization (legal person): existence, name, address and country of the organization are verified, using one of the following means:

    a. Consult the official registry depending on the type of organization in question. For example, for companies, the Commercial Registry will be consulted. In the case of public entities, a query will be made to a registry of public entities. A signed document issued by an official registry 825 days before the issuance of the certificate is also accepted.
    b. Consult a third party database periodically updated and considered a reliable data source. A reliable data source is understood to be a database used to verify information about the identity of organizations, recognized among commercial companies and public administrations as a reliable source and created by a third party, other than the applicant himself.

        A document or report issued by a trusted source, such as Legal Entity Identifier (LEI), is also valid.

    c. A statement written by a public official, notary or law firm.

    If the applicant wishes to incorporate the information of a registered trademark or trade name into the certificate, then it is verified that he has the right to use the trademark or name using one of the following means:

    a. Certificate issued by a governmental entity or consultation with an official registry, in which it is demonstrated that the applicant has the right to use the trademark or name that will appear on the certificate. For example, in Spain a search will be carried out in the Web registry of the Spanish Patent and

Trademark Office. Also, it would be useful for the applicant to provide a certificate from this same entity.

b. Consult a third party database periodically updated and considered a reliable data source. A reliable data source is understood to be a database used to verify that an organization has the right to use a trademark or trade name, and that it is recognized among commercial companies and public administrations as a reliable source and created by a third party, other than the same applicant.

   A document or report issued by a reliable source is also valid.

c. A statement written by a public official, notary or law firm, accompanied by documentation proving that the applicant has the right to use the trade name or trademark.

2. If the applicant is a natural person: the name, address and country are verified, using one of the following means:

   a. Photocopy of the DNI, passport or driving license, in which a photograph appears that allows the applicant's face to be discerned. This means will serve to verify the name and address of the applicant.

   b. If the location to be included in the certificate is not the same as the one that appears on the ID, passport or driver's license, the applicant can provide a water or electricity bill or a bank statement, in which the applicant is associated with the location to be included in the certificate.

3.2.1 Private key possession test method

As stated in the current Certification Practices Statement of Firmaprofesional.

3.2.2 Authentication of the organization's identity and domain identity

As stated in the current Certification Practices Statement of Firmaprofesional.

3.2.2.1 Domain validation

Firmaprofesional verifies, before issuing the SSL certificate, that the applicant has control over the domain for which the certificate is requested; If the request is made for a multi domain SSL certificate, Firmaprofesional verifies that all the domains that are added to the SAN (Subject Alternative Name) belong to the same organization. Verification will be done using at least one of the following methods:

1. A unique and random code is sent to the domain contact by email, fax, SMS message or letter by post. Anyone from the requesting organization can answer by any of these means, indicating the random code. Most often you will reply by Email.

   To send the random code, Firmaprofesional will use the email address, the fax number, the mobile phone number or the postal address that appears in the result of the search carried out in the Whois service.

2. A call is made to the administrative or technical contact of the domain name, which appears in the query made to the corresponding Whois service. The call confirms that the applicant has made the request for a certificate for the domain name in question. The call is made to the phone number that shows the search result to the Whois service. The call is recorded and stored by Firmaprofesional.

3. An email is sent to one or more of the following addresses "admin", "administrator", "webmaster", "hostmaster" or "postmaster", followed by the symbol "@" and the domain name for which it is requested the SSL certificate. The email sent by Firmaprofesional includes a random and unique code. Anyone from the requesting organization must respond to the email indicating the random code.

4. The requester makes a change to the DNS record of the domain for which the SSL certificate is requested. Firmaprofesional indicates a random and unique code. The

requester must add the random code in a CNAME, TXT or CAA field, in their DNS record. Once the change has been made by the applicant, Firmaprofesional verifies it.

3.2.3 Authentication of individual identity

As stated in the current Certification Practices Statement of Firmaprofesional.

3.2.4 Unverified subscriber information

No stipulation.

3.2.5 Validation of authority

As stated in the current Certification Practices Statement of Firmaprofesional.

3.2.6 Interoperation criteria

Currently Firmaprofesional does not have cross certification.

3.3 Identification and authentication for key renewal requests

3.3.1 Identification and authentication for routine key change

3.3.1.1 Online certificate renewal

The same steps must be followed as for the issuance of a new certificate (4.3 Certificate issuance).

3.3.1.2. Certificate renewal with persona

The identification process will be carried out in the same way as that of issuing a new one (section 4.3).

3.3.2 Identification and authentication for the renewal of certificates after their revocation

The identification process will be carried out in the same way as that of issuing a new one.

3.4 Identification and authentication for revocation request

As stated in the current Certification Practices Statement of Firmaprofesional.

4. Certificate life cycle operational requirements

4.1. Certificate request

4.1.1. Who can submit a certificate request

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

Application process differs between Electronic Office Certificates, SSL OV Certificates and SSL EV Certificates. The details of the process for each of them are 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. 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 1.3.3.

For the application process of Firmaprofesional SSL EV certificates it is necessary to use at least two of the persons mentioned in section 1.3.3.

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. Certificate application process and responsibilities

The applicant must contact Firmaprofesional or an authorized Intermediary.

The management of the issuance of this type of certificate can only be carried out by Firmaprofesional.

Sections 4.1.1.1, 4.1.1.2, 4.1.1.3 and 4.1.1.4 describe the specific process and documentation required to apply for each type of certificate.

4.2 Processing of certificate applications

In the case of Electronic Office certificates, the RA Operator will validate the veracity and accuracy of the applicant's data and the electronic office, as well as that the applicant is in possession of the private key associated with the public key included in the request.

certification. The RA Operator will generate the certificate request in a standard format and will send it to Firmaprofesional.

To process the SSL OV, SSL EV and PSD2 certificates, the applicant will deliver to Firmaprofesional, directly or through an authorized intermediary, a certificate request in PKCS # 10 format.

Firmaprofesional will carry out the technical validation of the PKCS # 10 request and the validation of the data it contains.

4.2.1 Performing identification and authentication functions

As stated in the current Certification Practices Statement of Firmaprofesional.

4.2.2 Approval or denial of certificate applications

Prior to the issuance of the Electronic Headquarters certificate, 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 request and that it has been generated by a duly authorized RA Operator. After this validation, the certificate will be issued.

In cases where Firmaprofesional has a guarantee that the requirements are met for the certificate to be considered to have a High level of security according to the Certificate Profiles document prepared by the Government of Spain, the certificate will be issued with the corresponding OID.

Prior to issuing the SSL OV, SSL EV and PSD2 certificates, the existence of a CAA record is validated for each DNS name of the CN and subjectAltName extensions of the certificate. In the event that the certificate is issued, validation will be done before the TTL of the CAA record. Firmaprofesional processes the "issue" and "issuewild" tags. The CAA record that identifies the domains for which the issuance by Firmaprofesional is authorized is "firmaprofesional.com".

If the request is electronically signed by means of a Corporate Certificate of Legal Representative of Firmaprofesional or a certificate of Legal Representative of another entity

that admits Firmaprofesional that has guaranteed the identification process in accordance with Spanish regulations, it will issue an SSL EV Web Server Certificate; otherwise, an SSL OV Web Server Certificate will be issued.

Additionally, the issuance of the SSL EV Web Server Certificate requires the approval of two people: the RA Operator in charge of managing the request and the Administrator of the Technical Department in charge of issuing the certificate. The same requirement is required for the issuance of a PSD2 Certificate

4.2.3 Processing time for certificate applications

As stated in the current Certification Practices Statement of Firmaprofesional.

4.3 Issuance of certificates

4.3.1 CA actions during certificate issuance

As stated in the current Certification Practices Statement of Firmaprofesional.

4.3.2 Notification to the subscriber by the CA of the issuance of the certificate and delivery

Firmaprofesional will deliver the certificate to the applicant allowing it to be downloaded safely from the Internet.

The headquarters certificates must be formally accepted by the applicant, leaving documentary evidence in the possession of the RA.

4.4. Certificate acceptance

4.4.1 Form in which the certificate is accepted

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

4.4.1.1. 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.

When 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.

4.4.1.1.1. Domain name control verification

For Electronic Office certificates, Firmaprofesional will follow the same method for domain name control verification than for SSL EV certificates. For more information, section "3.2.2 Authentication of the organization's identity and domain identity" of this document may be consulted.

4.4.1.2. 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.

4.4.1.3. Acceptance of application for EV Certificates

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

4.4.1.3.1. 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)	- Legal existence - Name of the organisation - Register number or VAT - Official Register	1) Online consultation with: - 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.
	- Representative	1) Online consultation with: - Trade Register. - National Chamber of Commerce. - Or Legal Entity Identifier (LEI). 2) Power of attorney 3) 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	- 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.
	- Representative	1) Official document (record) of appointment. 2) Power of attorney or Official document signed by Public attorney	Copy of the consultation, certificate or document issued.

Business Entity / Commercial Entity (Any entity that is not a private organisation, public entity or non-commercial entity)	- Legal existence - Name of the organisation - Register number or VAT	1) For Professional Associations: Creation bylaws, their publication in BOE and VAT card, or LEI. 2) For others: Consultation with public official register or LEI. 3) Certificate or document issued two years before the SSL Certificate issuance, by the Trade Register or LEI.	For Associations: - Bylaws copy -BOE publication copy - VAT copy - or LEI - Certificate or document issue copy. For others: - Consultation copy. -or LEI. - Certificate or document issued.
	- Representative	Official document (record) of appointment, either of the General Meeting of the entity, of the public registry or power of attorney	Copy of the Official document (record) or power of attorney
Non-Commercial Entities (International Organisation)	- Legal existence - Name of the organisation - Register number or VAT	1) Constitution document. 2) LEI.	-Constitution copy. - or LEI.
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	- The applicant has registered the commercial name or the brand.. - Registered brand or commercial name validity use.	1) Online Consultation with national official register. 2) Online consultation with international official register. 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.

4.4.1.3.2. 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.

4.4.1.3.3. 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.

4.4.1.3.4. 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.

4.4.1.3.5. 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 contact 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. Thus, the name, position, office and the approver authority are verified.

4.4.1.3.6. 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.

4.4.1.3.7. 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.

4.4.1.4. 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).

4.4.2 Publication of the certificate by the CA

As stated in the current Certification Practices Statement of Firmaprofesional.

4.4.3 Notification of the issuance of the certificate by the CA to other entities

As stated in the current Certification Practices Statement of Firmaprofesional.

4.5 Use of keys and certificate

4.5.1 Use of the private key and the certificate by the subscriber

As stated in the current Certification Practices Statement of Firmaprofesional.

4.5.2 Use of the public key and the certificate by third parties who trust the certificates

As stated in the current Certification Practices Statement of Firmaprofesional.

4.6 Renewal of the certificate without change of keys

No stipulation.

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who can request renewal

No stipulation.

4.6.3 Certificate renewal request process

No stipulation.

4.6.4 Notification to the subscriber of the issuance of a new certificate

No stipulation.

4.6.5 Conduct that constitutes acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of the issuance of the certificate by the CA to other entities

No stipulation.

4.7 Renewal of the certificate with change of keys

The same steps must be followed as for issuing a new certificate (section 4.3).

4.7.1 Circumstances for online renewal with password change

No stipulation.

4.7.2 Who can request the online renewal of a certificate

No stipulation.

4.7.3 Processing of online renewal requests

No stipulation.

4.7.4 Notification of the issuance of the renewed certificate

The same steps are followed as for issuing a new certificate (section 4.3.2).

4.7.5 Form of acceptance of the renewed certificate

The same steps are followed as for issuing a new certificate.

4.7.6 Publication of the renewed certificate

The same steps are followed as for issuing a new certificate.

4.7.7 Notification of the issuance of the certificate by the CA to other entities

The same steps are followed as for issuing a new certificate.

4.8 Modification of certificates

In case of modifying any data, Firmaprofesional will proceed to revoke and issue a new certificate.

4.8.1 Circumstance of certificate modification

No stipulation

4.8.2 Who can request the modification of the certificate

No stipulation

4.8.3 Processing of certificate modification requests

No stipulation

4.8.4 Notification of the issuance of a new certificate to the subscriber

No stipulation

4.8.5 Behavior that constitutes acceptance of a modified certificate

No stipulation

4.8.6 Publication of the certificate modified by the CA

No stipulation

4.8.7 Notification of the issuance of certificates by the CA to other entities

No stipulation

4.9 Revocation and suspension of certificates

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

Revocation is made as specified in Firmaprofesional's Certification Practice Statement (CPS).

4.9.1 Circumstances for revocation

As stated in the current Certification Practices Statement of Firmaprofesional.

4.9.2 Who can request revocation

As stated in the current Certification Practices Statement of Firmaprofesional.

4.9.3 Revocation request procedures

As stated in the current Certification Practices Statement of Firmaprofesional.

4.9.4 Grace period for the revocation request.

No stipulation.

4.9.5 Term in which the CA must resolve the revocation request

As stated in the current Certification Practices Statement of Firmaprofesional.

4.9.6 Obligation to verify revocations by third parties

As stated in the current Certification Practices Statement of Firmaprofesional.

4.9.7 Frequency of issuance of CRLs

As stated in the current Certification Practices Statement of Firmaprofesional.

4.9.8 Maximum time between generation and publication of CRLs

As stated in the current Certification Practices Statement of Firmaprofesional.

4.9.9 Availability of the online system for verifying the status of certificates

As stated in the current Certification Practices Statement of Firmaprofesional.

4.9.10 Online revocation check requirements

As stated in the current Certification Practices Statement of Firmaprofesional.

4.9.11 Other forms of revocation announcements available

Without stipulation.

4.9.12 Special needs in relation to key compromise

As stated in the current Certification Practices Statement of Firmaprofesional.

4.9.13 Circumstances for suspension

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

4.9.14 Who can request suspension

No stipulation.

4.9.15 Suspension request procedure

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

4.9.16 Limits of the suspension period

No stipulation.

4.10 Certificate status information services

4.10.1 Operational characteristics

As stated in the current Certification Practices Statement of Firmaprofesional.

4.10.2 Service availability

As stated in the current Certification Practices Statement of Firmaprofesional.

4.10.3 Additional features

As stated in the current Certification Practices Statement of Firmaprofesional.

4.11 Termination of subscription

As stated in the current Certification Practices Statement of Firmaprofesional.

4.12 Custody and recovery of keys

As stated in the current Certification Practices Statement of Firmaprofesional.

4.12.1 Fundamental Custody and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Physical security, facilities, management and operational controls

5.1 Physical controls

As stated in the current Certification Practices Statement of Firmaprofesional.

5.1.1. Physical location and construction

As stated in the current Certification Practices Statement of Firmaprofesional.

5.1.2. Physical access

As stated in the current Certification Practices Statement of Firmaprofesional.

5.1.3. Power supply and air conditioning

As stated in the current Certification Practices Statement of Firmaprofesional.

5.1.4 Exposure to water

As stated in the current Certification Practices Statement of Firmaprofesional.

5.1.5. Fire protection and prevention

As stated in the current Certification Practices Statement of Firmaprofesional.

5.1.6. Storage system

As stated in the current Certification Practices Statement of Firmaprofesional.

5.1.7 Disposal of information carriers

As stated in the current Certification Practices Statement of Firmaprofesional.

5.1.8. Off-site backups

As stated in the current Certification Practices Statement of Firmaprofesional.

5.2 Procedural controls

5.2.1. Roles of those responsible

As stated in the current Certification Practices Statement of Firmaprofesional.

5.2.2. Number of people required per task

As stated in the current Certification Practices Statement of Firmaprofesional.

5.2.3. Identification and authentication by role

As stated in the current Certification Practices Statement of Firmaprofesional.

5.2.4. Roles that require segregation of duties

As stated in the current Certification Practices Statement of Firmaprofesional.

5.3 Personnel controls

5.3.1. Requirements related to professional qualification, knowledge and experience

As stated in the current Certification Practices Statement of Firmaprofesional.

5.3.2. Background check procedures

As stated in the current Certification Practices Statement of Firmaprofesional.

5.3.3. Training requirements

As stated in the current Certification Practices Statement of Firmaprofesional.

5.3.4. Requirements and frequency of training update

As stated in the current Certification Practices Statement of Firmaprofesional.

5.3.5. Frequency and sequence of task rotation

As stated in the current Certification Practices Statement of Firmaprofesional.

5.3.6. Sanctions for unauthorized actions

As stated in the current Certification Practices Statement of Firmaprofesional.

5.3.7. Requirements for hiring third parties

As stated in the current Certification Practices Statement of Firmaprofesional.

5.3.8. Documentation provided to staff

As stated in the current Certification Practices Statement of Firmaprofesional.

5.4 Security audit procedures

5.4.1. Types of recorded events

As stated in the current Certification Practices Statement of Firmaprofesional.

5.4.2. Audit record processing frequency

As stated in the current Certification Practices Statement of Firmaprofesional.

5.4.3. Retention period for audit records

As stated in the current Certification Practices Statement of Firmaprofesional.

5.4.4. Protection of audit logs

As stated in the current Certification Practices Statement of Firmaprofesional.

5.4.5. Back-up procedures for audit records

As stated in the current Certification Practices Statement of Firmaprofesional.

5.4.6. Audit information collection system

As stated in the current Certification Practices Statement of Firmaprofesional.

5.4.7. Notification to the subject causing the event

No stipulation.

5.4.8. Vulnerability scan

As stated in the current Certification Practices Statement of Firmaprofesional.

5.5 Log file

5.5.1. Type of events files

According to what is stated in the current Certification Practices Statement of Firmaprofesional

5.5.2. Record retention period

According to what is stated in the current Certification Practices Statement of Firmaprofesional

5.5.3. File protection

According to what is stated in the current Certification Practices Statement of Firmaprofesional

5.5.4 File Backup Procedures

According to what is stated in the current Certification Practices Statement of Firmaprofesional

5.5.5 Requirements for time stamping of records

According to what is stated in the current Certification Practices Statement of Firmaprofesional

5.5.6. Audit Information File System

No stipulation

5.5.7. Procedures for obtaining and verifying archived information

As stated in the current Certification Practices Statement of Firmaprofesional.

5.6 CA password change

5.6.1. Root CA

As stated in the current Certification Practices Statement of Firmaprofesional.

5.6.2. Subordinate CA

As stated in the current Certification Practices Statement of Firmaprofesional.

5.7 Disaster recovery plan

5.7.1 Incident and vulnerability management procedures

As stated in the current Certification Practices Statement of Firmaprofesional.

5.7.2. Alteration of hardware, software and / or data resources

As stated in the current Certification Practices Statement of Firmaprofesional.

5.7.3. Procedure for action against the vulnerability of the private key of a Certification Authority or of the cryptographic suite

As stated in the current Certification Practices Statement of Firmaprofesional.

5.7.4. Business continuity after a disaster

As stated in the current Certification Practices Statement of Firmaprofesional.

5.8 Cessation of activity

5.8.1. Certification Authority

As stated in the current Certification Practices Statement of Firmaprofesional.

5.8.2.Registration Authority

As stated in the current Certification Practices Statement of Firmaprofesional.

6. Technical security controls

6.1 Generation and installation of the key pair

6.1.1 Key pair generation

As stated in the current Certification Practices Statement of Firmaprofesional.

Specifically, in relation to this PC, 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.

6.1.2 Delivery of the private key to the signer

As stated in the current Certification Practices Statement of Firmaprofesional.

6.1.3 Delivery of the public key to the certificate issuer

As stated in the current Certification Practices Statement of Firmaprofesional.

6.1.4 Delivery of the CA public key to third parties that trust the certificates

As stated in the current Certification Practices Statement of Firmaprofesional.

6.1.5. Key size

They must be RSA keys with a minimum length of 2,048 bits.

6.1.6. Public key generation parameters and quality verification

As stated in the current Certification Practices Statement of Firmaprofesional.

6.1.7. Supported uses of the key (X.509v3 KeyUsage field)

As stated in the current Certification Practices Statement of Firmaprofesional.

6.2 Protection of the private key and engineering controls of the cryptographic modules

6.2.1 Standards for cryptographic modules

As stated in the current Certification Practices Statement of Firmaprofesional.

6.2.2 Multi-person control (k of n) of private key

As stated in the current Certification Practices Statement of Firmaprofesional.

6.2.3 Private key custody

As stated in the current Certification Practices Statement of Firmaprofesional.

6.2.4. Private key backup

As stated in the current Certification Practices Statement of Firmaprofesional.

6.2.5. Private key file

As stated in the current Certification Practices Statement of Firmaprofesional.

6.2.6. Transfer of the private key to or from the cryptographic module

As stated in the current Certification Practices Statement of Firmaprofesional.

6.2.7 Storage of the private key in the cryptographic module

As stated in the current Certification Practices Statement of Firmaprofesional.

6.2.8. Private key activation method

As stated in the current Certification Practices Statement of Firmaprofesional.

6.2.9. Private key deactivation method

As stated in the current Certification Practices Statement of Firmaprofesional.

6.2.10 Private key destruction method

As stated in the current Certification Practices Statement of Firmaprofesional.

6.2.11 Classification of cryptographic modules

As stated in the current Certification Practices Statement of Firmaprofesional.

6.3. Other Aspects of Key Pair Management

6.3.1 Public key file

As stated in the current Certification Practices Statement of Firmaprofesional.

6.3.2 Certificate operational periods and period of use for the key pair

As stated in the current Certification Practices Statement of Firmaprofesional.

6.4 Activation data

6.4.1 Generation and installation of activation data

As stated in the current Certification Practices Statement of Firmaprofesional.

6.4.2 Protection of activation data

As stated in the current Certification Practices Statement of Firmaprofesional.

6.4.3 Other aspects of activation data

No stipulation

6.5 IT security controls

As stated in the current Certification Practices Statement of Firmaprofesional.

6.5.1 Specific technical safety requirements

As stated in the current Certification Practices Statement of Firmaprofesional.

6.5.2. IT security assessment

As stated in the current Certification Practices Statement of Firmaprofesional.

6.6. Lifecycle security controls

6.6.1 System development controls

As stated in the current Certification Practices Statement of Firmaprofesional.

6.6.2 Security management controls

As stated in the current Certification Practices Statement of Firmaprofesional.

6.6.3 Lifecycle management of cryptographic hardware

As stated in the current Certification Practices Statement of Firmaprofesional.

6.7 Network security controls

As stated in the current Certification Practices Statement of Firmaprofesional.

6.8. Time source

As stated in the current Certification Practices Statement of Firmaprofesional.

7. CRL and OCSP Certificate profiles

7.1. Certificate profile

The Practices Statement of Firmaprofesional describes the profile common to all certificates.

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).

7.1.1 Version number

As stated in the current Certification Practices Statement of Firmaprofesional.

7.1.2. Certificate extensions

In the document "Profiles of Firmaprofesional Certificates" the extensions required for each type of certificate contemplated in this policy will be specified.

7.1.3. Object identifiers (OID) of the algorithms used

In accordance with section 7.1 of this policy.

7.1.4. Name formats

As stated in the current Certification Practices Statement of Firmaprofesional.

7.1.5. Name restrictions

As stated in the current Certification Practices Statement of Firmaprofesional.

7.1.6. Policy Object Identifier (OID)

The OIDs of each certificate included in this policy are detailed in sections 1.2 and 7.1 of this policy.

7.1.7 Extension of the use of policy constraints

No stipulation.

7.1.8 Syntax and semantics of the “PolicyQualifier”

As stated in the current Certification Practices Statement of Firmaprofesional.

7.1.9 Semantic treatment for the "Certificate Policy" extension

As stated in the current Certification Practices Statement of Firmaprofesional.

7.2 CRL Profile

As stated in the current Certification Practices Statement of Firmaprofesional.

7.2.1 Version number

As stated in the current Certification Practices Statement of Firmaprofesional.

7.2.2 CRL and extensions

As stated in the current Certification Practices Statement of Firmaprofesional.

7.3 OCSP Profile

7.3.1 Version number

As stated in the current Certification Practices Statement of Firmaprofesional.

7.3.2 OCSP and extensions

No stipulation.

8. Compliance audits and other controls

8.1. Frequency of audits

As stated in the current Certification Practices Statement of Firmaprofesional.

8.2. Auditor qualification

As stated in the current Certification Practices Statement of Firmaprofesional.

8.3 Relationship between the auditor and the audited authority

As stated in the current Certification Practices Statement of Firmaprofesional.

8.4 Aspects covered by controls

8.4.1 Audits in Registration Authorities

As stated in the current Certification Practices Statement of Firmaprofesional.

8.5 Actions to be taken as a result of the detection of incidents

As stated in the current Certification Practices Statement of Firmaprofesional.

8.6 Communication of results

As stated in the current Certification Practices Statement of Firmaprofesional.

9. Other legal and business issues

9.1 Fees

Firmaprofesional may establish the rates it deems appropriate for subscribers, as well as establish the means of payment it deems most appropriate in each case. For more details on the price and payment conditions of this type of certificate, it will be necessary to consult the Commercial Department of Firmaprofesional.

9.1.1 Certificate issuance or renewal fees

As stated in the current Certification Practices Statement of Firmaprofesional.

9.1.2 Fees for access to certificates

As stated in the current Certification Practices Statement of Firmaprofesional.

9.1.3 Access fees to status or revocation information

As stated in the current Certification Practices Statement of Firmaprofesional.

9.1.4 Rates of other services

As stated in the current Certification Practices Statement of Firmaprofesional.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibilities

As stated in the current Certification Practices Statement of Firmaprofesional.

9.2.1 Insurance coverage

As stated in the current Certification Practices Statement of Firmaprofesional.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or guarantee coverage for end entities

No stipulation.

9.3 Confidentiality of information

As stated in the current Certification Practices Statement of Firmaprofesional.

9.3.1 Scope of confidential information

As stated in the current Certification Practices Statement of Firmaprofesional.

9.3.2 Non-confidential information

As stated in the current Certification Practices Statement of Firmaprofesional.

9.3.3 Responsibility for the protection of confidential information

As stated in the current Certification Practices Statement of Firmaprofesional.

9.4 Protection of personal information

9.4.1 Personal data protection policy

As stated in the current Certification Practices Statement of Firmaprofesional.

9.4.2 Information treated as private

As stated in the current Certification Practices Statement of Firmaprofesional.

9.4.3 Information not classified as private

As stated in the current Certification Practices Statement of Firmaprofesional.

9.4.4. Responsibility for the protection of personal data

As stated in the current Certification Practices Statement of Firmaprofesional.

9.4.5 Communication and consent to use personal data

As stated in the current Certification Practices Statement of Firmaprofesional.

9.4.6 Disclosure in the framework of a judicial process

As stated in the current Certification Practices Statement of Firmaprofesional.

9.4.7 Other circumstances of publication of information

As stated in the current Certification Practices Statement of Firmaprofesional.

9.5 Intellectual property rights

As stated in the current Certification Practices Statement of Firmaprofesional.

9.6 Obligations

9.6.1 Obligations of the CA

As stated in the current Certification Practices Statement of Firmaprofesional.

9.6.2 Obligations of the RA

As stated in the current Certification Practices Statement of Firmaprofesional.

9.6.3 Obligations of applicants

As stated in the current Certification Practices Statement of Firmaprofesional.

9.6.4 Obligations of third parties who trust the certificates

As stated in the current Certification Practices Statement of Firmaprofesional.

9.6.5 Obligations of other participants

No stipulation.

9.7 Disclaimer of warranty

As stated in the current Certification Practices Statement of Firmaprofesional.

9.8 Responsibilities

9.8.1 Responsibilities of the Certification Authority

As stated in the current Certification Practices Statement of Firmaprofesional.

9.8.2 Responsibilities of the Registration Authority

As stated in the current Certification Practices Statement of Firmaprofesional.

9.8.3 Subscriber Responsibilities

As stated in the current Certification Practices Statement of Firmaprofesional.

9.8.4 Delimitation of responsibilities

As stated in the current Certification Practices Statement of Firmaprofesional.

9.9 Indemnification

9.9.1 Scope of coverage

As stated in the current Certification Practices Statement of Firmaprofesional.

9.9.2 Insurance coverage and other guarantees for accepting third parties

There is no coverage for third party acceptors.

9.9.3 Loss limitations

As stated in the current Certification Practices Statement of Firmaprofesional.

9.10 Period of validity

9.10.1 Term

This CP will enter into force at the time of its publication.

9.10.2 Replacement and repeal of the CPS

This CP will be repealed when a new version of the document is published.

The new version will fully replace the previous document.

9.10.3 Effects of termination

For current certificates issued under a previous CP, the new version will prevail over the previous one in everything that is not opposed to it.

9.11 Individual notifications and communication with participants

In general, the Firmaprofesional website www.firmaprofesional.com will be used to carry out any type of notification and communication.

If the website authentication certificate subscriber detects any problem with the certificate, he / she can notify it by e-mail to support@firmaprofesional.com

Any mail that is sent to this email address enters the Firmaprofesional Customer Service System.

In the event that modifications are made to relevant information about PSD2 of the payment service provider that may affect the validity of the certificate, the Bank of Spain or the Competent National Authority will communicate this through the account soporte@firmaprofesional.com.

9.12 Changes in specifications

9.12.1 Procedure for changes

According to what is stated in the current Certification Practices Statement of Firmaprofesional

9.12.2 Notification period and procedure

According to what is stated in the current Certification Practices Statement of Firmaprofesional

9.12.3 Circumstances in which the OID must be changed

According to what is stated in the current Certification Practices Statement of Firmaprofesional.

9.13 Complaints and conflict resolution

According to what is stated in the current Certification Practices Statement of Firmaprofesional

9.14 Applicable regulations

According to what is stated in the current Certification Practices Statement of Firmaprofesional

9.15 Compliance with applicable regulations

According to what is stated in the current Certification Practices Statement of Firmaprofesional

9.16 Miscellaneous stipulations

9.16.1 Full acceptance clause

According to what is stated in the current Certification Practices Statement of Firmaprofesional

9.16.2 Independence

According to what is stated in the current Certification Practices Statement of Firmaprofesional

9.16.3 Resolution by judicial means

According to what is stated in the current Certification Practices Statement of Firmaprofesional

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force majeure

According to what is stated in the current Certification Practices Statement of Firmaprofesional

9.17 Other provisions

No stipulation.

firmaprofesional

Firmaprofesional, S.A.

February 2021