Updated April 2019 to match BR version 1.6.4

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

Introduction must include:
1) CA's Legal Name:
Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)
2) CA hierarchy.
ROOT 1: AC RAIZ FNMT-RCM SERVIDORES SEGUROS / 554153B13D2CF9DDB753BFBE1A4E0AE08D0AA4187058FE60A2B862B2E4B87BCB
INTERMEDIATE 1.1: AC SERVIDORES SEGUROS TIPO1 / 1EDB6BD91274882DB795BFC514F8AABE10AD955CBCCFD3FD5A5B5FEBB2CE5B68 - Issues: QCP-w. Not restricted by EKU extension
INTERMEDIATE 1.2: AC SERVIDORES SEGUROS TIPO2 / 9FF23CB9387B9E0083BD5AA1954EEDDF792890AA8E67CD4D38DD28AF4A439AD8 - Issues: OVCP certificates. Not restricted by EKU extension
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.
Compliant with CA-Browser Forum BR v.1.6.5
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.
All the CP/CPS documents are made available at https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion.
-TRUST SERVICES PRACTICES AND ELECTRONIC CERTIFICATION GENERAL STATEMENT (v.5.4): https://www.sede.fnmt.gob.es/documents/10445900/10536309/dpc_ss_english.pdf
- CERTIFICATION PRACTICES AND POLICIES STATEMENT ON WEBSITE AUTHENTICATION CERTIFICATES (v.1.1): https://www.sede.fnmt.gob.es/documents/10445900/10536309/dpc_ss_english.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 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, *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.*	CPS: Version 5.4 Effective date: March 05, 2019 CP: Version 1.1 Effective date: May 30, 2019	The current CPS is compliant with the requirements The CP and CPS are aligned to BR 1.6.5 as of effective date April 16, 2019 and in accordance with RFC 3647
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, *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.*	CPS: Version 5.4 Effective date: March 05, 2019 CP: Version 1.1 Effective date: May 30, 2019	Compliant.
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. *Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.*	CPS and CP Section 1.3.2 Registration Authority CPS Section 5.2. Procedure Controls CPS and CP Section 9.6.2 RA's obligations CP Section 4.1.2. Registration process and responsibilities	Compliant. Delegated Registration Authorities are not allowed.
2.1. Repositories *Provide the direct URLs to the CA's repositories*	CPS and CP Section 2.1 Repository	Compliant. CPS documents repository: https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion CPS Document: https://www.sede.fnmt.gob.es/documents/10445900/10536309/dgpc_english.pdf CP, PDS etc.. document repository: https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-1 https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-2 Public access to hierarchy certificate download: https://www.sede.fnmt.gob.es/en/descargas
2.2 Publication of information - RFC 3647 "Effective as of 31 May 2018, the Certificate Policy and/or Certification Practice Statement **MUST be structured in accordance with RFC 3647**."	CPS Section 5. PHYSICAL SECURITY, PROCEDURE AND PERSONNEL CONTROLS	Compliant. The CP and CPS are aligned and in accordance with RFC 3647
2.2 Publication of information - CAA Effective as of 8 September 2017 ... 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.**	CP Section 4.2.2. Approval or denial of the certificate request	Compliant. The FNMT-RCM checks to confirm that there is a CAA Record for each domain name that it includes in any Website authentication certificate, in accordance with the procedure established under the terms of RFC 6844 and following the processing instructions set forth in RFC 6844 for any record may be found. In the event that such CAA Record exists, no Certificate will be issued unless it is determined that the Certificate request is consistent with the applicable CAA resource record group. The issuer domain name recognized for the FNMT-RCM CAA Record is "fnmt.es"
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 9.17. OTHER STIPULATIONS CP Section 9.6.1. CA's obligations	Compliant. The FNMT-RCM manages its certification services and issues Certificates in accordance with the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", established by the entity CA/Browser forum, which may be consulted at the following address: https://cabforum.org/baseline-requirements-documents and in accordance with the latest version of the requirements defined by the entity CA / Browser forum in its "Guidelines for the Issuance and Management of Extended Validation Certificates" (which can be consulted at the address https://cabforum.org/extended-validation/). " and The FNMT-RCM issues the Website authentication certificate in accordance with the “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”, established by the entity CA/Browser forum, which may be consulted at the following address: https://cabforum.org/ Likewise, it will adapt its issuance practices for these Certificates to the version of the aforementioned requirements currently in effect. In the event of any inconsistency between this DPPP and the aforementioned version, said requirements shall prevail over those contained in 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.***		Pending. We are implementing the necessary modifications to align the profile to EV Guidelines 1.6.9.- Ballot SC16 of 16 Apr 2019 (Removal of the OrganizationIdentifier field from the Subject) as to be able to generate new EV test websites Until then, the following OV test websites are available. https://testactivetipo2.cert.fnmt.es https://testrevokedtipo2.cert.fnmt.es https://testexpiredtipo2.cert.fnmt.es
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. Section 3.3 of Mozilla's Root Store Policy states: "CPs and CPSes MUST be reviewed and updated as necessary at least once every year, as required by the Baseline Requirements. **CAs MUST indicate that this has happened by incrementing the version number and adding a dated changelog entry**, even if no other changes are made to the document." *Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.*	CPS and CP Section 1.5.4 General Statement approval procedure CPS and CP Section 2.3 Publication frequency	Compliant. The FNMT-RCM review its certification policies and practices and annually update both the CPS and CP. BRs and CA/B Forum Extended Validation SSL Guidelines requirements are also regulary reviewed and consecuently CPS and CP modified accordingly when needed.

2.4. Access controls on repositories *Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.*	CPS and CP Section 2.4 Repository access control	Compliant. All FNMT-RCM repositories are freely accessible for information consultation and, if applicable, download purposes. Moreover, the FNMT-RCM has put in place controls to prevent unauthorised persons from adding, altering or deleting information included in its repositories and to protect the authenticity and integrity of the information.
3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	CPS and CP Section 3.2.2. Authentication of the organisation's identity	Compliant. In cases where the Subscriber is a private entity, its existence, which is legally recognised, active at that moment, and formally registered, will be verified by direct consultation by the RA of the FNMT-RCM using service that the Mercantile Registry provides for this purpose. For cases of public entities, such verification will be carried out by direct consultation of the RA of the FNMT-RCM of the inventory of public sector entities contained at the General Intervention Board of the State Administration, under the Ministry of Finance, or in the corresponding Official Gazette. If the nature of the Subscriber is different from the two previous examples, verifications related to its legal capacity and identity will be made by direct consultation with the corresponding official registry. The FNMT-RCM does not issue Website authentication certificates for Subscribers who are individuals.
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	CPS Section 3.1.6. Registered trademark recognition and authentication	Compliant. Certificates including tradenames may only be requested when the Holder owns the right of use or is authorised to use it.
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	CPS and CP Section 3.2 INITIAL VALIDATION OF IDENTITY	Compliant. Verification of the identity and more especifically those concerning the country, are checked against publications in Official State Gazettes and Regional Government Gazettes, public registers and registers accessible to the FNMT-RCM (e.g.Official Mercantile Registry, INVENTE, etc...)
3.2.2.4 Validation of Domain Authorization or Control *Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS.* ***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)."***	CPS Section 3.2 INITIAL VALIDATION OF IDENTITY CP Section 3.2.7. Domain validation	Compliant. FNMT-RCM uses one of the following methods described in the CA/Browser Forum's Baseline Requirements document: "3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact", "3.2.2.4.4 Constructed Email to Domain Contact" or "3.2.2.4.7 DNS Change".
3.2.2.4.1 Validating the Applicant as a Domain Contact For certificates issued on or after August 1, 2018, **this method SHALL NOT be used** for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates.	This method is not used.	
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact 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.*	CP Section 3.2.7. Domain validation	Compliant. FNMT-RCM's RA emails the Domain contact with a random reference to confirm the aplicants control over the FQDN
3.2.2.4.3 Phone Contact with Domain Contact **CAs SHALL NOT perform validations using this method after May 31, 2019**. Completed validations using this method SHALL continue to be valid for subsequent issuance per the applicable certificate data reuse periods.	This method is not used.	
3.2.2.4.4 Constructed Email to Domain Contact 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.*	CP Section 3.2.7. Domain validation	Compliant. FNMT-RCM's RA sends an email to 'admin', 'administrator', 'webmaster', 'hostmaster', and 'postmaster' followed by @ and followed by the Authorization Domain Name. This email includes a random reference which is expected to be included in the response confirming the aplicants control over the FQDN.
3.2.2.4.5 Domain Authorization Document "For certificates issued on or after August 1, 2018, **this method SHALL NOT be used** for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates."	This method is not used.	This method is not used.
3.2.2.4.6 Agreed-Upon Change to Website 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.*	This method is not used.	This method is not used.
3.2.2.4.7 DNS Change 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.*	CP Section 3.2.7. Domain validation	Compliant. FNMT-RCM's RA checks the presence of the Request Token in the DNS TXT record for confirming the applicants control over the FQDN
3.2.2.4.8 IP Address 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.*	This method is not used.	This method is not used.
3.2.2.4.9 Test Certificate **"This method has been retired and MUST NOT be used."**	This method is not used.	This method is not used.
3.2.2.4.10. TLS Using a Random Number 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.* *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.***	This method is not used.	This method is not used.
3.2.2.4.11 Any Other Method **"This method has been retired and MUST NOT be used."**	This method is not used.	This method is not used.
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." 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* .	This method is not used.	This method is not used.
3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, ***indicate which methods your CA uses*** *and how your CA meets the requirements in this section of the BRs.* **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."**	CP Section 3.2.7. Domain validation and CP Section 3.2.8. Recognition and Identification of IP addresses	Compliant. This method is not used. Ip addresses are not to be listed in certificates.
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 *indicate how your CA meets the requirements in this seciton of the BRs.*	CP Section 3.2.7. Domain validation	Compliant. FNMT-RCM validate the full control of the organization over the entire Domain Namespace. For those Certificates that incorporate more than one domain name (SAN Certificates and Wildcard OV Certificate), the corresponding checks will be made for each individual domain name included in the Certificate. In the event that any these domain names do not meet the requirements, after a verification process using the checks performed, the Certificate will not be issued.
3.2.2.7 Data Source Accuracy *Indicate how your CA meets the requirements in this section of the BRs.*	CPS Section 3.2 INITIAL VALIDATION OF IDENTITY	Compliant. FNMT-RCM's only accepts document sources from public and official registers
3.2.2.8 CAs MUST check and process CAA records *Indicate how your CA meets the requirements in this section of the BRs.* *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."***	CP Section 4.2.2. Approval or denial of the certificate request	Compliant. The FNMT-RCM checks to confirm that there is a CAA Record for each domain name that it includes in any Website authentication certificate, in accordance with the procedure established under the terms of RFC 6844 and following the processing instructions set forth in RFC 6844 for any record may be found. In the event that such CAA Record exists, no Certificate will be issued unless it is determined that the Certificate request is consistent with the applicable CAA resource record group. The issuer domain name recognized for the FNMT-RCM CAA Record is "fnmt.es"

3.2.3. Authentication of Individual Identity	CP Section 3.2.3 Authentication of the individual applicant's identity	Compliant. The FNMT-RCM's RA verifies that the Subscriber Representative matches with the individual requesting a Website authentication certificate, by means of the electronic signature of the application form using a verified Certificate of electronic signature, thus guaranteeing the authenticity of their identity
3.2.5. Validation of Authority	CP Section 3.2.5. Verification of capacity to represent	Compliant. The FNMT-RCM's RA verifies that the Applicant has been granted sufficient representation capacity through the electronic signature of the application form, as described in section 3.2.3 of this DPPP, accepting the use of a qualified Certificate of sole or joint administrator representative of the subscribing legal person or a qualified Certificate of Personnel at the service of the Public Administration, for whose issuance the capacity of representation has been accredited.
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	CPS and CP Section 3.2.6. Interoperation criteria	Compliant. FNMT doesn't use cross certificates. There are no interoperational relationships with Certification Authorities external to FNMT-RCM
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	CP Section Section 4.1.1. Who may request a Certificate? CP Section 4.2.2. Approval or denial of the certificate request CPS Section 9.6.1.4 Preservation of information by the FNMT-RCM	Compliant. Only Subscriber representatives who have demonstrated control over the name of the domain to be included in the Certificate are able to request Website authentication certificates. The aforementioned control over the domain name will be verified by the FNMT-RCM as described in section "3.2 Initial Validation of Identity" The FNMT-RCM maintains an internal database of all revoked Certificates and all requests for Certificates that were previously rejected due to suspected phishing or other forms of fraudulent use. This information is then taken into account to identify subsequent requests for Suspicious certificates before proceeding with the approval of the issuance thereof
4.1.2. Enrollment Process and Responsibilities	CP Section 4.1.2. Registration process and responsibilities	Compliant. The Applicant shall send a certificate request and a electronically signed contract by the Subscribing Representative accepting the terms of use and obligations in order to start the application procedure. The RA of the FNMT-RCM performs the verification of the identity of the subscribing Organisation and of the Subscriber Representative, and verifies that the application for the Certificate is correct and duly authorised, in accordance with the requirements contained in section "3.2 Initial Validation of identity" of the CP. The FNMT-RCM may carry out additional verification on the validation processes described in the aforementioned section.
4.2. Certificate application processing	CP Section 4.2. CERTIFICATION APPLICATION PROCEDURE	
4.2.1. Performing Identification and Authentication Functions *Indicate how your CA identifies high risk certificate requests.* **Re-use of validation information is limited to 825 days**	CP Section 3.2.5. Verification of capacity to represent CP Section 3.2.7. Domain validation CP Section 4.2.1. Performance of identification and authentication functions CP Section 4.2.2. Approval or denial of the certificate request	Compliant. The FNMT-RCM maintains an internal database of all revoked Certificates and all requests for Certificates that were previously rejected due to suspected phishing or other forms of fraudulent use. This information is then taken into account to identify subsequent requests for Suspicious certificates before proceeding with the approval of the issuance thereof. Before issuing a Website authentication certificate, it is verified that the domain to be included in the Certificate is public (i.e. it is not an internal domain) and public records are consulted to verify that it is not a high risk domain (for example, the Google registry created for this purpose, or the Safe Browsing site status). The validity of the evidence obtained as a result of the consultations carried out for the authentication of the identity of the Organisation and/or the authentication of the identity of the requesting natural person, according to sections 3.2.2 and 3.2.3 of this document, will be the validity of the Certificate to be issued, at a maximum. The certificate validity is in any case no longer than 825 days. Therefore, if there is an active Certificate and the issuance of another Certificate of the same type and for the same Subscriber and domain name(s) is requested, it will not be necessary to obtain the aforementioned identification evidence from the subscribing organisation of the Certificate and/or of the identity of the requesting individual.
4.2.2. Approval or Rejection of Certificate Applications "Within 30 days after ICANN has approved a new gTLD for operation, as evidenced by publication of a contract with the gTLD operator on [www.ICANN.org] each CA MUST (1) compare the new gTLD against the CA's records of valid certificates and (2) cease issuing Certificates containing a Domain Name that includes the new gTLD until after the CA has first verified the Subscriber's control over or exclusive right to use the Domain Name in accordance with Section 3.2.2.4. Within 120 days after the publication of a contract for a new gTLD is published on [www.icann.org], CAs MUST revoke each Certificate containing a Domain Name that includes the new gTLD unless the Subscriber is either the Domain Name Registrant or can demonstrate control over the Domain Name."	CP Section 4.2.2. Approval or denial of the certificate request	Compliant. The FNMT-RCM maintains an internal database of all revoked Certificates and all requests for Certificates that were previously rejected due to suspected phishing or other forms of fraudulent use. This information is then taken into account to identify subsequent requests for Suspicious certificates before proceeding with the approval of the issuance thereof. No certificates for gTLDs under consideration are issued.
4.3.1. CA Actions during Certificate Issuance	CPS Section 6.4.2. Activation data protection CP Section 4.3.1. CA actions during issuance	Compliant. FNMT-RCM physical and logical environment has a dual role access control. Root keys are offline and the activation data for the Certification Authorities' Private keys are protected using the method described in paragraph "6.2.8 Private key activation method" of CPS, including multi-person access based on cryptographic cards and related PINs in a simultaneous use M of N (2 of 5) system. Once the application for the Certificate has been approved by the RA of the FNMT-RCM's, the system then performs certain checks, such as the size of the Public key generated and CAA record checking, and proceeds to issue the Certificate according to the profile approved for each corresponding type of Certificate. The processes related to the issuance of electronic Certificates guarantee that all the accounts that interact with them include multi-factor authentication

4.9.1.1 Reasons for Revoking a Subscriber Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking certificates.*	CP Section 4.9 REVOCATION AND SUSPENSION OF CERTIFICATE CP Section 4.9.1. Circumstances for revocation	Compliant. Web Authentication certificates issued by the FNMT-RCM will cease to be valid in the following cases: a) Termination of the Certificate's validity period. b) Discontinuance of the FNMT-RCM's activities as a Trust Service Provider unless, upon express previous consent of the Subscriber, the Certificates issued by the FNMT-RCM are transferred to a different Trust Service Provider. In these two cases [a) and b)], the loss of the Certificate's effectiveness will occur as soon as the circumstances arise. c) Revocation of the Certificate due to any of the causes stipulated in this document. In addition the following will be causes for revocation of a Website authentication certificate: a) The request for revocation by authorised individuals. The following may give rise to this request: • Loss of support of the Certificate. • Use of the Private Key associated with the Certificate by a third party. • Any violation or endangerment of the details of the Private Key associated with the Certificate. • The non-acceptance of new conditions that may imply the issuance of new Certification Practices Statement, during the period of one month subsequent to its publication. b) Judicial or administrative resolution ordering such request. c) Termination, deletion, or closure of the website identified by the Certificate. d) Extinction or dissolution fo the legal personality of the Subscriber. e) Termination of the form of representation of the Certificate Subscriber representative. f) Total or partial supervening lack of capacity of the Subscriber's representative. g) Inaccuracies in the data provided by the Subscriber's Representative in order to obtain the Certificate, or alteration of any of the data provided to obtain the Certificate, or modification of the verified information relating to the issuance of the Certificate, so that it is no longer in accordance with reality. h) Violation of a substantial obligation of this Certification Practices Statement by the Subscriber, the Subscriber Representative or a Registry Office, in the event that, in the latter case, this might have potentially affected the procedure for issuing the Certificate. i) Use the Certificate with the purpose of generating doubt for users regarding the origin of the products or services offered, indicating that their origin is different from
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking subordinate CA certificates.*	CP Section 4.9. REVOCATION AND SUSPENSION OF CERTIFICATE	Compliant. We do not issue subCAS for third party exploitation
4.9.2. Who Can Request Revocation	CP Section 4.9.2. Who may apply for revocation	Compliant. The revocation of a Website authentication certificate may only be requested by the person with powers of representation of the Subscriber to whom the Certificate has been issued and the FNMT-RCM itself in cases included in the CP
4.9.3. Procedure for Revocation Request	CP Section 4.9.3. Revocation application procedure	Compliant. There is a 24/7 service available at phone number 902 200 616, to which applications for the revocation of Website authentication certificates can be addressed. The communication will be recorded and registered, to be used as support and guarantee of the acceptance of the requested revocation request. Additionally, it is possible to submit the revocation request form, electronically signed, to the Registration Area of the FNMT-RCM which will be in charge to process it. The registrar of the FNMT-RCM will carry out the same checks regarding the identity and capacity of the Subscriber's Representative as would be performed for cases of issuance requests and, if approved, will process the revocation of the Certificate
4.9.5. Time within which CA Must Process the Revocation Request	CP Section 4.9.5. Time period for revocation application processing	Compliant. The FNMT – RCM proceeds with the immediate revocation of the Website authentication certificate at the time of performing the checks described above or, where applicable, once the veracity of the request resulting from judicial or administrative resolution has been verified
4.9.7. CRL Issuance Frequency *Indicate if your CA publishes CRLs. If yes, then please test your CA's CRLs.*	CPS and CP Section 4.9.7. CRL generation frequency	Compliant. Revocation lists (CRLs) for end-entity Certificates are issued at least every 12 hours, or whenever there is a revocation; they have a 24-hour validity period. CRLs of Authority certificates are issued every six months, or whenever there is a revocation by a Certification Authority; they have a 6-month validity period.
4.9.9. On-line Revocation/Status Checking Availability	CPS and CP Section 4.9.9. Availability of the online certificate status verification system	Compliant. Information on the status of certificates will be available online 24 hours a day, seven days a week. In the event of system failure, the business continuity plan will be implemented to resolve the incident as soon as possible
4.9.10. On-line Revocation Checking Requirements *Indicate how your CA meets all of the requirements listed in this section,* ***including support of GET, update frequency, preventing errounious return of "good" status.***	CPS and CP Section 4.9.10. Online revocation verification requirements	Compliant. If the request is valid, an OCSP response will be issued on the status at that moment of the Certificates included in the request.This OCSP response is signed/stamped using the Signature/Stamp Creation Data of the FNMT-RCM If the OCSP responder receives a request for status of a certificate that has not been issued, then responds with a revoked certificateHold Jan 1 1970 as per RFC. OCSP services support GET method
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	CP Section 4.9.11. Other available revocation notification methods	Compliant. No other forms of revocation are defined.
4.10.1. Operational Characteristics	CPS and CP Section 4.9.10. Online revocation verification requirements CPS and CP Section 4.10.1. Operational features	Compliant. Revocation entries on a CRL or OCSP Response are not removed until after the Expiry Date of the revoked Certificate due to CA implementation
4.10.2. Service Availability	CPS Section 4.9.9. Availability of the online certificate status verification system and 4.10.2. Service availability	Compliant. The FNMT-RCM guarantees access to this service, 24/7, for all Certificate users, holders and trusting parties, securely, quickly and free of charge
5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS		
5.2.2. Number of Individuals Required per Task	CPS Section 5.2.2. Number of persons per task	Compliant. Internal document "*Trusted roles and security profiles*". Copy, backup or recovery operations relating to the Signature creation data are controlled exclusively by authorised personnel employing, at minimum, dual control in a secure environment. Mechanisms to activate and use the Certification Authorities' Private keys are based on the segmentation of management and operation roles that the FNMT-RCM has implemented, including multi-person access based on cryptographic cards and related PINs in a simultaneous use M of N (2 of 5) system.
5.3.1. Qualifications, Experience, and Clearance Requirements	CPS Section 5.3.1. Knowledge, qualifications, experience and accreditation requirements	Compliant. All the personnel involved in the activity of the FNMT-RCM, as a Trusted Service Provider, and especially the managerial staff, possess necessary experience and knowledge to manage said activity. These requirements are guaranteed by the corresponding criteria in the personnel selection processes so that the employee's professional profile is as appropriate as possible to the characteristics of the tasks to be developed Trusted positions within the scope of this document will be those that entail access to or control of components that could directly affect the management of systems that implement the services related to Certificates and information on the status of Certificates Personnel recruitment and policies are included in the Collective Agreement regulating work relationships between the FNMT-RCM and its employees, as well as in legislation applicable to the civil service and the related Statute (Royal Decree 1114/1999 of 25 June adapting the Spanish Mint to Law 6/1997 of 14 April on the Organisation and Functioning of the General State Administration. For trusted roles, people are selected for these roles applying the principle of least privilege and taking into account training, experience and the Personnel Security controls described below. The people holding these roles will be designated by the CSP's Management Committee

5.3.3. Training Requirements and Procedures	CPS Section 5.3.3. Training requirements	Compliant. The FNMT-RCM manages the Annual Training Plan, through its Training Centre attached to the Human Resources Department, on the basis of the Entity's general needs and each department's specific needs. All employees, whether on the payroll or subcontracted, who have access to or control of the trustworthy systems on which the trusted third-party services are based are covered by the annual Training Plan focused on information security training and awareness building needs, as laid down in the internal document “Information security training and awareness raising standard”
5.3.4. Retraining Frequency and Requirements	CPS Section 5.3.3. Training requirements and 5.3.4. Refresher training requirements and frequency	Compliant. All personnel in Trusted Roles SHALL maintain skill levels consistent with the CA’s training and performance programs. The FNMT-RCM implements ongoing training plans, paying particular attention to substantial modifications of Trust Service infrastructure operations
5.3.7. Independent Contractor Controls	CPS Section 5.3.7.1. Third-party contracting requirements	Compliant. There are no Delegated Third Party’s personnel involved in the issuance of a Certificate. The contracting of third parties by the FNMT-RCM is subject to the Law 9/2017, of November 8, on Contracts of the Public Sector
5.4.1. Types of Events Recorded *Indicate how your CA meets the requirements of this section.*	CPS Section 5.4.1. Event types logged	Compliant. The FNMT-RCM 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 will 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. All events relating to the life cycle of keys managed by the CA, including any subject keys generated by the CA. The FNMT-RCM archives 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. Log retention period	Compliant. Audit logs are held for at least fifteen (15) years
5.4.8. Vulnerability Assessments *Indicate how your CA meets the requirements of this section.*	CPS Section 5.4.8. Vulnerability analysis	Compliant. The FNMT-RCM carries out quarterly vulnerability analyses in its systems. An annual penetration test is also performed
5.5.2. Retention Period for Archive	CPS Section 5.5.2. Archive retention period	Compliant. The retention period for logs archived will not be less than 15 years
5.7.1. Incident and Compromise Handling Procedures *Indicate how your CA meets the requirements of this section.*	CPS Section 5.7.1. Incident and vulnerability management	Compliant. In the case of a security incident, the affected parties will be notified as described in the Security Policy and the related implementing rules, particularly the incident response plan. In the event of a high-impact incident, the FNMT-RCM will send notification in less than 24 hours following detection. The internal document “Information Security Management System - Security Manual” lays down incident management procedures and responsibilities, guaranteeing a fast, effective and orderly response to security incidents
6.1.1. Key Pair Generation	CPS Section 6.1. KEY GENERATION AND INSTALLATION CP Section 6.1.1. Key pair generation	Compliant. The FNMT-RCM possess a procedure described in the document “Gestión del ciclo de vida de las claves de la FNMT-RCM como Prestador de Servicios de Certificación y Sellado”, for conducting CA key pair generation for all CAs, whether root CAs or subordinate CAs that issue certificates to end users. As a result of this procedure, a report is produced proving that ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair is ensured. This report is signed by the persons who exercise the corresponding trust roles in the generation of Keys of a subordinate CA, and in the case of a root CA will be additionally signed by a reliable and independent person of the management team of the Provider The Private keys of the Subscribers of the Website authentication certificates are generated and guarded by the Subscriber of the Certificate
6.1.2. Private Key Delivery to Subscriber	CP Section 6.1.2. Sending of private key to the subscriber	Compliant. The private key is generated by a process initiated by the owner himself in the software device that he owns. There is therefore no private key transfer.
6.1.5. Key Sizes	CP Section 6.1.5. Key sizes and algorithms used	Compliant. The algorithm used is ECDSA-with-SHA384. The Key size, depending on each case, is: • FNMT root CA Keys: ECC P-384 bits. • CA Subordinate keys: ECC P-384 bits. • Website authentication certificate keys: ECC P-384 bits
6.1.6. Public Key Parameters Generation and Quality Checking	CP Section CPS Section 6.1.6. Public key generation parameters and quality verification	Compliant. The Public keys for the Website authentication certificates are encoded under RFC5280 and PKCS#1
6.1.7. Key Usage Purposes	CP Section 6.1.7. Permitted uses of keys (KeyUsage field X.509v3)	Compliant. The root Certificate of the CA has enabled the uses of Keys to sign/stamp the Certificates of the Subordinated CAs and the ARLs. The Certificates of the Subordinate CAs that issue Website Authentication Certificates are exclusively authorised to sign/stamp end user Certificates (Website authentication certificates) and CRLs. The Website authentication certificate is enabled for use of a digital signature. Additionally, these Certificates feature the extended use of a server authentication key (server authentication).
6.2. Private Key Protection and Cryptographic Module Engineering Controls	CPS Section 6.2.1. Cryptographic module standards, 6.2.2. Private key multi-person control (n of m), 6.2.3. Private key custody and 6.2.4. Private key backup	Compliant. The Trust Service Provider's Signature creation data are protected by a cryptographic device that fulfils FIPS PUB 140-2 Level-3 security standards
6.2.5. Private Key Archival	CPS Section 6.2.5. Private key filing	Compliant. The FNMT-RCM may make a backup of the Private keys, guaranteeing that the security level of the copied data is at least equal to that of the original data and that the number of data duplicated does not exceed the minimum necessary to assure service continuity. The Signature creation data are not duplicated for any other purpose.
6.2.6. Private Key Transfer into or from a Cryptographic Module	CPS Section 6.2.6. Transfer of private key to or from the cryptographic module. CPS Section 6.2.4. Private key backup	Compliant. Keys cannot be transferred, although there is a recovery procedure as a contingency measure
6.2.7. Private Key Storage on Cryptographic Module	CPS Section 6.2.7. Storage of private key in the cryptographic module and 6.2.8. Private key activation method	Compliant. Root CA private keys of the FNMT-RCM are held and used physically isolated from normal operations such that only designated trusted personnel have access to the keys for use in signing subordinate CA Certificates. The Certification Authorities’ Private keys are generated and custodied by a cryptographic device that meets FIPS PUB 140-2 Level 3 security requirements
6.3.2 Certificates issued after March 1, 2018, MUST have a Validity Period no greater than 825 days ***Indicate how your CA meets the requirements of this section.***	CP Section 6.3.2. Certificate operating periods and key pair usage periods	Compliant. Certificate and associated Key operating periods are as follows: • Root CA Certificate and set of Keys: 20 December 2043. • The certificate of the subordinate CA that issues the authentication certificates for websites and their set of Keys: 20 December 2033 • The Website authentication certificates and their set of Keys: the maximum period of validity of the Certificates and their set of Keys issued under the Organisation validation policies (OV Certificate, SAN OV Certificate and Wildcard OV Certificate) is 24 months, and that of the EV Certificates, SAN EV Certificates or Website certificates is 12 months.

6.5.1. Specific Computer Security Technical Requirements **The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.** *Indicate how your CA meets the requirements of this section.*	CPS Section 6.5.1. Specific technical requirements for IT security	Compliant. When defining security for all the technical components used by the FNMT-RCM in the course of its Trust Service Provider activities and in its structure and procedures, all aspects of Information System security certification are taken into consideration, in accordance with the National Information System Security Certification Framework approved in Spain, in particular those relating to EESSI published in the Official Journal of the European Union or in the relevant Spanish Official Journals. Information technology security evaluation under ISO 15408 (Common Criteria) is also taken into account in the design, development, evaluation and acquisition of IT products and systems for use by the Trust Service Provider, in addition to the EESSI regulations. Infrastructure security management processes will be evaluated periodica
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.** *Indicate how your CA meets the requirements of this section.*	CP Section 7.1. CERTIFICATE PROFILE	Compliant. Website authentication certificates are in accordance with the European standard ETSI EN 319 412-4 "Certificate profile for web site certificates". Certificates issued with EV policies (Website certificate, EV Certificate and SAN EV Certificate) contain the policy identifier 0.4.0.2042.1.4. Certificates issued with OV policies (OV certificate, OV Wildcard Certificate and SAN OV Certificate) contain the policy identifier 0.4.0.2042.17 Serial numbers are randomly generated obtaining a positve "integer" no bigger than 20 octets
7.1.1. Version Number(s)	CP Section 7.1.1. Version number	Compliant. Website authentication certificates are compliant with the X.509 version 3 standard.
7.1.2. Certificate Content and Extensions; Application of RFC 5280	CP Section 7.1.2. Certificate extensions	Compliant. The document describing the profiles of the Website authentication certificates, including all extensions, is published at https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-1 and https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-2
7.1.2.1 Root CA Certificate	CP Section 7.1.2. Certificate extensions	Compliant. FNMT-RCM meets the requirements. See profile document published at https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-1 and https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-2
7.1.2.2 Subordinate CA Certificate	CP Section 7.1.2. Certificate extensions	Compliant. FNMT-RCM meets the requirements. See profile document published at https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-1 and https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-2
7.1.2.3 Subscriber Certificate	CP Section 7.1.2. Certificate extensions	Compliant. FNMT-RCM meets the requirements. See profile document published at https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-1 and https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-2
7.1.2.4 All Certificates	CP Section 7.1.2. Certificate extensions	Compliant. FNMT-RCM meets the requirements. See profile document published at https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-1 and https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-2
7.1.2.5 Application of RFC 5280		Compliant
7.1.3. Algorithm Object Identifiers	CP Section 7.1.3. Algorithm object identifiers	Compliant. The object identifier (OID) relating to the cryptographic algorithm used (ecdsa-with-SHA384) is 1.2.840.10045.4.3.3
7.1.4. Name Forms	CP Section 7.1.4. Name formats and 3.1. DENOMINATION	Compliant. Website authentication certificate encoding follows the RFC 5280 recommendation "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. All the fields defined in the Certificate profile, except where expressly stated in the relevant fields, use UTF8String encoding
7.1.4.1 Issuer Information	CP Section 7.1.4. Name formats	Compliant. FNMT-RCM meets the requirements. Certificate encoding follows the RFC 5280 recommendation "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". All the fields defined in the Certificate profile, except where expressly stated in the relevant fields, use UTF8String encoding. See profile document published at https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-1 and https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-2
7.1.4.2 Subject Information - Subscriber Certificates Section 7.1.4.2.1 states: Certificate Field: extensions:**subjectAltName** Required/Optional: Required Contents: **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. Section 7.1.4.2.2 states: Certificate Field: subject:commonName (OID 2.5.4.3) Required/Optional: Deprecated (Discouraged, but not prohibited) Contents: **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)	CP Section 7.1.4. Name formats	Compliant. FNMT-RCM meets the requirements. Certificate encoding follows the RFC 5280 recommendation "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". All the fields defined in the Certificate profile, except where expressly stated in the relevant fields, use UTF8String encoding. See profile document published at https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-1 and https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-2
7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates	CP Section 7.1.4. Name formats	Compliant. FNMT-RCM meets the requirements. Certificate encoding follows the RFC 5280 recommendation "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". All the fields defined in the Certificate profile, except where expressly stated in the relevant fields, use UTF8String encoding. See profile document published at https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-1 and https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-2
7.1.5. Name Constraints ***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.*** ***"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. ..."***	CP Section 7.1.5. Name restrictions CP Section 3.2.6. Interoperation criteria	Compliant. FNMT Roots are publicly diclosed in the CCADB and audited in accordance with the Mozilla Root program. FNMT-RCM does not issue Subordinate CA Certificates to external parties and its internal Issuing CA is currently not technically constrained. See profile document published at https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-1 and https://www.sede.fnmt.gob.es/dpcs/ac-servidores-seguros-tipo-2
7.1.6. Certificate Policy Object Identifier		
7.1.6.1 Reserved Certificate Policy Identifiers	CP Section 7.1.6. Certificate policy object identifier and 1.2. DOCUMENT NAME AND IDENTIFICATION	Compliant. FNMT-RCM uses proprietary policy object Identifiers and 2.23.140.1.2.2 for certificates issued by AC Servidores Seguros Tipo 2 and 2.23.140.1.1 for certificates issued by AC Servidores Seguros Tipo 1
7.1.6.2 Root CA Certificates	CP Section 7.1.6. Certificate policy object identifier and 9.6.1. CA's obligations	Compliant. No policy extension is contained. CP's indicates compliance with BR.
7.1.6.3 Subordinate CA Certificates	CP Section 7.1.6. Certificate policy object identifier and 9.6.1. CA's obligations	Compliant. FNMT-RCM does not issue CA certificates to Subordinate CA that are not an affiliate of FNMT-RCM CP's indicates compliance with BR.

7.1.6.4 Subscriber Certificates	CP Section 7.1.6. Certificate policy object identifier and 9.6.1. CA's obligations	Compliant. **EV Website certificate** (FNMT OID: 1.3.6.1.4.1.5734.3.16.1.1) EV OID: 2.23.140.1.1 EVCP ETSI OID: 0.4.0.2042.1.4 QCP-w ETSI OID: 0.4.0.194112.1.4 **EV Certificate** (FNMT OID: 1.3.6.1.4.1.5734.3.16.1.2) EV OID: 2.23.140.1.1 EVCP ETSI OID: 0.4.0.2042.1.4 QCP-w ETSI OID: 0.4.0.194112.1.4 **EV SAN Certificate** (FNMT OID: 1.3.6.1.4.1.5734.3.16.1.3) EV OID: 2.23.140.1.1 EVCP ETSI OID: 0.4.0.2042.1.4 QCP-w ETSI OID: 0.4.0.194112.1.4 **OV Certificate** (FNMT OID 1.3.6.1.4.1.5734.3.16.2.1) OV OID: 2.23.140.1.2.2 OVCP ETSI OID: 0.4.0.2042.1.7 **OV Wildcard Certificate** (FNMT OID 1.3.6.1.4.1.5734.3.16.2.2) OV OID: 2.23.140.1.2.2 OVCP ETSI OID: 0.4.0.2042.1.7 **OV SAN Certificate** (FNMT OID 1.3.6.1.4.1.5734.3.16.2.3) OV OID: 2.23.140.1.2.2 OVCP ETSI OID: 0.4.0.2042.1.7 CP's indicates compliance with BR
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS		
8.1. Frequency or circumstances of assessment **The period during which the CA issues Certificates SHALL be dividied 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 SHAL 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. *Indicate your CA's understanding of this requirement, and how your CA meets the requirements of this section.*	CP Section 8.1. AUDIT FREQUENCY	Compliant. The following audits are carried out annually: ETSI EN 319 401 “General Policy Requirements for Trust Service Providers” ETSI EN 319 411-1 "Policy and security requirements for Trust Service Providers issuing certificates” ETSI EN 319 411-2 “Requirements for trust service providers issuing EU certificates” ETSI EN 319 412- 4 “Certificate profile for web site certificates”
8.2. Identity/qualifications of assessor *Indicate how your CA meets he requirements of this section.*	CPS Section 8.2. AUDITOR QUALIFICATIONS	Compliant. The auditor that verifies and checks the proper performance of the FNMT-RCM Trust Service Provider must be a person or professional with sufficient official qualifications and suitable experience in the matter to be audited, pursuant to legislation in force from time to time. The auditor must at least be accredited under the European standard ETSI EN 319 403.The audit report issued will identify the auditors. The audit report will be signed by the auditors and the head of the entity audited
8.4. Topics covered by assessment	CPS Section 8.4. ASPECTS AUDITED	Compliant. FNMT-RCM has been audited in accordance with ETSI scheme.The following controls will be carried out: • Internal network security controls. • Internal contingency plan controls and tests. • Internal Quality and Security controls. • Extraordinary controls: Where required in the circumstances, at the FNMT-RCM’s discretion.
8.6. Communication of results	CPS Section 8.6. NOTIFICATION OF FINDINGS	Compliant. FNMT-RCM makes the Audit Report publicly available. The summarized report is deemed public and also communicated as required by the different CA Programs. The competent administrative authorities or courts of law may request the audit reports to verify the proper functioning of the Trust Service Provider.
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).** **....** **The publicly-available documentation relating to each audit MUST contain at least the following clearly-labelled information:** **- 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).** **“**		Compliant. FNMT-RCM understands and comply with section 3 of Mozilla’s Root Store Policy
8.7. Self-Audits	CPS Section 8.1. AUDIT FREQUENCY	The FNMT – RCM performs self-assessments, on a quarterly basis at a minimum, of 20% of all Certificates issued during the period that begins immediately after the previous self-assessment sample
9.6.1. CA Representations and Warranties	CPS and CP 9.6.1. CA's obligations	Compliant. The FNMT – RCM complies with all requirements contained in the technical specifications of the ETSI EN 319 411 standard for the issuance of Certificates and undertakes to continue complying with said regulation or those that replace it
9.6.3. Subscriber Representations and Warranties	CPS and CP 9.6.3. Subscriber obligations	Compliant. Prior to the issuance of a Certificate, the Applicant must ellectronically sign and submit the agreement and acknowledging the Terms of Use.

9.8. Limitations of liability	CPS Section 9.8. LIABILITY	Compliant. The FNMT-RCM will only be answerable for the correct personal identification of the Applicant and future Holder, and for including these data in a Certificate. In order for the guarantees, obligations and responsibilities to be applicable, the event must have taken place within the scope of the Electronic Community. The FNMT-RCM will only be answerable for weaknesses in the procedures pertaining to its own activities as a Trust Service Provider and in accordance with these Certification Policies or the Law. It will not in any circumstances be liable for actions or losses that may be incurred by Holders, Subscribers, User entities or third parties which are not due to errors attributable to the FNMT-RCM in the above-mentioned Certificate issuance and/or management procedures. The FNMT-RCM will not be liable for force majeure events, terrorist attacks, wildcat strikes or actions constituting offences or misdemeanours that affect its facilities in which the services are provided, unless the Entity is guilty of serious negligence. In any event, the FNMT-RCM may include disclaimers in the relevant contracts and/or agreements. In any case, the amount of damages that the FNMT-RCM would be required to pay to affected third parties and/or members of the Electronic community as a result of a court order, in the absence of specific provisions of contracts or agreements, is limited to a maximum of SIX THOUSAND EUROS (€6,000). The FNMT-RCM will not be answerable to persons whose behaviour in the use of the Certificates has been negligent; for these purposes, and in any event, negligence will be regarded as the failure to comply with the provisions of this Certification Practices and Policies Statement and, in particular, the provisions of the sections that refer to the parties' obligations and liability. The FNMT-RCM will not be liable for any software that it has not provided directly. Nonetheless, the FNMT-RCM will put in place adequate measures to protect its systems against Malicious software (Malware) and will diligently keep them up to date to cooperate with users in the avoidance of the damage that such software may cause.
9.9.1. Indemnification by CAs	CPS Section 9.8. LIABILITY and 9.9. INDEMNITIES	Compliant. The FNMT-RCM may include indemnity clauses in the legal instruments linking it to the Holder for the infringement of the latter's obligations or of applicable legislation
9.16.3. Severability		Compliant. No conflict between these Requirements and a law, regulation or government order has been noticed.