

Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1



CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)

Introduction must include:

1) CA's Legal Name: **Firmaprofesional S.A.**

2) Clear indication (subject and SHA1 or SHA256 fingerprints) about which root certificates are being evaluated, and their full CA hierarchy. In considering a root certificate for inclusion in NSS, Mozilla must also evaluate the current subordinate CAs and the selection/approval criteria for future subordinate CAs. Mozilla's CA Certificate Policy requires full disclosure of non-technically-constrained intermediate certificates chaining up to root certificates in NSS.

CN=Autoridad de Certificacion Firmaprofesional CIF A62634068 (SHA1) 04048028BF1F2864D48F9AD4D83294366A828856553F3B14303F90147F5D40EF

CN=Autoridad de Certificacion Firmaprofesional CIF A62634068 (SHA256) 57DE0583EFD2B26E0361DA99DA9DF4648DEF7EE8441C3B728AFA9BCDE0F9B26A

CN=AC Firmaprofesional - INFRAESTRUCTURA (SHA256) CD74198D4C23E4701DEA579892321B9E4F47A08BD8374710B899AAD1495A4B35

CN = AC Firmaprofesional - Secure Web 2020 (SHA256) 933B80F7B97255DF5CF1D95A123E901722DDB30B481AF3AA83548201119ED303

CN = AC Firmaprofesional - Secure Web 2021 (SHA256) 59228535D114E8D29F9B92D422518BC63DDCB57097428D8C98777D907C6EEFE

3) List the specific version(s) of the BRs that you used. For example: BR version 1.4.2, with the exception of the Domain Validation section 3.2.2.4 for which we used BR version 1.4.1.

BR version 1.7.3

4) List the specific versions of the CA's documents that were evaluated, and provide direct URLs to those documents. All provided CA documents must be public-facing, available on the CA's website, and translated into English.

CPS 210322 (https://www.firmaprofesional.com/wp-content/uploads/pdfs/FP_CPS-210322-EN-sFP.pdf)


CP Website (https://www.firmaprofesional.com/wp-content/uploads/pdfs/FP_CP_Autenticacion_Web-210322-EN-sFP.pdf)

Certificate profiles (https://www.firmaprofesional.com/wp-content/uploads/pdfs/FP_Perfiles_Certificados-210322-EN-sFP.pdf)

5) If you intend to submit your self-assessment with statements such as "will add/update in our next version of CP/CPS", indicate when you plan to provide the updated documents.

Note: When you are doing your BR Self Assessment, if you find that the required information is not currently in your CP/CPS documents, then you may indicate what your CA currently does, how it is currently documented, that the next version of your CP/CPS will contain this information, and when the next version of your CP/CPS will be available.

BR/RFC 3647 Section Number	List the specific documents and section numbers of those documents which meet the requirements of each BR section	Explain how the CA's listed documents meet the requirements of each BR section.
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, <i>indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.</i>	CPS: Version 210322 Effective date: 22/03/2021	We consider the current CPS compliant with the requirements The CP and CPS are aligned to BR 1.7.4 as of effective date 5 April 2021 in accordance with RFC 3647. The CPS is regularly revised and modified in accordance with BR and having in mind the effective dates of the items reviewed in BR. Each certificate created after effective date is in compliance with the changed items, verified by regular audits.
1.2.2. Relevant Dates Note the Compliance date for each item in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, <i>indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.</i>	CPS: Version 210322 Effective date: 22/03/2021	We consider the current CPS compliant with the items specified in relevant dates.
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. <i>Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs (including non-delegation of domain validation to RAs).</i>	CPS Section 1.3.2. Registration Authority (RA) CP Website Authentication - Section 1.3.2 Register Authority (RA)	As stated in the CPS, Firmaprofesional will contractually formalise the relationship between itself and each of the entities who act as an RA of Firmaprofesional. The CP indicates that web authentication certificates issuance management will be performed solely by Firmaprofesional.
1.5.2 Contact person BR Section 4.9.3 requires that this section 1.5.2 contain clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates.	CPS Section 1.5.2. Contact person	The CPS (and CP by reference) includes an email to be used in case of complaints, suggestions and communication of unauthorized uses of certificates.
2.1. Repositories <i>Provide the direct URLs to the CA's repositories</i>	CPS Section 2.1 Repositories	CPS, Certification Policies and PDS repository: http://www.firmaprofesional.com/cps Root CA repository: http://crl.firmaprofesional.com/caroot.crt CA INFRAESTRUCTURA: http://crl.firmaprofesional.com/infraestructura.crt CA Secure Web 2020: https://crl.firmaprofesional.com/secureweb2020.crt CA Secure Web 2021: https://crl.firmaprofesional.com/secureweb2021.crt

Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1		
2.2 Publication of information - RFC 3647 "The Certificate Policy and/or Certification Practice Statement MUST be structured in accordance with RFC 3647. "	CPS Section 1.1 Presentation	The structure of this document is based on the specifications of standard "RFC3647 - Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework", created by the working group PKIX of the IETF.
2.2 Publication of information - CAA Section 4.2 of a CA's Certificate Policy and/or Certification Practice Statement SHALL state the CA's policy or practice on processing CAA Records for Fully Qualified Domain Names; that policy shall be consistent with these Requirements. It shall clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuwild" records as permitting it to issue. The CA SHALL log all actions taken, if any, consistent with its processing practice.	CPS Section 4.2. Processing of certificate applications	Firmaprofesional processes tag "issue" and "issuwild". The CAA register that identifies those domains whose issuance is authorised by Firmaprofesional is "firmaprofesional.com".
2.2. Publication of information - BR text "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." --> Copy the specific text that is used into the explanation in this row. (in English)	CPS Section 9.14. Applicable regulations	FIRMAPROFESIONAL conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org . In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.
2.2. Publication of information - test websites "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired." --> List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.		The test URLs are: https://testssl.firmaprofesional.com https://testexpiredssl.firmaprofesional.com https://testrevokedssl.firmaprofesional.com https://testsslev.firmaprofesional.com https://testexpiredslev.firmaprofesional.com https://testrevokedslev.firmaprofesional.com https://testsede.firmaprofesional.com https://testexpiredsede.firmaprofesional.com https://testrevokedsede.firmaprofesional.com
2.3. Time or frequency of publication "The CA SHALL ... annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements. The CA SHALL indicate conformance with this requirement by incrementing the version number and adding a dated changelog entry, even if no other changes are made to the document." <i>Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.</i>	CPS Section 1.5.3 Frequency of review	The CPS, CPs and PDSs are reviewed and updated annually. BR requirements are reviewed regularly.
2.4. Access controls on repositories <i>Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.</i>	CPS Section 2.4 Access controls on repositories	The CPS, CPs and PDSs, CA certificates and CRL will be published in repositories accessible to the public and without any access control.
3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, <i>indicate how your CP/CPS meets the requirements in this section of the BRs.</i>	CPS Section 3.2.2 Authentication of the identity of a legal person	The RA must verify the data concerning the business name or corporate name of the organization.
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, <i>indicate how your CP/CPS meets the requirements in this section of the BRs.</i>	CPS Section 3.1.6 Recognition, authentication and the role of trademarks	Firmaprofesional will seek evidence of the possession of the right to the trademark requested before the issuance of the certificates, through consultation with official records or documents issued by them.
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, <i>indicate how your CP/CPS meets the requirements in this section of the BRs.</i>	CPS Sections 3.2.2 Authentication of the identity of a legal person and 3.2.3 Authentication of the identity of a natural person	Verification of the CountryName field is done through the official documentation provided by the applicant, using a valid official identity document or a certificate of registration in commercial register for organizations.

Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1





<p>3.2.2.4 Validation of Domain Authorization or Control <i>Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS.</i></p> <p>Section 2.2 of Mozilla's Root Store Policy states: "For a certificate capable of being used for SSL-enabled servers, the CA must ensure that the applicant has registered all domain(s) referenced in the certificate or has been authorized by the domain registrant to act on their behalf. This must be done using one or more of the methods documented in section 3.2.2.4 of the CA/Browser Forum Baseline Requirements. The CA's CP/CPS must clearly specify the procedure(s) that the CA employs, and each documented procedure should state which subsection of 3.2.2.4 it is complying with. CAs are not permitted to use 3.2.2.5 (4) ("any other method") to fulfill the requirements of method 3.2.2.4.8 (IP Address)."</p>	<p>Make sure the CP/CPS states what the CA actually does, not what it could do. Such as which of the allowed domain validation methods the CA uses.</p> <p>CP Website Authentication Certificates Section 3.2.2.1 Domain validation</p>	<p>Prior to the SSL Certificate issuance, Firmaprofesional verifies, before issuing the SSL certificate, that the applicant has control over the domain for which the certificate is requested.</p> <p>Verification is done using at least one of the following methods, according to the methods defined in the BR of the CA / Browser Forum in points 3.2.2.4.4 and 3.2.2.4.7.</p>
<p>3.2.2.4.1 Validating the Applicant as a Domain Contact This method SHALL NOT be used.</p>	<p>This method SHALL NOT be used.</p>	<p>Not used.</p>
<p>3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact <i>If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.</i></p>	<p>CP Website Authentication Certificates Section 3.2.2.1 Domain validation</p>	<p>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.</p> <p>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.</p>
<p>3.2.2.4.3 Phone Contact with Domain Contact This method has been replaced by 3.2.2.4.15 and SHALL NOT be used. (Validations completed as of 31-May-2019 may be used until 20-August-2021.)</p>	<p>This method SHALL NOT be used.</p>	<p>Not used.</p>
<p>3.2.2.4.4 Constructed Email to Domain Contact <i>If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.</i></p>	<p>CP Website Authentication Certificates Section 3.2.2.1 Domain validation</p>	<p>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.</p>
<p>3.2.2.4.5 Domain Authorization Document "This method SHALL NOT be used."</p>	<p>This method SHALL NOT be used.</p>	<p>Not used.</p>
<p>3.2.2.4.6 Agreed-Upon Change to Website Replaced with BR section 3.2.2.4.18 (effective 3/3/2020)</p>	<p>This method SHALL NOT be used.</p>	<p>Not used.</p>
<p>3.2.2.4.7 DNS Change <i>If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.</i></p>	<p>CP Website Authentication Certificates Section 3.2.2.1 Domain validation</p>	<p>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.</p>
<p>3.2.2.4.8 IP Address <i>If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.</i></p>		<p>Not used.</p>
<p>3.2.2.4.9 Test Certificate "This method SHALL NOT be used."</p>	<p>This method SHALL NOT be used.</p>	<p>Not used.</p>

Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1



<p>3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, <i>indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.</i></p> <p><i>This subsection contains major vulnerabilities. If the CA uses this method, then the CA should describe how they are mitigating those vulnerabilities. If not using this method, the CPS should say so.</i></p>	<p>Further explanation is required if this method is used.</p>	<p>Not used.</p>
<p>3.2.2.4.11 Any Other Method "This method SHALL NOT be used."</p>	<p>This method SHALL NOT be used.</p>	<p>Not used.</p>
<p>3.2.2.4.12 Validating Applicant as a Domain Contact "This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name."</p> <p>If your CA uses this method of domain validation, <i>indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.</i></p>	<p>Use of this method is restricted, per the BRs.</p>	<p>Not used.</p>
<p>3.2.2.4.13 Email to DNS CAA Contact If your CA uses this method of domain validation, <i>indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.</i></p>		<p>Not used.</p>
<p>3.2.2.4.14 Email to DNS TXT Contact If your CA uses this method of domain validation, <i>indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.</i></p>		<p>Not used.</p>
<p>3.2.2.4.15 Phone Contact with Domain Contact If your CA uses this method of domain validation, <i>indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.</i></p>	<p>CP Website Authentication Certificates Section 3.2.2.1 Domain validation</p>	<p>Not used.</p>
<p>3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact If your CA uses this method of domain validation, <i>indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.</i></p>		<p>Not used.</p>
<p>3.2.2.4.17 Phone Contact with DNS CAA Phone Contact If your CA uses this method of domain validation, <i>indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.</i></p>		<p>Not used.</p>
<p>3.2.2.4.18 Agreed-Upon Change to Website v2 If your CA uses this method of domain validation, <i>indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.</i></p>		<p>Not used.</p>
<p>3.2.2.4.19 Agreed-Upon Change to Website - ACME If your CA uses this method of domain validation, <i>indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.</i></p>		<p>Not used.</p>
<p>3.2.2.4.20 TLS Using ALPN - If your CA uses this method of domain validation, <i>indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.</i></p>		<p>Not used.</p>
<p>3.2.2.5 Authentication for an IP Address If your CA allows IP Addresses to be listed in certificates, <i>indicate which methods your CA uses and how your CA meets the requirements in this section of the BRs.</i></p> <p>Section 2.2 of Mozilla's root store policy says: "the CA must ensure that the applicant has control over all IP Address(es) referenced in the certificate. This must be done using one or more of the methods documented in section 3.2.2.5 of the CA/Browser Forum Baseline Requirements. The CA's CP/CPS must clearly specify the procedure(s) that the CA employs, and each documented procedure should state which subsection of 3.2.2.5 it is complying with."</p>	<p>Method 3.2.2.5.4, Any Other Method, SHALL NOT be used.</p> <p>"After July 31, 2019, CAs SHALL maintain a record of which IP validation method, including the relevant BR version number, was used to validate every IP Address."</p>	<p>Not used.</p>
<p>3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then <i>indicate how your CA meets the requirements in this section of the BRs.</i></p>	<p>CP Website Authentication Certificates Section 1.4.1.3. Multi-domain certificates</p>	<p>CA allows SSL Web Server certificates with a wildcard character as defined in the RFC 2818 "HTTP Over TLS". It is solely permitted to issue wildcard certificates for SSL OV Web Server Certificates.</p>
<p>3.2.2.7 Data Source Accuracy <i>Indicate how your CA meets the requirements in this section of the BRs.</i></p>	<p>CPS Section 3.2 Initial Identity Validation</p>	<p>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.</p>

Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1		 firmaprofesional
3.2.2.8 CAs MUST check and process CAA records <i>Indicate how your CA meets the requirements in this section of the BRs.</i> Section 2.2 of the BRs states: " CA's Certificate Policy and/or Certification Practice Statement ... shall clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue." "	CPS Section 4.2. Processing of certificate applications CP Website Authentication Certificates Section 4.2.2 Approval or denial of certificate applications	Prior to the issuance of the SSL OV, SSL EV and PSD2 certificates, the existence of CAA registry for each DNS of the CN extensions and subjectAltName of the certificate is validated. In the event that the certificate is issued, the validation will be carried out before the TTL of the CAA record. Firmaprofesional processes the tags "issue" and "issuewild". The CAA registry that identifies domains for which the issuance by Firmaprofesional is authorized is "firmaprofesional.com".
3.2.3. Authentication of Individual Identity	CPS Section 3.2.3. Authentication of the identity of a natural person	No stipulation.
3.2.5. Validation of Authority	CPS Section 3.2.2. Authentication of the identity of a legal person and domain identity	The RA must verify the following information in order to authenticate the identity of the organisation: - The data concerning the business name or corporate name of the organisation. - The data relating to the constitution and legal status of the subscriber. - The data concerning the extent and validity of the powers of representation of the applicant. - The data concerning the tax identification code of the organisation or equivalent code used in the country to whose legislation the subscriber is subject.
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	CPS Section 3.2.6. Criteria for interoperation	Currently Firmaprofesional does not have cross certification.
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	CPS Section 3.2.7. Identification of high risk certificates	Firmaprofesional has methods to identify high-risk / suspicious certificates requests through the use of blacklists, which require additional checks.
4.1.2. Enrollment Process and Responsibilities	CPS Section 4.1.2. Certificate application processes CP Website Authentication Certificates Section 4.1.2. Certificate application process and responsibilities	The requirements to be met by an applicant will depend on the certificate type requested and they are specified in the "Certification Policy" of each specific type of certificate. The Website Authentication Certification Policy states the application process for Electronic Office Certificates, OV Certificates, EV Certificates and PSD2 Certificates.
4.2. Certificate application processing BR section 2.2 says that section 4.2 of the CP/CPS SHALL state the CA's policy or practice on processing CAA Records for Fully Qualified Domain Names.	CPS Section 4.2. Processing of certificate applications	Prior to the issuance of the SSL OV, SSL EV and PSD2 certificates, the existence of CAA registry for each DNS of the CN extensions and subjectAltName of the certificate is validated. In the event that the certificate is issued, the validation will be carried out before the TTL of the CAA record. Firmaprofesional processes the tags "issue" and "issuewild". The CAA registry that identifies domains for which the issuance by Firmaprofesional is authorized is "firmaprofesional.com".
4.2.1. Performing Identification and Authentication Functions Indicate how your CA identifies high risk certificate requests. Re-use of domain / IP address validation is limited to 398 days and re-use of other validation information is limited to 825 days	CPS Section 4.2.1. Performing identification and authentication functions	It is the responsibility of the RA to identify and authenticate the signatory. This process should be performed prior to issuing the certificate. The identification process will be carried out in the same way as when issuing a new certificate.
4.2.2. Approval or Rejection of Certificate Applications "CAs SHALL NOT issue certificates containing Internal Names."	CPS Section 4.2.2 Approval or rejection of certificate applications	Once a certificate has been requested the RA will verify the information provided by the applicant, including validation of the signer's identity. If the information is not correct, the RA will reject the request and contact the applicant to inform them of the reason. If it is correct, the RA will proceed to the signing of a legally binding instrument between the subscriber and/or the applicant and Firmaprofesional.
4.3.1. CA Actions during Certificate Issuance	CPS Section 6.2.3. Custody of the private key	For Root CA, ctivation and use of the private key requires the multiperson control, and the session is closed after the operation has been performed, so disabling the private key.
4.9.1.1 Reasons for Revoking a Subscriber Certificate Indicate how your CA's CP/CPS lists the reasons for revoking end entity certificates and is consistent with the timeframes required by this section of the BRs.	CPS Section 4.9.1 Grounds for revocation	Circumstances relating to the subscriber or signer: - Failure on the part of the subscriber or signer to adhere to the usage rules of the certificate set out in the CPS or the legally binding instrument between Firmaprofesional and the subscriber. - Termination of the legal relationship between Firmaprofesional and the Subscriber. - Modification or expiry of the underlying legal relationship or cause which allowed the issuance of the signer's certificate, including temporary professional disqualification. - Infringement by the certificate's applicant of the pre-agreed requirements the application. - Infringement by the subscriber with regard to their obligations, liabilities and guarantees established in the relevant legal documents or CPS. - Unexpected incapacity, either total or partial. - Death of the subscriber or signer. - Receipt of a valid revocation request issued by the subscriber or the signatory. - The authorization to be a payment service provider has been revoked by the ANC All subscriber certificates are revoked in a timeframe of 24 hours since receipt of a revocation request (ETSI requirement).

Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1		
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate <i>Indicate how your CA's CP/CPS lists the reasons for revoking subordinate CA certificates and is consistent with the timeframes required by this section of the BRs.</i>	CPS Section 4.9.1 Grounds for revocation	A certificate may be revoked for the following reasons: a. Circumstances affecting the information contained in the certificate b. Circumstances affecting the security of the private key or the certificate c. Circumstances affecting the security of the cryptographic device d. Circumstances relating to the subscriber or signatory e. Other circumstances
4.9.2. Who Can Request Revocation	CPS Section 4.9.2 Who can request revocation	Revocation may be requested by the signer or any person if they have knowledge of any of the circumstances mentioned.
4.9.3. Procedure for Revocation Request The CA SHALL publicly disclose the instructions through a readily accessible online means and in section 1.5.2 of their CPS.	CPS Section 4.9.3 Procedures for requesting revocation CP Autenticación Web 4.9.3 Revocation request procedures	There are various options for the subscriber or signer when requesting the revocation of a certificate: - Online procedure: Firmaprofesional has an online form available for the subscriber or signer where they can request revocation of their certificate. Once the operation has been approved, the certificate will be immediately revoked. - Revocation during office hours: The subscriber or the signer should contact their RA, who, in turn, must identify and authenticate their identity. Once correctly identified, the operator will execute the revocation. - Revocation outside of office hours: To request the revocation of a certificate outside of office hours contact Firmaprofesional's telephonic 24x7 Revocation Service. As a precautionary measure Firmaprofesional will suspend the certificate within 24 hours of receiving the request for revocation (for non website authentication certificates), and send a message to the RA with the suspension data and reason. The RA will have a maximum of 5 days to verify the authenticity of the revocation request and to complete the revocation. This term will be reduced to 24 hours in the following cases: - The subscriber requests in writing that Firmaprofesional revokes the certificate. - The subscriber notifies Firmaprofesional that they have not authorised the original certificate request and do not retroactively grant this authorisation. - Firmaprofesional obtains proof that the subscriber private key corresponding to the public key in the certificate has been compromised. - Firmaprofesional obtains evidence that the validation of the domain authorisation, or the control of any qualified domain name or IP address in the certificate cannot be trusted.
4.9.5. Time within which CA Must Process the Revocation Request		
4.9.7. CRL Issuance Frequency <i>Indicate if your CA publishes CRLs. If yes, then please test your CA's CRLs.</i>	CPS Section 4.9.7. Frequency of announcement of CRLs	The CRL of the end entity certificates are issued at least every 24 hours, or whenever a revocation occurs, and are valid for 7 days. The CRL of the certificates of authority is issued every 6 months or whenever a revocation occurs.
4.9.9. On-line Revocation/Status Checking Availability	CPS Section 4.9.9. Availability of the online system for verification of the status of certificates	Information concerning the status of the certificates will be available online 24 hours a day, 7 days a week. In case of system failure, or any other factor which is not under the control of the CA, every effort will be made to ensure that this information service is available within a maximum of 24 hours.
4.9.10. On-line Revocation Checking Requirements <i>Indicate how your CA meets all of the requirements listed in this section, including support of GET, update frequency (recently updated), and preventing erroneous return of "good" status.</i>	CPS Section 4.9.10. Requirements for checking revocation online	To use the CRL service, the following must be considered: - In all cases the last issued CRL must be checked, this can be downloaded from the URL contained in the certificate itself in the "CRL Distribution Point" extension. - The user should also check the CRL(s) related to the certification chain of the hierarchy - The user must ensure that the revocation list is signed by the authority that issued the certificate to be validated - Revoked certificates which expire will be removed from the CRL To use the OCSP service, the following must be considered: - The revocations can be checked using GET or POST methods - Information provided via OCSP service is updated at least every four days
4.9.12 "CA's CP/CPS MUST clearly specify the methods that parties may use to demonstrate private key compromise." (MRSP 6)	CPS Section 4.9.12. Special needs regarding a key compromise	A certificate is revoked if the security of the key or of the subscriber's certificate is compromised or suspected of having been compromised.
4.9.13 Certificate suspension must not be supported	CP Section 4.9.13 Circumstances for suspension	The suspension of any of the types of certificates contemplated in this policy is not allowed.
4.10.1. Operational Characteristics	CPS Section 4.10.1 Operational Characteristics	Firmaprofesional publishes Certificate Revocation Lists (CRLs) online, this service is free and with unrestricted access. Firmaprofesional offers a free online certificate verification service using the OCSP protocol.

Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1





4.10.2. Service Availability	CPS Section 4.10.2 Service Availability	Information concerning the status of the certificates will be available online 24 hours a day, 7 days a week.
5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS		
5.2.2. Number of Individuals Required per Task	CPS Section 5.2.2 Number of persons required per task	The CA guarantees at least two people to perform task that require multiperson control as detailed below: <ul style="list-style-type: none"> - Generation of the CA's keys. - Recovery and backup of the CA's private key. - Issuing the CA's certificates. - Activation of the CA's private keys. - Any activity performed on the hardware and software resources that support the Root CA.
5.3.1. Qualifications, Experience, and Clearance Requirements	CPS Section 5.3.1 Requirements for qualifications, knowledge and professional experience	All personnel who have been qualified as sufficiently trustworthy to perform tasks without supervision must have spent at least six months working in the production centre and have a fixed employment contract. All staff is qualified and have been fully trained to perform the operations to which they have been assigned.
5.3.3. Training Requirements and Procedures	CPS Section 5.3.3 Training requirements	Firmaprofesional provides the courses necessary to ensure the successful completion of the certification tasks, especially when substantial changes are made to them and dependent on the personal knowledge of each operator.
5.3.4. Retraining Frequency and Requirements	CPS Section 5.3.4 Requirements and frequency of training updates	Updates are made on an annual basis, except for changes to the CPS, which are notified as they are approved.
5.3.7. Independent Contractor Controls	CPS Section 5.3.7 Requirements for contracting third parties	Employees contracted to perform trusted task must first sign confidentiality clauses and also the operational requirements used by the CA.
5.4.1. Types of Events Recorded <i>Indicate how your CA meets the requirements of this section.</i>	CPS Section 5.4.1 Types of event recorded	Firmaprofesional logs all significant events so as to verify that all the internal procedures necessary to carry out its activities are executed as stipulated in this document, in applicable legislation and in the Internal Security Plan and Quality and Security Procedures, allowing the causes of any anomalies to be identified. These logged events will be made available, if necessary, so as to provide evidence of the proper functioning of the services for the purposes of court proceedings. The events logged include all operations carried out during the management of keys, Certificates, Electronic time stamp issuance, Certificate status information, publication, filing, recovery, directory, event logs and user logs. Firmaprofesional will archive all the most important events logged and will keep them accessible for a period of not less than 15 years.
5.4.3. Retention Period for Audit Logs	CPS Section 5.4.3 Retention period of the audit logs	To ensure system security audit log information are stored for 15 years.
5.4.8. Vulnerability Assessments <i>Indicate how your CA meets the requirements of this section.</i>	CPS Section 5.4.7 Vulnerability Assessments	In accordance with the internal procedure established for this purpose in the security policies, the CA performs periodic reviews of discrepancies in the information in the logs and of suspicious activity, as well as vulnerability assessments of internal and external IP addresses.
5.5.2. Retention Period for Archive	CPS Section 5.5.2 Period for the conservation of records	All system data related to the lifecycle of the certificates will be kept for the period specified by the current law, whenever it is applicable. Certificates will be kept in the repository for at least one year after their expiration. The contracts with the subscribers and any information concerning the identification and authentication of subscribers will be retained for at least 15 years (from the time of expiry of the certificate) or the period established by the applicable legislation.
5.7.1. Incident and Compromise Handling Procedures <i>Indicate how your CA meets the requirements of this section, including notifying Mozilla in the event of key compromise.</i>	CPS Section 5.7.1 Procedures for the management of incidents and vulnerabilities	The CA has developed a contingency plan, detailed in the "Security Policy" document, for the recovery of all systems in less than 48 hours, while the revocation and publication of information on the status of certificates is guaranteed in less than 24 hours.
6.1.1. Key Pair Generation	CPS Section 6.1.1 Key Pair Generation	The key generation of the CAs is performed on Hardware Security Modules (HSM) located within the security room of the CSP. It is carried out by staff deemed appropriate according to their trusted roles and, with at least one dual control and witnesses from Firmaprofesional, the head organisation of the CA and the external auditor.
6.1.1.3 Subscriber Key Pair Generation - the CA SHALL NOT generate a Key Pair on behalf of a Subscriber, and SHALL NOT accept a certificate request using a Key Pair previously generated by the CA.	CP Website Authentication Certificates Section 6.1.1. Key Pair Generation	Signature keys are generated within the applicant systems using their own compatible applications with the PKI standards.
6.1.2. Private Key Delivery to Subscriber	CPS Section 6.1.2 Private key delivery to the signer	The RA is responsible for ensuring the delivery of the certificate to the signatory, whether by delivering the signature device or making available the means for its download and subsequent use, ensuring that the signatory is in possession of the signature creation data corresponding to the verification data which appears in the certificate.


Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1



6.1.5. Key Sizes	CPS Section 6.1.5 Key Sizes CP Website Authentication Certificates Section 6.1.5. Key size	The Key size, depending on each case, is: - Root CA: 4096 bits - Subordinate CA: 2048 bits - End entity: 2048 bits
6.1.6. Public Key Parameters Generation and Quality Checking	CPS Section 6.1.6 Public key parameters generation and quality checking	The parameters recommended in the technical specifications document ETSI TS 119 312 are used. Specifically the parameters used are the following: - Signature Suite: sha256-with-rsa - Hash Function: sha256 - Padding Method: emsa-pkcs1-v1.5 - Signature algorithm: rsa
6.1.7. Key Usage Purposes	CPS Section 6.1.7. Acceptable key usage (as per the Key Usage Field of X.509 v3)	All certificates include the extension Key Usage and Extended Key Usage, indicating authorised uses of the key. Permitted uses of the key for each certificate are defined in the corresponding Certification Policy.
6.2. Private Key Protection and Cryptographic Module Engineering Controls	CPS Sections 6.2.1 Cryptographic Module Standards and 6.2.2 Private Key (m out of n) multi-person control	The cryptographic modules used to generate and store the keys of the CA are certified with the FIPS-140-2 standard Level 3. Access to private keys of the CA requires the simultaneous participation of two different cryptographic devices out of a possible five, protected by a password.
6.2.5. Private Key Archival	CPS Section 6.2.5 Private Key Archival	The CA will not archive the private signing key for certificates after the expiration of their validity period. The private keys of the internal certificates used by the distinct components of the CA's system to communicate with each other, to sign and to encrypt the information will be archived for a period of at least 10 years after the last certificate has been issued. No other parties archive the CA's private keys.
6.2.6. Private Key Transfer into or from a Cryptographic Module	CPS Section 6.2.6 Private key transfer into or from a cryptographic module	There is a CA key ceremony document which describes the processes for generating the private key and the use of the cryptographic hardware that guarantees the security of the keys.
6.2.7. Private Key Storage on Cryptographic Module	CPS Sections 6.2.1 Cryptographic Module Standards and 6.2.7 Method for activating the private key	The cryptographic modules used to generate and store the keys of the CA are certified with the FIPS-140-2 standard Level 3.
6.3.2 Certificates issued SHOULD NOT have a Validity Period greater than 397 days and MUST NOT have a Validity Period greater than 398 days . Indicate how your CA meets the requirements of this section.	CPS Section 6.3.2 Periods for certificate operation and key pair usage CP Website Authentication Certificates Section 1.4.1.1. Certificates validity period	The periods of use of the keys will be those determined by the duration of the certificate, and once they have elapsed, they will not be able to continue using. Validity period will be indicated within the certificate, up until a maximum of 1 (one) year for all Website Authentication certificates
6.5.1. Specific Computer Security Technical Requirements The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance. <i>Indicate how your CA meets the requirements of this section.</i>	CPS Section 6.5.1 Specific security technical requirements	Each server of the CA includes the following features: - Access control to the CA services and privilege management. - Imposition of separation of duties for the management of privileges. - Identification and authentication of roles associated with identities. - Archive of the history file of the subscribers, the CA and the audit data. - Audit events related to security. - Self-diagnosis of security related to the CA services. - Mechanisms for recovery of keys and the CA system. All accounts capable of directly causing certificate issuance are configured with multi-factor authentication to access to the RA or CA applications.
7.1. Certificate profile CAs SHALL generate non-sequential Certificate serial numbers greater than 0 containing at least 64 bits of output from a CSPRNG. <i>Indicate how your CA meets the requirements of this section.</i>	CPS Section 7.1 Certificate Profile	The profile of certificates is consistent with those set out in the following standards: - ETSI 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles - RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" - RFC 3739 "Qualified Certificates Profile" The serialNumber is a unique random code with respect to the issuer's DN with at least 64 bits of entropy.
7.1.1. Version Number(s)	CPS Section 7.1.1 Version Number	The certificates follow standard X.509 version 3.

Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1		
7.1.2. Certificate Content and Extensions; Application of RFC 5280	CPS Section 7.1 Certificate Profile and 7.1.2. Certificate extensions Profiles of Certificates Version: 210322	The profile of certificates is consistent with those set out in the following standards: - ETSI 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles - RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" - RFC 3739 "Qualified Certificates Profile"
7.1.2.1 Root CA Certificate	CPS Section 1.3.1.1 and following	Firmaprofesional meets the requirements.
7.1.2.2 Subordinate CA Certificate	CPS Section 1.3.1.1 and following	Firmaprofesional meets the requirements.
7.1.2.3 Subscriber Certificate	CPS Section 7.1 Certificate Profile Profiles of Certificates Version: 210322	Firmaprofesional meets the requirements.
7.1.2.4 All Certificates	CPS Section 7.1 Certificate Profile Profiles of Certificates Version: 210322	Firmaprofesional meets the requirements.
7.1.2.5 Application of RFC 5280	CPS Section 7.1 Certificate Profile	The profile of certificates is consistent with those set out in the following standards: - ETSI 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles - RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" - RFC 3739 "Qualified Certificates Profile"
7.1.3. Algorithm Object Identifiers	CPS Section 7.1.3. Object identifiers (OID) of the algorithms used	Firmaprofesional declares that during their validity periods the keys of the signatory or subscriber created by the CA are generated using an algorithm recognised as appropriate for the uses identified in this CPS or in the corresponding CP.
7.1.3.1 SubjectPublicKeyInfo	CPS Section 7.1.3. Object identifiers (OID) of the algorithms used	The object identifier (OID) relating to the cryptographic algorithm used (RSA) is 1.2.840.113549.1.1.1.
7.1.3.2 Signature AlgorithmIdentifier	CPS Section 7.1.3. Object identifiers (OID) of the algorithms used	The object identifier (OID) relating to the cryptographic algorithm used (SHA-256 with RSA Encryption) is 1.2.840.113549.1.1.11.
7.1.4. Name Forms	CPS Section 7.1.4 Name Formats	The Certification Entity will fill in the names fields of the certificates with the information established in the corresponding certificate profile.
7.1.4.1 Name Encoding - Subject and Issuer Names for all possible certification paths MUST be byte-for-byte identical	CPS Section 7.1 Certificate Profile	The profile of certificates is consistent with those set out in the following standards: - ETSI 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles - RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" - RFC 3739 "Qualified Certificates Profile"
7.1.4.2 Subject Information - Subscriber Certificates		
7.1.4.2.1 Subject Alternative Name Extension This extension MUST contain at least one entry. Each entry MUST be either a dNSName containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server. The CA MUST confirm that the Applicant controls the Fully-Qualified Domain Name or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate. Wildcard FQDNs are permitted. CAs SHALL NOT issue certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name. Entries in the dNSName MUST be in the "preferred name syntax", as specified in RFC 5280, and thus MUST NOT contain underscore characters ("_").	CPS Section 7.1 Certificate Profile and Profiles of Certificates Section 4. Description of the Profiles of the Website Authentication Certificates	The profile of certificates is consistent with those set out in the following standards: - ETSI 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles - RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" - RFC 3739 "Qualified Certificates Profile" The Subject Alternative Name Extension includes only dNSName fields containing the FQDNs verified and formatted as specified in RFC 5280.
7.1.4.2.2 Subject Distinguished Name Fields If present, this field MUST contain a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension (see Section 7.1.4.2.1).	CPS Section 7.1 Certificate Profile and Profiles of Certificates Section 4. Description of the Profiles of the Website Authentication Certificates	The profile of certificates is consistent with those set out in the following standards: - ETSI 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles - RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" - RFC 3739 "Qualified Certificates Profile" The Website authentication certificates includes the subject:commonName with a FQDN that is one of the values contained in the Certificate's subjectAltName extension.

Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1		
7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates	CPS Section 7.1 Certificate Profile	The profile of certificates is consistent with those set out in the following standards: - ETSI 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles - RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" - RFC 3739 "Qualified Certificates Profile"
7.1.5. Name Constraints <i>Indicate your CA's understanding of section 5.3 of Mozilla's root store policy, and requirement to disclose in the CCADB all subordinate CA certificates that are not technically constrained as described in this section of the BRs.</i> <i>"All certificates that are capable of being used to issue new certificates, that are not technically constrained, and that directly or transitively chain to a certificate included in Mozilla's root program: MUST be audited in accordance with Mozilla's Root Store Policy. ... MUST be publicly disclosed in the CCADB by the CA that has their certificate included in Mozilla's root program. The CA with a certificate included in Mozilla's root program MUST disclose this information within a week of certificate creation, and before any such subordinate CA is allowed to issue certificates. ..."</i>	CPS Section 7.1.5. Name restrictions	All certificates that are capable of being used to issue new certificates are audited in accordance with Mozilla's Root Store Policy.
7.1.6. Certificate Policy Object Identifier		
7.1.6.1 Reserved Certificate Policy Identifiers	CPS Section 7.1.6. Certificate policy object identifier (OID)	Firmaprofesional uses the next Reserved Certificate Policy Identifiers: - ca-browser-forum.certificate-policies.baseline-requirements.organization-validated: 2.23.140.1.2.2 - ca-browser-forum.certificate-policies.extended-validation: 2.23.140.1.1
7.1.6.2 Root CA Certificates	CPS Section 7.1. Certificate profile	Root CA Certificates do not include reserved Certificate Policy Identifiers.
7.1.6.3 Subordinate CA Certificates	CPS Section 7.1. Certificate profile	Subordinate CA Certificates do not include reserved Certificate Policy Identifiers.
7.1.6.4 Subscriber Certificates Certificates MUST contain "one or more policy identifier(s) that are specified beneath the CA/Browser Forum's reserved policy OID arc of {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum (140) certificate-policies(1)} (2.23.140.1)."	CPS Section 7.1. Certificate profile and CP Section 5.1	Subscriber Certificates contain one of the next Reserved Certificate Policy Identifiers: - ca-browser-forum.certificate-policies.baseline-requirements.organization-validated: 2.23.140.1.2.2 - ca-browser-forum.certificate-policies.extended-validation: 2.23.140.1.1
7.2 and 7.3 - All OCSP and CRL responses for Subordinate CA Certificates MUST include a meaningful reason code.	CPS Section 7.2. Profile of the CRL CPS Section 7.3. Profile of the OCSP CPS Section 4.9.3.1. Online procedure	CRL ReasonCode and OCSP RevocationReason indicated are not unspecified (0). The subscriber must enter the reason for the revocation request.
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS		
8.1. Frequency or circumstances of assessment The period during which the CA issues Certificates SHALL be divided into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration. For new CA Certificates: The point-in-time readiness assessment SHALL be completed no earlier than twelve months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate. <i>Indicate your CA's understanding of this requirement, and how your CA meets the requirements of this section.</i>	CPS Section 8.1 Frequency of audits	Periodic audits are carried out, usually on an annual basis.
8.2. Identity/qualifications of assessor <i>Indicate how your CA meets the requirements of this section.</i>	CPS Section 8.2 Qualification of the auditor	Audits can be either internal or external. In this latter case they are carried out by companies well known in the auditing field. In the case of external compliance audits of eIDAS, Firmaprofesional will perform them with a CAB (Conformity Assessment Body). For audits of compliance with the CA / Browser Forum requirements, Firmaprofesional will perform them with an organization accepted by the Mozilla Foundation for this purpose.

Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1		
8.4. Topics covered by assessment	CPS Section 8.4 Aspects covered by the controls	<p>The audit will verify the following principles:</p> <ul style="list-style-type: none"> - Publication of information - Service integrity - General controls <p>Firmaprofesional undergo an audit in accordance with ETSI EN 319 411-1 and ETSI EN 319 411-2, which includes normative references to ETSI EN 319 401.</p>
<p>8.6. Communication of results</p> <p>The Audit Report must contain certain information formatted in a certain way, including but not limited to:</p> <ul style="list-style-type: none"> - name of the company being audited; - name and address of the organization performing the audit; - Distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope; - audit criteria (with version number) that were used to audit each of the certificates; - a list of the CA policy documents (with version numbers) referenced during the audit; - whether the audit is for a period of time or a point in time; - the start date and end date of the period, for those that cover a period of time; - the point-in-time date, for those that are for a point in time; - the date the report was issued (which will necessarily be after the end date or point-in-time date); and - For ETSI, a statement to indicate if the audit was a full audit, and which parts of the criteria were applied, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part1 (General Requirements), and/or Part 2 (Requirements for trust service providers). <p>Also indicate your understanding and compliance with section 3 of Mozilla's Root Store Policy, which says: "Full-surveillance period-of-time audits MUST be conducted and updated audit information provided no less frequently than annually. Successive audits MUST be contiguous (no gaps)."</p>	CPS Section 8.6 Reporting of Results	<p>The auditor shall pass on the results to the Technical Director and the Director-General, as well as the person with ultimate responsibility in Firmaprofesional.</p> <p>The audit reports are publicly available and include all required information.</p>
<p>8.7. Self-Audits</p>	Not disclosed in the CPS as a separate section	<p>In the case of external compliance audits of eIDAS, Firmaprofesional will perform them with a CAB (Conformity Assessment Body).</p> <p>For audits of compliance with the CA / Browser Forum requirements, Firmaprofesional will perform them with an organization accepted by the Mozilla Foundation for this purpose.</p> <p>Firmaprofesional understands section 3 of Mozilla's Root Store Policy and transmits it to the auditors. All audits are contiguous (without gaps).</p>
9.6.1. CA Representations and Warranties	CPS Section 9.6.1 Obligations of the CA	<p>Firmaprofesional is obliged to issue certificates in accordance with this CPS and the application standards, to issue certificates according to the information at its disposal, free of errors in the entered data, and to issue certificates whose minimum content is defined by the current regulations, when applicable. So, Firmaprofesional makes the needed warranties.</p>
9.6.3. Subscriber Representations and Warranties	CPS Section 9.6.3 Obligations of the applicants	<p>An applicant for a certificate is required to comply with the rules and also to provide the RA the information necessary to carry out the proper identification, to confirm the accuracy and veracity of the information provided, To report any change in the data provided for the creation of the certificate during its period of validity and to respect the provisions of the contractual documents signed with the CA and the RA.</p>
9.8. Limitations of liability	CPS Section 9.8.4 Limitation of liabilities	<p>Firmaprofesional will not be liable in any case where the following circumstances are encountered:</p> <ul style="list-style-type: none"> - State of war, natural disasters, malfunction of electrical services, data transfer and/or telephonic networks or computer equipment used by the Subscriber or by third parties, or any other act of God. - By improper or fraudulent use of the certificate directory and CRL issued by the Certification Authority. - For misuse of the information contained in the Certificate or CRL - For the content of messages or documents signed or encrypted using the certificates. - With regard to actions or omissions of the Applicant and Subscriber. - With regard to actions or omissions of the relying party.
9.9.1. Indemnification by CAs	CPS Section 9.9.1 Extent of the coverage	<p>Up to the limit of the contracted coverage the insurance will take care of any amounts which Firmaprofesional SA is legally obliged to pay as a result of any legal proceedings in which it can declare its liability, arising from any negligent act, error or unintentional breach of the current legislation among others.</p>
9.16.3. Severability	CPS Section 9.16.3 Resolution by legal means	<p>Any controversy or dispute arising from the present document, will be ultimately settled by means of legal arbitration by an arbitrator, within the framework of the Spanish Court of Arbitration and in accordance with its Rules and Regulations.</p>

Updated April 2021 to match BR v. 1.7.4 and Mozilla Root Store Policy v. 2.7.1



<p>APPENDIX A - RFC 6844 ERRATA 5065 To prevent resource exhaustion attacks, CAs SHOULD limit the length of CNAME chains that are accepted. However CAs MUST process CNAME chains that contain 8 or fewer CNAME records.</p>		<p>CAA records are performed automatically according to RFC 6844 ERRATA 5065</p>
<p>APPENDIX B – CAA CONTACT TAG These methods allow domain owners to publish contact information in DNS for the purpose of validating domain control.</p>		<p>Not used.</p>
<p>APPENDIX C - Issuance of Certificates for .onion Domain Names</p>		<p>Firmaprofesional does not issue certificates for .onion Domain Names.</p>