Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

SPECIFIC CERTIFICATION POLICIES AND CERTIFICATION PRACTICES FOR THE JUDICIAL CAREER CERTIFICATES

	NAME	DATE
Prepared by:	FNMT-RCM	11/09/2024
Revised by:	FNMT-RCM	11/09/2024
Approved by:	FNMT-RCM	11/09/2024

Version	DATE	Description
1.0	11/09/2024	Document creation: Specific Certification Policies and Certification Practices for the Judicial Career Certificates

Reference: DPC/DPCCJ_0100/SGPSC/2024

Table of contents

1. Introduction 9

1.1. Overview 9

1.2. Document name and identification 10

1.3. PKI participants 12
1.3.1. Certification Authority 12
1.3.2. Registration Authority 13
1.3.3. Signatories 14
1.3.4. Certificate Subscribers 14
1.3.5. Relying parties 14
1.3.6. Other participants 14

1.4. Certificate usage 14
1.4.1. Appropriate certificate uses 14
1.4.2. Prohibited certificate uses 15

1.5. Policy Administration 16
1.5.1. Organisation administering the document 16
1.5.2. Contact details 16
1.5.3. Person determining CPS suitability for the policy 16
1.5.4. CPS approval procedure 16

1.6. Definitions and Acronyms 17
1.6.1. Definitions 17
1.6.2. References 18

2. Publication and repository responsibilities 19

2.1. Repository 19

2.2. Publication of certification information 19

2.3. Time and frequency of publication 19

2.4. Access controls on repositories 19

3. Identification and authentication 19

3.1. Naming 19
3.1.1. Types of names 19
3.1.2. Need for names to be meaningful 20
3.1.3. Anonymity or pseudonymity of subscribers 20
3.1.4. Rules for interpreting various name forms 20
3.1.5. Uniqueness of names 20
3.1.6. Recognition, authentication and role of trademarks 20

3.2. Initial identity validation 20
3.2.1. Methods to prove possession of private key 20
3.2.2. Authentication of organisation identity 21
3.2.3. Authentication of individual applicant identity 21
3.2.3.1 Direct check by physical presence 21
3.2.3.2 Indirect check by reliable means equivalent to physical presence under national Law 22
3.2.4. Non-verified Subscriber information 22

3.2.5. Validation of authority 22
3.2.6. Criteria for interoperation 22

3.3. Identification and authentication for re-key requests 22
3.3.1. Identification and authentication for routine re-key 22
3.3.2. Identification and authentication for re-key after revocation 22

3.4. Identification and authentication for revocation requests 23

4. Certificate life-cycle operational requirements 23

4.1. Certificate application 23
4.1.1. Who can submit a Certificate application 23
4.1.2. Registration process and responsibilities 23

4.2. Certificate application processing 23
4.2.1. Performing identification and authentication functions 23
4.2.2. Approval or rejection of certificate applications 24
4.2.3. Time to process applications 24

4.3. Certificate issuance 24
4.3.1. CA actions during issuance 24
4.3.2. Notification of issuance 26

4.4. Acceptance of the certificate 26
4.4.1. Conduct constituting certificate acceptance 26
4.4.2. Publication of the certificate by the CA 26
4.4.3. Notification of issuance to other entities 26

4.5. Key pair and certificate usage 26
4.5.1. Private Key and certificate usage 26
4.5.2. Relying party public key and certificate usage 26

4.6. Certificate renewal 26
4.6.1. Circumstances for certificate renewal 26
4.6.2. Who may request renewal 27
4.6.3. Processing certificate renewal requests 27
4.6.4. Notification of new certificate issuance to subscriber 27
4.6.5. Conduct constituting acceptance of a renewal certificate 27
4.6.6. Publication of the renewal certificate by the CA 27
4.6.7. Notification of certificate issuance by the CA to other other entities 27

4.7. Certificate re-key 27
4.7.1. Circumstances for certificate re-key 27
4.7.2. Who may request re-key 27
4.7.3. Processing certificate re-keying requests 28
4.7.4. Notification of certificate re-key 28
4.7.5. Conduct constituting acceptance of a re-keyed certificate 28
4.7.6. Publication of the re-keyed certificate 28
4.7.7. Notification of certificate re-key to other entities 28

4.8. Certificate modification 28
4.8.1. Circumstance for certificate modification 28
4.8.2. Who may request certificate modification 28
4.8.3. Processing certificate modification requests 28
4.8.4. Notification of new certificate issuance to subscriber 28
4.8.5. Conduct constituting acceptance of modified certificate 28

4.8.6. Publication of the modified certificate by the CA 28
4.8.7. Notification of the certificate issuance by the CA to other entities 29

4.9. Certificate revocation and suspension 29
4.9.1. Circumstances for revocation 29
4.9.1.1 Reasons for revoking a subscriber certificate 29
4.9.1.2 Reasons for revoking a subordinate CA certificate 31
4.9.2. Who can request revocation 31
4.9.3. Procedure for revocation request 31
4.9.4. Revocation request grace period 32
4.9.5. Time within which to process the revocation request 32
4.9.6. Revocation checking requirement for relying parties 32
4.9.7. CRL issuance frequency 32
4.9.8. Maximum latency for CRLs 32
4.9.9. Online revocation/status checking availability 32
4.9.10. Online revocation verification requirements 33
4.9.11. Other forms of revocation advertisements available 33
4.9.12. Special requirements related to key compromise 33
4.9.13. Circumstances for suspension 33
4.9.14. Who can request suspension 33
4.9.15. Procedure for suspension request 33
4.9.16. Limits on suspension period 33

4.10. Certificate status services 33
4.10.1. Operational characteristics 33
4.10.2. Service availability 33
4.10.3. Optional features 34

4.11. End of subscription 34

4.12. Key escrow and recovery 34
4.12.1. Key escrow and recovery policy and practices 34
4.12.2. Session key encapsulation and recovery policy and practices 34

5. Physical security, procedural and personnel controls 34

5.1. Physical security controls 34
5.1.1. Site location and construction 34
5.1.2. Physical access 34
5.1.3. Power and air conditioning 34
5.1.4. Water exposures 35
5.1.5. Fire prevention and protection 35
5.1.6. Media storage 35
5.1.7. Waste disposal 35
5.1.8. Off-site backup 35

5.2. Procedural Controls 35
5.2.1. Trusted roles 35
5.2.2. Number of persons required per task 35
5.2.3. Identification and authentication for each role 35
5.2.4. Roles requiring separation of duties 35

5.3. Personnel Controls 35
5.3.1. Qualifications, experience, and clearance requirements 35
5.3.2. Background check procedures 36

5.3.3. Training requirements 36
5.3.4. Retraining frequency and requirements 36
5.3.5. Job rotation frequency and sequence 36
5.3.6. Sanctions for unauthorized actions 36
5.3.7. Independent contractor requirements 36
5.3.8. Documentation supplied to personnel 36

5.4. Audit-logging procedures 36
5.4.1. Types of events recorded 36
5.4.2. Frequency of processing log 36
5.4.3. Retention period for audit log 36
5.4.4. Protection of audit log 36
5.4.5. Audit log backup procedures 37
5.4.6. Log collection systems 37
5.4.7. Notification to event-causing subject 37
5.4.8. Vulnerability assessments 37

5.5. Records archival 37
5.5.1. Types of records archived 37
5.5.2. Retention period for archive 37
5.5.3. Protection of archive 37
5.5.4. Archive backup procedures 37
5.5.5. Requirements for time-stamping of records 37
5.5.6. Log collection systems 37
5.5.7. Procedures to obtain and verify archive information 37

5.6. CA key changeover 38

5.7. Compromise and disaster recovery 38
5.7.1. Incident and compromise handling procedures 38
5.7.2. Computing resources, software, and/or data are corrupted 38
5.7.3. Entity private key compromise procedures 38
5.7.4. Business continuity capabilities after a disaster 38

5.8. Trust Service Provider termination 38

6. Technical security controls 38

6.1. Key pair generation and installation 38
6.1.1. Key pair generation 38
6.1.1.1 CA key pair generation 38
6.1.1.2 RA key pair generation 38
6.1.1.3 Subscriber key pair generation 39
6.1.2. Private key delivery to the subscriber 39
6.1.3. Public key delivery to certificate issuer 39
6.1.4. CA public key delivery to relying parties 39
6.1.5. Key sizes and algorithms used 39
6.1.6. Public key parameters generation and quality checking 39
6.1.7. Key usage purposes (KeyUsage field X.509v3) 39

6.2. Private key protection and cryptographic module engineering controls 40
6.2.1. Cryptographic module standards and controls 40
6.2.2. Private key (n out of m) multi-person control 40
6.2.3. Private key escrow 40
6.2.4. Private key backup 40

6.2.5. Private key archival 40
6.2.6. Private key transfer into or from a cryptographic module 40
6.2.7. Private key storage on cryptographic module 40
6.2.8. Activating private keys 41
6.2.9. Deactivating private keys 41
6.2.10. Destroying private keys 41
6.2.11. Cryptographic module capabilities 41

6.3. Other aspects of key pair management 41
6.3.1. Public key archival 41
6.3.2. Certificate operational periods and key pair usage periods 41

6.4. Activation data 42
6.4.1. Activation data generation and installation 42
6.4.2. Activation data protection 42
6.4.3. Other aspects of activation data 42

6.5. Computer security controls 42
6.5.1. Specific computer security technical requirements 42
6.5.2. Computer security rating 42

6.6. Life cycle technical controls 42
6.6.1. System development controls 42
6.6.2. Security management controls 43
6.6.3. Life cycle security controls 43

6.7. Network security controls 43

6.8. Time-stamping 43

6.9. Other additional controls 43
6.9.1. Control of the ability to provide services. 43
6.9.2. Control of systems development and computer applications 43

7. Certificate, CRL and OCSP profiles 43

7.1. Certificate profile 43
7.1.1. Version number 43
7.1.2. Certificate extensions 43
7.1.3. Algorithm object identifiers 44
7.1.4. Name forms 44
7.1.5. Name constraints 44
7.1.6. Certificate policy object identifier 44
7.1.7. Usage of policy constraints extension 44
7.1.8. Policy qualifiers syntax and semantics 44
7.1.9. Processing semantics for the critical certificate policies extension 45

7.2. CRL profile 45
7.2.1. Version number 45
7.2.2. CRL and CRL entry extensions 45

7.3. OCSP profile 45
7.3.1. Version number 45
7.3.2. OCSP extensions 46

8. Compliance audit and other assessments 46

8.1. Frequency or circumstances of assessment 46
8.2. Qualifications of assessor 47
8.3. Assessor's relationship to assessed entity 47
8.4. Topics covered by assessment 47
8.5. Actions taken as a result of deficiency 47
8.6. Communication of results 47
8.7. Autoevaluation 47

9. Other business and legal matters 47

9.1. Fees 47
9.1.1. Certificate issuance or renewal fees 47
9.1.2. Certificate access fees 47
9.1.3. Revocation or status information access fees 47
9.1.4. Fees for other services 48
9.1.5. Refund policy 48

9.2. Financial responsibility 48
9.2.1. Insurance coverage 48
9.2.2. Other assets 48
9.2.3. Insurance or warranty coverage for end-entities 48

9.3. Confidentiality of business information 48
9.3.1. Scope of confidential information 48
9.3.2. Information not within the scope of confidential information 48
9.3.3. Responsibility to protect confidential information 48

9.4. Privacy of personal information 48
9.4.1. Privacy plan 49
9.4.2. Information treated as private 49
9.4.3. Information not deemed private 49
9.4.4. Responsibility to protect private information 49
9.4.5. Notice and consent to use private information 49
9.4.6. Disclosure pursuant to judicial or administrative process 49
9.4.7. Other information disclosure circumstances 49

9.5. Intellectual property rights 49

9.6. Representations and warranties 49
9.6.1. CA representations and warranties 49
9.6.2. RA representations and warranties 50
9.6.3. Subscriber and signatory representations and warranties 50
9.6.4. Relying party representations and warranties 51
9.6.5. Representations and warranties of other participants 52

9.7. Disclaimer of warranties 52

9.8. Limitations of liability 52

9.9. Indemnities 52
9.9.1. CA indemnity 52
9.9.2. Subscribers indemnity 52
9.9.3. Relying parties indemnity 52

9.10. Term and termination *52*
9.10.1. Term 52
9.10.2. Termination 53
9.10.3. Effect of termination and survival 53
9.11. Individual notices and communications with participants *53*
9.12. Amendments *53*
9.12.1. Procedure for amendment 53
9.12.2. Notification mechanism and period 53
9.12.3. Circumstances under which OID must be changed 53
9.13. Dispute resolution provisions *53*
9.14. Governing law *53*
9.15. Compliance with applicable law *53*
9.16. Miscellaneous provisions *53*
9.16.1. Entire agreement 53
9.16.2. Assignment 54
9.16.3. Severability 54
9.16.4. Enforcement (attorneys' fees and waiver of rights) 54
9.16.5. Force Majeure 54
9.17. Other provisions *54*

Index of Tables

Table 1 – Root FNMT CA Certificate 12
Table 2 – Subordinate CA Certificate 13
Table 3 – CRL profile 45

1. INTRODUCTION

1. The Law 18/2011, 5 July, regulating the use of information and communication technology in the Courts Service, under its article 21 assigns the General Council of the Judiciary the establishment of the electronic signatures systems for judges and magistrates.

2. Citizens' Electronic Access to Public Services Act 11/2007, 22 June, established citizens' right to engage in electronic exchanges with the various Public Administrations (Public Authorities). The legal framework resulting from the approval of Public Administration Common Administrative Procedure Act 39/2015, 1 October, and of Public Sector Legal Regime Act 40/2015, 1 October, systematises all administrative procedure laws, clarifying and consolidating the contents of Public Administration Legal Regime and Common Administrative Procedure Act 30/1992, 26 November, and of the aforementioned Act 11/2007, 22 June. In addition, Justice Administration Information and Communication Technologies Use Act 18/2011, 5 July, makes provision for electronic signature and identification systems to be used within the sphere of Justice Administration.

3. Regulation (EU) No. 910/2014 of the European Parliament and of Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation), lays down a general legal framework for the use of *Electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and website authentication Certificate services.*

1.1. OVERVIEW

4. The purpose of this document is to provide public information as to the terms and features of the trust services and, in particular, the electronic *Certificate* issuance services provided by FNMT-RCM as a *Trust Service provider*, setting out in particular the obligations and procedures FNMT-RCM undertakes to fulfil in connection with the issuance of *Judicial Career Certificates*, and the obligations FNMT-RCM agrees to fulfil in connection with:

   - management of *Signature creation and verification data* and of the *Certificates*, the terms applicable to the application for, issuance, use and termination of the *Certificates* and their *Signature Creation Data*, and, where appropriate, the existence of procedures for coordination with the relevant Public Registers to allow immediate and confidential data interchange as to the validity of the powers specified in the *Certificates* and which must mandatorily be entered in those registers
   - provision of the *Certificate* status checking service.

5. This document further sets out, directly or with reference to the FNMT-RCM *Trust Services Practices and Electronic Certification General Statement* to which this Statement is subject, details as to the scope of liability applicable to participants using and/or relying on the services referred to in the preceding paragraph, security controls applied to its procedures and facilities to the extent they may be disclosed without detracting from their effectiveness, and secrecy and confidentiality standards, as well as matters relating to the ownership of its property and assets, protection of personal data, and such other information as may be deemed of interest to be made available to the public.

6. The *Certificates* issued by FNMT-RCM under these *Specific Certification Policies and Certification Practices* are *Qualified Certificates*, as defined in the aforementioned eIDAS Regulation, Public Sector Legal Regime Act 40/2015, 1 October, and Justice Administration Information and Communication Technologies Use Act 18/2011 (Law 18/2011 of 5 July 2011 regulating the use of information and communication technology in the Courts Service) and in accordance with the Law 06/2020, 11 November, regulating certain issues in electronic trust services. These *Certificates* comply with article 23 of the Royal Decree 203/2021, 30 March, approving the Regulation on the Performance and Functioning of the Public Sector by Electronic Means

1.2. DOCUMENT NAME AND IDENTIFICATION

7. The structure of FNMT-RCM's *Certification Practice Statement* as *Trust Service Provider* comprises on the one hand the common part of FNMT-RCM's *Trust Services Practices and Electronic Certification General Statement* (*GCPS*), for there are actions commons to all of the Entity's trust services, and, on the other hand, the specific sections of this *Specific Certification Policies and Certification Practices* document. However, the *Issuance Law* for each type of *Certificate* or group of *Certificates* may provide for special features applicable to the bodies, agencies, entities and employees using FNMT-RCM's trust services.

8. Accordingly, FNMT-RCM's *Certification Practice Statement* is structured as follows:

- On the one hand, the ***Trust Services Practices and Electronic Certification General Statement***, which must be regarded as the main body of the *Certification Practice Statement,* describing the scope of liability applicable to members of the *Electronic Community*, security controls applied to FNMT-RCM's procedures and facilities, to the extent they may be disclosed without detracting from their effectiveness, and secrecy and confidentiality standards, as well as matters relating to the ownership of its property and assets, protection of personal data and such other general information issues as should be made available to the public, whatever their role in the Electronic Community may be.

- And on the other hand, for every trust service or set or group of *Certificates*, identified and distinguished from the rest based on typology and specific or distinctive regime, there is a specific ***Certification Policy*** describing participants' obligations, restrictions on the use of the *Certificates* and responsibilities, and there are ***Specific Certification Practices*** implementing the terms defined in the relevant policy and making provision for additional or specific practices with respect to the general practices established in the *Trust Services Practices and Electronic Certification General Statement*.

  These *Specific Certification Policies and Certification Practices* actually elaborate on the contents of the main body and are therefore an integral part of the *Trust Services Practices and Electronic Certification General Statement*, and together they make up the FNMT-RCM *Certification Practice Statement*. However, they apply only to the set of *Certificates* characterised and identified in the relevant *Specific Certification Policies and Practices* and may also cover special provisions introduced by the *Issuance Law* governing the relevant *Certificate* or group of *Certificates*, where specific features or functionalities exist.

- This document also sets out the *Specific Certification Policies and Certification Practices* for the following *Certificates* within the Judicial sphere:

i. Judicial Career Certificate

- *Judicial Career Centralised Certificate*

9. The name of this document is *"SPECIFIC CERTIFICATION POLICIES AND CERTIFICATIONS PRACTICES FOR THE JUDICIAL CAREER CERTIFICATES*", and the document will hereinafter be referred to, within the scope herein defined, as the "*Specific Policy and Practice Statement*" or abbreviated as "*SPPS*".

10. These *Specific Certification Policies and Certification Practices* are part of the *Certification Practice Statement* and will prevail over the standard provisions of the *Trust Services Practices and Electronic Certification General Statement (GCPS)*.

11. The provisions hereof will prevail in the event of conflict between this document and the provisions of the *Trust Services Practices and Electronic Certification General Statement (GCPS)*.

12. Additionally, for the *Centralized Certificates*, the provisions of the Policy and Practices of the server signing service will apply, establishing the set of specific rules and procedures followed by the FNMT-RCM for the provision of its server signing service.

13. The following *Certification Policies* are included in this document identified as follows:

Name: *Judicial Career Centralised Certificate* Certification Policy

Reference / OID: 1.3.6.1.4.1.5734.3.17.8

Type of associated policy: QCP-n-qscd. OID: 0.4.0.194112.1.2

Type of Judicial Career associated policy QSCD HSM. OID: 2.16.724.6.0.1.1.5

Version: 1.0

Approval date: 11/09/2024

Location: http://www.cert.fnmt.es/dpcs/

Related CPS: FNMT-RCM Trust Services Practices and Electronic Certification General Statement

Location: http://www.cert.fnmt.es/dpcs/

14. A *Judicial Career Certificate* is an *Electronic Certificate* issued by FNMT-RCM linking the *Signatory* to *Signature verification data* and jointly confirming:

- the *Signatory's* identity (natural person serving as a *member of the Judiciary*), including, as appropriate, the *Signatory's* personal identification number, office, job and/or authorised capacity, and
- the *Certificate Subscriber's* identity, where the *Signatory* uses its powers, provides its services, or carries out its activity.

15. The *Judicial Career Centralised Certificate* is designed for remote or server-based signatures, i.e., *Public and private keys* are not directly generated in the Signatory's Internet browser or other device and the *Certificate* is not downloaded, but is generated and stored in an FNMT-RCM qualified signature creation device. In addition, the electronic signature is centrally

provided, and it is guaranteed at all times that the signature process is exclusively controlled by the *Signatory* to whom the *Certificate* has been issued.

16. FNMT-RCM will interpret, register, maintain and publish the procedures referred to in this section and may also receive communications from interested parties in this connection using the contact information provided in section 1.5.2 Contact details hereof.

1.3. PKI PARTICIPANTS

17. The following participants are involved in managing and using the *Trust Services* described in this *SPPS*:

1. Certification Authority
2. Registration Authority
3. *Signatories*
4. *Certificate Subscribers*
5. Relying Parties
6. Other participants

1.3.1. Certification Authority

18. FNMT-RCM is the *Certification Authority* issuing the electronic *Certificates* subject of this *SPPS*. The following Certification Authorities exist for these purposes:

a) Root Certification Authority. This Authority issues subordinate Certification Authority Certificates only. This CA's root Certificate is identified by the following information:

Table 1 – Root FNMT CA Certificate

Root FNMT CA Certificate	
Subject	OU = FNMT-RCM ROOT CA, O = FNMT-RCM, C = ES
Issuer	OU = FNMT-RCM ROOT CA, O = FNMT-RCM, C = ES
Serial number (hex)	5D:93:8D:30:67:36:C8:06:1D:1A:C7:54:84:69:07
Validity	Not before: 29 October 2008. Not after: 1 January 2030
Public key length	RSA 4096 bits

Root FNMT CA Certificate	
Signature algorithm	RSA – SHA256
Key identifier	F7 7D C5 FD C4 E8 9A 1B 77 64 A7 F5 1D A0 CC BF 87 60 9A 6D

b) Subordinate Certification Authority: it issues the end-entity Certificates subject of this *SPPS*. This Authority's *Certificate* is identified by the following information:

Table 2 – Subordinate CA Certificate

Subordinate CA Certificate	
Issuer	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Serial number (hex)	34 81 60 C5 1F 5E DB CB 5D DF 89 CA B4 57 33 92
Validity	Not before: 28 November 2019 Not after: 28 November 2029
Public key length	RSA 4096 bits
Signature algorithm	RSA – SHA256
Key identifier	E7:04:EE:70:91:11:92:44:F9:0E:92:8F:56:43:1E:07:1D:BF:04:9C

1.3.2. Registration Authority

19. The Registration Authority deals with identifying the applicant who must be a *member of the Judiciary*, and with checking the documentation supporting the facts recorded in the *Certificates*, validating and approving applications for those *Certificates* to be issued, revoked and, where appropriate, renewed.

20. Registration Offices designated by the *Certificate Subscriber* body, agency or entity with which the *Subscriber* signs the relevant legal instrument for that purpose may act as FNMT-RCM registration entities.

1.3.3. Signatories

21. *Signatories* are natural persons who act as *member of the Judiciary*. *Signatories* maintain the *Signature Creation Data* associated with that *Certificate* for their own use only. They are the holder and responsible for the use of their *Certificate* under their exclusive control and decision making over the Certificate.

1.3.4. Certificate Subscribers

22. The *Subscriber* for the *Judicial Career Certificates* is the legal person, public body, recipients of the FNMT-RCM's activities as a *TSP (Trust Service Provider),* that accepts the terms and conditions of the service and are referenced by the *Subject* in the *Certificate*.

1.3.5. Relying parties

23. Relying parties are natural or legal persons other than the *Signatory* / *Subscriber* that receive and/or use *Certificates* issued by FNMT-RCM and, as such, are subject to the provisions of this *SPPS* where they decide to effectively rely on such *Certificates*.

1.3.6. Other participants

24. No stipulation.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate certificate uses

25. *Judicial Career Certificates* to which this *SPPS* applies are *Qualified Certificates* as defined in Regulation (EU) No. 910/2014 of the European Parliament and of Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93 (eIDAS Regulation) and subject to the requirements established in European standards ETSI IN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" and ETSI IN 319 412-2 "Certificate profile for certificates issued to natural persons".

26. The *Judicial Career Certificates* issued under this *Certification Policy* are issued to members of the Judiciary. These *Certificates* are valid as electronic signature systems under Public Sector Legal Regime Act 40/2015, 1 October, and under Justice Administration Information and Communication Technologies Use Act 18/2011, 5 July and the Royal Decree 203/2021, of 30 March, approving the Regulation on the Performance and Functioning of the Public Sector by Electronic Means.

27. The scope of application of *Certificates* issued under the *Judicial Career Centralised Certificate Policies* for the purposes of identifying as a *member of the Judiciary* and can be used for authentications and electronic signatures required, exclusively, in *the Judicial sphere*.

1.4.2. Prohibited certificate uses

28. The restrictions on the use of the *Judicial Career Certificates* are set by reference to the various powers and functions of the *Certificate Signatory* as a *member of the Judiciary*, having regard to office, employment and, where appropriate, authorisation terms. FNMT-RCM and the Administrations, public agencies and entities may establish other additional restrictions by way of arrangements or agreements, in the relevant relationship document, or, if appropriate, in the *Issuance Law* governing those *Certificates*.

29. The restrictions on the use of the *Judicial Career Certificates* are set, in accordance with Act 40/2015 and Act 18/2011, 5 July, for authentications and electronic signatures within the exercise of *Judicial Authority*.

30. FNMT-RCM shall have no control over actions taken with and use of *Judicial Career Certificates* and their *Private keys* by the *members of the Judiciary*, so FNMT-RCM will be saved harmless from the effects of any such uses, and from the consequences and implications, if any, of potential third-party claims or, where appropriate, actions for recovery.

31. As for activities carried out by *Registration Office* employees, FNMT-RCM shall have the obligations and responsibilities established in electronic signature laws, notwithstanding the specific provisions of article 11 of Royal Decree 1317/2001, 30 November, implementing article 81 of Tax, Administrative and Social Measures Act 66/1997, 30 December, in regard to the provision of security services by the Spanish Mint ("Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda"), in communications with Public Administrations through electronic, information technology and telematics means. In order to be properly used, the *Certificates* will require prior membership of the *Electronic Community* and that the Public Administration involved acquires *Subscriber* capacity.

32. FNMT-RCM and the Administration, agencies and entities may establish other additional restrictions by way of arrangements or agreements, or in the relevant relationship document, or, if appropriate, in the *Issuance Law* governing those *Certificates*.

33. In any case, if a third party wishes to rely on the *Electronic signature* affixed under one of these *Certificates* without accessing the *Status information service* for *Certificates* issued under this *Certification Policy*, no cover will be obtained under these *Specific Certification Policies and Certification Practices* and there will be no lawful basis whatsoever for any complaint or for legal actions to be taken against FNMT-RCM based on damages, losses or disputes resulting from the use of or reliance on a *Certificate*.

34. In addition, even within the sphere of the *Electronic Community*, this type of *Certificates* may not be used for the following:

- To sign or seal any other *Certificate*, except where previously authorised on a case-by-case basis.
- For personal or private uses.
- (Particular or private uses) Uses to interact with the Administrations unless they allow it.
- To sign or seal software or components – with the exception of *Code Signing Certificates*.

- To generate time stamps for *Electronic dating* procedures.
- To provide services for no consideration or for valuable consideration, except where previously authorised on a case-by-case basis, including, but not limited to:
    - Providing *OCSP* services.
    - Generating *Revocation Lists.*
    - Providing notification services.
- Any use exceeding the purpose of this type of *Certificates* without the prior consent of FNMT-RCM.

1.5. POLICY ADMINISTRATION

1.5.1. Organisation administering the document

35. The Spanish Mint ("Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda"), with Tax Identification Number Q2826004-J, is the *Certification Authority* issuing the *Certificates* to which this *Certification Policy and Practice Statement* applies.

1.5.2. Contact details

36. FNMT-RCM's contact address as *Trust Service Provider* is as follows:

Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda

Dirección de Sistemas de Información - Departamento CERES

C/ Jorge Juan, 106

28071 – MADRID

Email: ceres@fnmt.es

Telephone: +34 91 740 69 82

37. To report security issues such as suspected key compromise, certificate misuse, fraud or other matters, send us a Certificate Problem Report to incidentes.ceres@fnmt.es

1.5.3. Person determining CPS suitability for the policy

38. The FNMT-RCM Management's remit includes the capacity to specify, revise and approve the procedures for revising and maintaining both Specific Certification Practices and the relevant Certification Policy.

1.5.4. CPS approval procedure

39. Through its *Trust Service Provider* Management Committee, FNMT-RCM oversees compliance with the *Certification Policy and Practice Statements*, and approves and then duly reviews the Statements on a yearly basis to keep them aligned with the latest version of the applicable requirements, by incrementing the version number and adding a dated changelog entry, even if no other changes were made to the document.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

40. For the purposes of the provisions of this *SPPS*, capitalised and italicised terms used herein will generally have the definitions given in the *GCPS* and, in particular, the following:

- *Jurisdictional action:* exercise of the judicial authority as established in Organic Law 6/1985 of 1 July, on the Judiciary and other regulations in force
- *Centralised Certificate: Electronic Certificate* designed for remote or server-based signatures. This means that *Public and private keys* are generated and stored in a secure environment belonging to FNMT-RCM, and it is guaranteed at all times that use of those *Keys* is exclusively controlled by the *Signatory*. Under this *SPPS* the following *Certificates* are issued as *Centralised Certificates*:
  - *Judicial Career Centralised Certificate*
- *Judicial Career Centralised Certificate*: Is the Centralised Signature Certificate whose *Signatory* will always be a *member of the Judiciary* and that links the validation data of a natural person and confirms the professional identification number granted by the General Council of the Judiciary as a means of identification and signature under Justice Administration Information and Communication Technologies Use Act 18/2011, of July 5th.
- *Activation Code*: alphanumeric key used to validate and activate an account in the Identity Management Portal.
- *Specific Policy and Practice Statement (SPPS):* a specific *CPS* which applies to the issuance of a given set of *Certificates* issued by FNMT-RCM under the specific terms contained in that Statement and to which the specific Policies defined therein apply.
- *Qualified signature creation device (QSCD):* electronic signature creation device that meets the requirements listed in Annex II of Regulation (EU) 910/2014.
- *Signatory*: a *Natural person* who acts as a *member of the Judiciary* using his or her *Signature Creation Data.*
- *Supervisory body:* a body designated by a Member State responsible for supervisory tasks in the provision of trust services, in accordance with article 17 of the eIDAS Regulation
- *Member of the Judiciary:* According to Organic Law 6/1985 of July 1, on the Judiciary, professional Judges and Magistrates shall constitute the Judicial Career. The Judicial professional comprises three ranks: Supreme Court Judges, Judges and Magistrates. professional magistrates and judges which are members of the Judicial Profession
- *Policy and Practices of the server signing service:* document that establishes the set of specific rules and procedures followed by the FNMT-RCM for the provision of its server signing service.
- *Registration Operations Officer*: a natural person appointed by the representative of the Public Administration, public agency or public-law entity whose duty it is to

oversee the tasks assigned to the *Registration Office*, and who has the obligations and responsibilities provided for in these *Specific Policies and Certification Practices*.

- *Subscriber*: the Public Administration, public body, agency or public-law entity.

1.6.2. References

41. The following references apply for the purposes of the provisions of this *SPPS*, their meaning being in accordance with European standard ETSI EN 319 411 "Policy and security requirements for Trust Service Providers issuing certificates":

CA: Certification Authority

AR: Registration Authority

ARL: Certification Authority Revocation List

CGPJ: General Council of the Judiciary (Consejo General del Poder Judicial)

CN: Common Name

CRL: *Certificate* Revocation List

DN: Distinguished Name

CPS: Certification Practice Statement

GCPS: Trust Services Practices and Electronic Certification General Statement

eIDAS: Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

ETSI: European Telecommunications Standards Institute

HSM: Hardware Security Module. This is a security module that generates and protects cryptographic passwords.

LCP: Lightweight *Certificate* Policy

NCP: Normalised *Certificate* Policy

NCP+: Extended Normalised *Certificate* Policy

OCSP: Online *Certificate* Status Protocol

OID: Object IDentifier

PIN: Personal Identification Number

PKCS: Public Key Cryptography Standards developed by RSA Laboratories

SIGOC: Integrated Management System for Judicial Bodies and the Judicial Professions

TLS/SSL: Transport Layer Security/Secure Socket Layer protocol.

UTC: Coordinated Universal Time.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORY

42. Being a *Trust Service Provider*, FNMT-RCM has a public information repository available 24x7x365, with the characteristics set out in the following sections, and accessible at the following address:

https://www.sede.fnmt.gob.es/descargas

2.2. PUBLICATION OF CERTIFICATION INFORMATION

43. Information on the issuance of electronic *Certificates* subject of this *SPPS* is published at the following address:

https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

2.3. TIME AND FREQUENCY OF PUBLICATION

44. Any amendment to the *Trust Services Practices and Electronic Certification General Statement* or to the *Specific Certification Policy and Practice Statement* will be published immediately at the URL where they may be accessed.

45. The CRL publication frequency is defined in section "4.9.7 Additional features. Time and frequency of publication".

2.4. ACCESS CONTROLS ON REPOSITORIES

46. The above repositories are all freely accessible to search for and, where appropriate, download information. In addition, FNMT-RCM has established controls to prevent unauthorised persons from adding, altering or deleting information included in its repositories and to protect the authenticity and integrity of that information.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

47. *Certificate* encoding is based on the RFC 5280 standard "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". All the fields defined in the *Certificate* profile in the *Specific Certification Policies and Certification Practices,* other than fields specifically providing otherwise, use the UTF8String encoding.

3.1.1. Types of names

48. The end-entity electronic *Certificates* subject of this *SPPS* contain a distinguished name (*DN*) in the Subject Name field, composed as described in the information on the Certificate profile.

49. In processing proof of identity prior to issuing *Electronic Certificates,* FNMT-RCM shall, through the *Registration Office,* ascertain the *Signatory's* true identity and retain the supporting documentation.

3.1.2. Need for names to be meaningful

50. All distinguished names (*DNs*) of the Subject Name field are meaningful. The description of the attributes associated with the *Certificate Subscriber* is human-readable (see section 7.1.4 Name forms hereof).

51. The Common Name field of *Judicial Career Certificates* defines the *member of the Judiciary* to whom the Certificate has been issued.

3.1.3. Anonymity or pseudonymity of subscribers

52. The use of pseudonyms as a method for identifying the Subscriber is not allowed for the Certificates issued under the present SPPS.

3.1.4. Rules for interpreting various name forms

53. The requirements defined by X.500 referred to in standard ISO/IEC 9594 are applied.

3.1.5. Uniqueness of names

54. The distinguished name (*DN*) assigned to *Certificates* issued to a *Subject* under these SPPS within the *Trust Service Provider's* domain will be unique.

3.1.6. Recognition, authentication and role of trademarks

55. FNMT–RCM makes no warranty whatsoever regarding the use of distinctive signs, whether registered or otherwise, with respect to *Certificates* issued under this *Certification Policy. Certificates* including distinctive signs may only be requested where the right to use the sign belongs or is duly licensed to the *Owner*. FNMT–RCM is under no obligation to previously check the ownership or registration of distinctive signs before issuing the *Certificates,* even where they are recorded in public registers.

3.2. INITIAL IDENTITY VALIDATION

3.2.1. Methods to prove possession of private key

56. The issuance of *Centralised Certificates* shall require that the *Applicant,* a *member of the Judiciary,* generate the *Public and private keys* in FNMT-RCM's system, after being registered therein and once that generation is validated by the *Registration Office*, after the aforementioned *Applicant's* identity has been checked and the *Applicant's* consent has been obtained.

57. In the case of *Centralised Certificates*, after the *Applicant* is informed that the *Applicant's Certificate* is to be issued, the system generates the *Key* pair, and the *Private Key* will therefore be stored and protected, guaranteeing that its use will be exclusively controlled by the *member of the Judiciary*.

3.2.2. Authentication of organisation identity

58. Before entering into any institutional relationship with *Subscribers*, FNMT-RCM uses the website addresses and means referred to in these *Specific Certification Practices* and otherwise the *GCPS* to inform about the terms of service and representations, warranties and responsibilities of the parties involved in the issuance and use of the *Certificates* issued thereby in its capacity as *Trust Service Provider*.

59. The identity checks of *members of the Judiciary*, *Applicants* for *Judicial Career Certificates*, will be carried out by authorised employees of the *Registration Offices* set up by the relevant Public Administration body, agency or entity, thereby guaranteeing the identity of the *Administration Subscriber* of the *Certificate*.

60. Therefore, and in this connection, *Registration Offices* shall not be deemed to be authorities with powers delegated by or reporting to FNMT-RCM.

3.2.3. Authentication of individual applicant identity

61. This Certificate can be issued to all the *members of the Judiciary* composed of Judges, Magistrates and Magistrates of the Supreme Court. Moreover, it can also be issued to acting Judges and Magistrates during their appointment period.

62. For the record, FNMT-RCM will consider, based on the list of *members of the Judiciary* submitted by the Administration, public agency or entity, for which the relevant body, agency and/or entity will be responsible, acting through the *Registration Offices*, that these are incumbent employees, that their Personal Identification number, employment or authorisation is authentic and in force and, therefore, that they have authority to obtain and use Judicial Career Centralised Certificates. FNMT-RCM shall not be responsible, insofar as this type of Certificate is concerned, for checking the member's position or employment or that these requirements continue to be met throughout the life of the Certificate, because FNMT-RCM has no legal civil service, administrative or employment relationship whatsoever with those employees, beyond the document containing the terms of use or, as the case may be, the issuance agreement, the effect of which is strictly instrumental for the discharge of employment-related duties.

63. These *Certificates* are issued with the intervention of the General Council of the Judiciary, which has the capacity of ensure the person identified in the Certificate's status as a *member of the Judiciary* and assign the professional identification number, which is unique and non-transferable, to each *member of the Judiciary*.

64. The above-mentioned checks shall be carried out by officers at the *Registration Offices* set up by the relevant Public Administration body, agency or entity, which shall in each case be the agency or entity where the *judicial professionals* perform jurisdictional functions. Therefore, and in this connection, *Registration Offices* shall not be deemed to be authorities with powers delegated by or reporting to FNMT-RCM.

3.2.3.1 Direct check by physical presence

65. *Applicants* for *Judicial Career Certificates* shall be physically present in order for their personal identity to be formally confirmed, through any of the identification means legally

admitted under the national laws in force, and will go to the *Registration Office* designated for that purpose by the *Subscriber* body, public agency or entity where the *Applicant* is employed. That *Registration Office* is created by the *Subscriber* Public Administration, which provides FNMT-RCM with a list of persons authorised to perform these Registration activities, in accordance with the procedures established for such purpose, and notifies any change to the Office structure.

3.2.3.2 Indirect check by reliable means equivalent to physical presence under national Law

66. There will be no need for physical presence where the *Registration Office* of the competent Administration body is acquainted with the identity or other permanent circumstances of the applicants for the *Certificates* (identity, validity of the position and other terms to be included in the *Certificate*) based on a previously existing relationship between those *Applicants* and the Administration where they serve, provided that it is guaranteed that those *Applicants* (member of Judiciary) were identified by physical presence (as described in the preceding paragraph), and less than five years have elapsed since their physical presence.

3.2.4. Non-verified Subscriber information

67. All information included in the electronic *Certificate* is verified by the *Registration Authority*.

3.2.5. Validation of authority

68. The Registration Authority verifies that the *Applicant* for a Judicial Career Certificate issued under this SPPS has been previously authorised by the Subscriber to submit that application.

3.2.6. Criteria for interoperation

69. There are no interactivity relationships with Certification Authorities external to FNMT-RCM.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

70. Under these Certification Policies, FNMT-RCM makes no provision for a re-keying process.

71. The authentication terms for a renewal request are set out in the section dealing with the Certificate renewal procedure hereof.

3.3.1. Identification and authentication for routine re-key

72. Under these Certification Policies, FNMT-RCM makes no provision for routine renewal.

3.3.2. Identification and authentication for re-key after revocation

73. Under these Certification Policies, FNMT-RCM makes no provision for renewal after revocation.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

74. Before actually revoking the *Certificates*, the Registration Authority shall authoritatively identify who requested the Revocation to link them to the unique data of the *Certificate* to be revoked.

75. The authentication terms for a revocation request are set out in the relevant section hereof dealing with the *Certificate* revocation procedure.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who can submit a Certificate application

76. Only members of the Judiciary, composed of Judges, Magistrates and Magistrates of the Supreme Court, may apply for this type of Certificates. Moreover, acting Judges and Magistrates may apply during their appointment period.

4.1.2. Registration process and responsibilities

77. *Applicants, members of the Judiciary,* through *Certificate* application web-based software developed for that purpose, will accept the terms of use of the *Certificate* and provide their identification particulars, including, but not limited to, Tax Identification Number (NIF), first surname, and their email address to which an application code shall be sent.

78. After receiving this information, FNMT-RCM will check that the information on the signed application is valid, and the size of keys generated.

79. Section 9.8 “Responsibilities” hereof defines the parties’ responsibilities in this process.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing identification and authentication functions

80. For *Judicial Career Certificates*, *Applicants* will supply the requested information and evidence of their personal identity and status as a *member of the Judiciary*. FNMT-RCM shall in any event accept the function performed and report prepared by the Administration’s designated *Registration Office.*

81. In the case of *Centralised Certificates*, *Applicants* shall, during the process to establish their identity, sign the terms of use of the *Certificate*, and will be provided with identification credentials, finally, *Applicants* shall configure an *Activation Code*.

82. FNMT-RCM may agree with Administrations, public agencies and entities so requesting to create delegated Registration Offices in order to centralise the performance of registration procedures for other related or dependent Administrations that do not have sufficient means to do so, in conformity with cost rationalisation laws.

4.2.2. Approval or rejection of certificate applications

83. In the case of *Centralised Certificates,* once the information is confirmed, the *Applicant* shall be registered in FNMT-RCM's system to be provided with complete identity credentials. Keys will be generated once the *Signatory* configures the signature password which shall protect the keys and request generation of signature identity. These actions will be carried out accessing the *Certificate* application software (Identity Management Portal) with a high level of security.

84. Information will be submitted to FNMT-RCM via secure communications established for such purpose between the *Registration Office* and FNMT-RCM.

85. FNMT-RCM will have *Applicants* provide such information received from the *Registration Office* as may be necessary for the *Certificates* to be issued and for the identity to be checked, storing the information required by electronic signature laws for a period of fifteen (15) years, duly processing that information in compliance with the national personal data protection laws in force from time to time.

86. Personal information and processing of such information shall be subject to specific laws.

4.2.3. Time to process applications

87. An approved application for *Judicial Career Centralised Certificate* is automatically processed by the system, so there is no stipulated time for this process.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA actions during issuance

88. Once FNMT-RCM receives the *Applicant's* personal information, information describing the *Applicant's* relationship with the CGPJ and/or its dependent components, and the application code obtained at the application stage, the *Certificate* will be issued.

89. The issuance of *Certificates* results in the generation of electronic documents confirming the information to be included in the *Certificate*, and that it matches the associated *Public Key*. FNMT-RCM *Certificates* may only be issued by FNMT-RCM in its capacity as *Trust Service Provider*, and no other entity or organisation has authority to issue the same. The FNMT-RCM *Certification Authority* only accepts *Certificate* generation applications from authorised sources. The information contained in each application is fully protected against alterations through *Electronic Signature* mechanisms prepared using *Certificates* issued to those authorised sources.

90. FNMT-RCM will in no case have a *Certificate* include information other than that referred to herein, or any circumstances, specific attributes of the *Signatories* or restrictions other than as provided for in the agreements or arrangements and, as the case may be, those provided for in the relevant *Issuance Law*.

91. In any case, FNMT-RCM will use its best efforts:

- To check that the *Certificate Applicant* or the *Registration Operations Officer* use the *Private Key* for the *Public Key* linked to the *Certificate.* FNMT-RCM will therefore check that the *Private Key* corresponds to the *Public Key*.
- To ensure that the information included in the *Certificate* is based on the information provided by the relevant *Registration Office*.
- Not to ignore known facts potentially affecting *Certificate* reliability.
- To ensure that the *DN* (distinguished name) assigned to a *Subject* under this SPPS is unique.

92. The following steps will be taken to issue the *Certificate*:

1. Certificate data structure composition.

   The data collected when processing the Certificate application is used to compose the distinguished name (DN) based on standard X.500, making sure that the name is meaningful and unambiguous.

   The attribute CN contains the *member of the Judiciary*'s identification data, following the corresponding *Certificate*'s profile.

2. Certificate generation in accordance with the relevant Certificate profile.

93. The form of *Certificates* issued by FNMT-RCM under this *Certification Policy*, in keeping with standard UIT-T X.509 version 3 and under the laws applicable to *Qualified Certificates*, may be viewed at http://www.cert.fnmt.es/dpcs/.

94. Within the process of issuing the *Judicial Career Certificates in QSCD*, it will be verified that the device used to generate authentication and signing keys is a *Qualified signature creation device* (*QSCD*) in accordance with the eIDAS Regulation.

95. In processing issuance of *Centralised Certificates,* the system requires *Applicants* to identify themselves using the credentials received plus a second authentication factor which shall be sent to their email address[1] and, once their identity has been verified, they must expressly request the issuance of their *Centralised Certificate.* The infrastructure thereby securely links the identification details provided by Applicants, as described in section "4.1.2 Registration process" hereof, with the process to generate their *Certificate*.

96. The system will then generate the *Public and private keys* in a protected HSM and issue the requested *Centralised Signature Certificate* to the members of the Judiciary. In addition, the system requires *Applicants* to establish their signature password which they will have be asked to provide when carrying out transactions using their *Private Key*. This password is not known (or stored) at any time by FNMT-RCM's system.

[1] FNMT-RCM may use other communication methods to submit this second authentication factor, subject to the *Applicant's* prior consent, namely for instance the use of mobile telephones with a previously accredited number.

4.3.2. Notification of issuance

97. Upon the *Certificate* being issued, FNMT-RCM will inform *members of the Judiciary* that the *Certificate* is available for download.

4.4. ACCEPTANCE OF THE CERTIFICATE

4.4.1. Conduct constituting certificate acceptance

98. During the *Certificate* application process, *members of the Judiciary* accept the terms of use and express their willingness to obtain the *Certificate*, and the requirements necessary for the *Certificate* to be generated.

4.4.2. Publication of the certificate by the CA

99. *Certificates* generated are stored in a secure repository of FNMT-RCM, with restricted access.

4.4.3. Notification of issuance to other entities

100. Notification of issuance is not provided to other entities.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Private Key and certificate usage

101. FNMT-RCM generates and stores the Private Keys associated with *Centralised Certificates*.

102. These Certificates are valid electronic signature systems as provided for in Public Sector Legal Regime Act 40/2015, 1 October, and in Justice Administration Information and Communication Technologies Use Act 18/2011, 5 July.

4.5.2. Relying party public key and certificate usage

103. Third parties relying on *Electronic signatures* based on the *Private keys* associated with the *Certificate* shall observe the representations and warranties defined in this *SPPS*.

4.6. CERTIFICATE RENEWAL

104. FNMT-RCM does not renew *Certificates* under these *Certification Policies* maintaining their *Public key*.

4.6.1. Circumstances for certificate renewal

105. FNMT-RCM does not renew *Certificates* under these *Certification Policies* maintaining their *Public key*.

4.6.2. Who may request renewal

106. FNMT-RCM does not renew *Certificates* under these *Certification Policies* maintaining their *Public key*.

4.6.3. Processing certificate renewal requests

107. FNMT-RCM does not renew *Certificates* under these *Certification Policies* maintaining their *Public key*.

4.6.4. Notification of new certificate issuance to subscriber

108. FNMT-RCM does not renew *Certificates* under these *Certification Policies* maintaining their *Public key*.

4.6.5. Conduct constituting acceptance of a renewal certificate

109. FNMT-RCM does not renew *Certificates* under these *Certification Policies* maintaining their *Public key*.

4.6.6. Publication of the renewal certificate by the CA

110. FNMT-RCM does not renew *Certificates* under these *Certification Policies* maintaining their *Public key*.

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

111. FNMT-RCM does not renew *Certificates* under these *Certification Policies* maintaining their *Public key*.

4.7. CERTIFICATE RE-KEY

112. Under these Certification Policies, *Certificate* re-key is always carried out issuing new keys, following the same process described for a new *Certificate* to be issued.

4.7.1. Circumstances for certificate re-key

113. *Certificates* shall be re-keyed in the following events:

- Where the current keys will expire soon, upon request by the renewal requestor.
- Due to key compromise or any other circumstance set out in section "*4.9 Certificate revocation and suspension"* of this *SPPS.*

4.7.2. Who may request re-key

114. The same process described for the issuance of a new *Certificate* will be followed.

4.7.3. Processing certificate re-keying requests

115. The same process described for the issuance of a new *Certificate* will be followed.

4.7.4. Notification of certificate re-key

116. The same process described for the issuance of a new *Certificate* will be followed.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

117. The same process described for the issuance of a new *Certificate* will be followed.

4.7.6. Publication of the re-keyed certificate

118. The same process described for the issuance of a new *Certificate* will be followed.

4.7.7. Notification of certificate re-key to other entities

119. The same process described for the issuance of a new *Certificate* will be followed.

4.8. CERTIFICATE MODIFICATION

120. *Certificates* issued cannot be modified. Therefore, any modification required shall result in a new *Certificate* being issued.

4.8.1. Circumstance for certificate modification

121. The modification is not stipulated.

4.8.2. Who may request certificate modification

122. The modification is not stipulated.

4.8.3. Processing certificate modification requests

123. The modification is not stipulated.

4.8.4. Notification of new certificate issuance to subscriber

124. The modification is not stipulated.

4.8.5. Conduct constituting acceptance of modified certificate

125. The modification is not stipulated.

4.8.6. Publication of the modified certificate by the CA

126. The modification is not stipulated.

4.8.7. Notification of the certificate issuance by the CA to other entities

127. The modification is not stipulated.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

128. *Certificates* issued by FNMT-RCM will cease to be valid in the following cases:

a) Termination of the *Certificate* validity period.

b) Discontinuance of FNMT-RCM's activity as a *Trust Service Provider* unless, subject to the *Subscriber's* prior express consent, the *Certificates* issued by FNMT-RCM have been transferred to another *Trust Service Provider*.

In these two cases [a) and b)], the Certificates will cease to be valid forthwith upon the occurrence of these circumstances.

c) Revocation of the Certificate in any of the events provided for herein.

129. Revocation of the *Certificate*, i.e. termination of its validity, shall be effective from the date on which FNMT-RCM actually learns of the occurrence of any trigger events and records that in its *Certificate status information and checking service*.

130. FNMT-RCM provides *Subscribers*, relying parties, software providers and third parties with a communication channel through the FNMT-RCM website https://www.sede.fnmt.gob.es/

4.9.1. Circumstances for revocation

4.9.1.1 Reasons for revoking a subscriber certificate

131. The *Certificate* revocation request may be made during the validity period specified in the *Certificate.*

132. The following are admissible grounds for a *Certificate* to be revoked:

a) Revocation request by authorised persons. This request shall in any case be based on:

- Third-party use of the *Private Key* associated with the *Certificate.*
- Breach or compromise of the *Signature Creation Data* or of the private key associated with the *Certificate.*
- The failure to accept new terms resulting from the issuance of new *Certification Policy and Practice Statements*, during a period of one month after publication.

b) Court or administrative ruling ordering revocation.

c) Termination or dissolution of the *Subscriber's* legal personality.

d) Death or subsequent total or partial incapacity of the *Signatory* or of the *Subscriber's* representative.

e) Inaccurate data supplied by the *Applicant* to obtain the *Certificate*, or alteration of the data supplied to obtain the *Certificate* or change of the circumstances checked for the

Certificate to be issued, and in relation to the position held or powers conferred, to the extent that the *Certificate* no longer reflects the true facts.

f) Breach of a material obligation provided for in this *Certification Policy and Practice Statement* by the *Certificate Signatory* or *Applicant*, or by a *Registration Office* if, in the latter case, that may have affected the procedure to issue the *Certificate*.

g) Breach or compromise of the Private Key Signature Creation Data.

h) Termination of the agreement entered into between the *Signatory* or the Subscriber and FNMT-RCM.

i) Breach of a material obligation provided for in this *Certification Policy and Practice Statement* by a *Registration Office* where that may have affected the process to issue the *Certificate*.

j) Discontinuance of the *Trust Service Provider's activity* unless management of the electronic *Certificates* issued thereby is transferred to another *Trust Service Provider*.

k) Cancellation of the *Signatory's* identification credentials in the case of *Centralised Signature Certificates.*

l) Loss of qualified electronic signature creation device (QSCD) certification status in the case of *Centralised Signature Certificates.*

133. FNMT-RCM shall in no case accept any obligation whatsoever to check the particulars referred to in c) to e) above, which this entity must be duly notified of by delivering the documents and information required for the same to be checked.

134. FNMT-RCM will only be responsible for the consequences of the failure to revoke a *Certificate* in the following events:

- Where it should have been revoked following termination of the agreement entered into with the *Subscriber.*
- Where revocation was requested through the *Subscriber's* relevant *Registration Office* observing the procedure established for this type of *Certificates*.
- Where it received notice of the revocation request or the underlying cause by means of a court or administrative decision.
- Where it is duly provided with proof of the grounds referred to in c) to e) above, after the revocation *Requestor* is identified.

135. FNMT-RCM shall be held harmless in the event of actions in the nature of criminal offences or misdemeanours which FNMT-RCM is unaware of in connection with the data or the *Certificate*, data inaccuracies or untimely communication thereof to FNMT-RCM.

136. In addition to their termination and the inability to carry on using the *Signature creation data* or associated private keys, the revocation of a *Certificate* terminates the relationship and terms of use of that *Certificate* and its *Private key* with FNMT-RCM.

4.9.1.2 Reasons for revoking a subordinate CA certificate

137. The provisions of the "FNMT-RCM Public Key Infrastructure Compromise Action Plan" will be observed.

4.9.2. Who can request revocation

138. Revocation of a *Certificate* may only be requested by:

- the *Certification Authority* and the *Registration Authority*
- the *Subscriber* through its representative or authorised person, at the Registration Office with authority for that purpose
- as the case may be, the *Signatory,* calling the telephone number provided for that purpose (subject to identification of the Requestor) and posted at FNMT-RCM's website, which shall be operational 24x7, or through that Registration Office.

139. FNMT-RCM may revoke the *Certificates* of its own accord in the events referred to in this Certification Policy and Practice Statement.

4.9.3. Procedure for revocation request

140. A *Judicial Career Certificate's* revocation request may be made during the validity period specified in the *Certificate*.

141. Revocation may be processed continuously 24x7 through the telephone Revocation Service available to users for such purpose, and revocation of the *Certificate* is guaranteed within less than 24h.

142. During telephone revocation, the requestor shall have to provide whatever details may be required, and supply such information as may be essential to unequivocally validate the requestor's authority to request revocation.

143. Additionally, a request for revocation of any *Certificate* may be made through the *Registration Office.* Personal information and processing of such information shall be subject to specific laws. The revocation process at the Registration Office is as follows:

i. For *Judicial Career Centralised Certificates,* the requestor shall go to the *Registration Office,* where the requestor's identity shall be established, along with the requestor's capacity to revoke that *Certificate,* and the ground for revocation shall be specified. The Office will send the information to FNMT-RCM electronically using registration software, and will process revocation of the *Certificate.*

144. As soon as revocation is effective, the following will be notified using the email address provided:

i. The *Signatory* and the requestor in the case of a *Judicial Career Certificate*

145. Once FNMT-RCM has processed *Certificate* revocation, the relevant *Certificate Revocation List* will be published in the secure *Directory,* including the revoked *Certificate* serial number, along with the date, time and reason for revocation. Once a *Certificate* is revoked, its validity shall definitively terminate and revocation may not be reversed.

146. In order to report suspected Private Key Compromise, *Certificate* misuse, or other types of fraud, inappropriate conduct or any other matter related to Certificates, a certificate problem request (CPR) can be sent to the email address incidentes.ceres@fnmt.es as indicated in section 1.5.2.

4.9.4. Revocation request grace period

147. No grace period is associated with this process, for revocation occurs forthwith upon verified receipt of the revocation request.

4.9.5. Time within which to process the revocation request

148. FNMT-RCM processes *Certificate* revocation immediately upon checking the *Requestor's* identity or, as the case may be, once the authenticity of a request made by means of a court or administrative decision has been checked. In any case, the *Certificate* will be effectively revoked within less than 24 hours of the revocation request being received.

4.9.6. Revocation checking requirement for relying parties

149. Third parties relying on and accepting the use of the *Certificates* issued by FNMT-RCM must check, by any of the available means (CRL Revocation Lists and/or OCSP), the status of the *Certificates*:

- the *Advanced Electronic Signature* of the *Trust Service Provider* issuing the *Certificate,*
- that the *Certificate* is still valid and active, and
- the status of the *Certificates* included in the *Certification Chain.*

4.9.7. CRL issuance frequency

150. *Judicial Career Centralised Certificate*'s *Revocation Lists (CRLs*) are issued at least every 12 hours, or whenever a revocation occurs, and they are valid for a period of 24 hours. *Authority Certificate CRLs* are issued every 6 months, or whenever a subordinate *Certification Authority* revocation occurs, and they are valid for a period of 6 months.

4.9.8. Maximum latency for CRLs

151. *Revocation Lists* are published upon being generated, and therefore there is no latency between CRL generation and publication.

4.9.9. Online revocation/status checking availability

152. On-line *Certificate* revocation/status information will be available 24x7. In the event of system failure, the Business Continuity Plan shall be put in place to resolve the incident as soon as possible.

4.9.10. Online revocation verification requirements

153. The revocation status of *Judicial Career Centralised Certificate* may be checked on line through the OCSP *Certificate status information service* offered as described in section 4.10 below. The party interested in using that service must:

- Check the address contained in the *Certificate* AIA (Authority Information Access) extension.
- Check that the OCSP response is signed / sealed.

4.9.11. Other forms of revocation advertisements available

154. Not defined.

4.9.12. Special requirements related to key compromise

155. See the relevant section in the *GCPS*.

4.9.13. Circumstances for suspension

156. *Certificate* suspension is not supported.

4.9.14. Who can request suspension

157. *Certificate* suspension is not supported.

4.9.15. Procedure for suspension request

158. *Certificate* suspension is not supported.

4.9.16. Limits on suspension period

159. *Certificate* suspension is not supported.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational characteristics

160. Validation information regarding the electronic *Certificates* subject of this *SPPS* is accessible using the means described in the *GCPS*.

4.10.2. Service availability

161. FNMT-RCM guarantees 24x7 access to this service by *Certificate Users* and relying parties securely, quickly and free of charge.

4.10.3. Optional features

162. Not stipulated.

4.11. END OF SUBSCRIPTION

163. Subscription will end when the Certificate ceases to be valid, whether upon the validity period ending or due to revocation thereof. If the Certificate is not renewed, the relationship between the Signatory and FNMT-RCM will be deemed to have terminated.

164. It is noted in the above connection that where an application for FNMT-RCM to issue a Judicial Career Centralised Certificate and the same Signatory and same Subscriber have another Certificate in force under the same Issuance Law, the first Certificate obtained will be revoked.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key escrow and recovery policy and practices

165. FNMT-RCM will not recover the *Private keys* associated with the *Certificates*.

166. In the case of *Judicial Career Centralised Certificates,* where the password protecting access to that *Key* by the *Signatory* is lost, that *Certificate* must be revoked and a request must be made for a new one to be issued.

4.12.2. Session key encapsulation and recovery policy and practices

167. No stipulation.

5. PHYSICAL SECURITY, PROCEDURAL AND PERSONNEL CONTROLS

168. See the relevant section in the *GCPS*.

5.1. PHYSICAL SECURITY CONTROLS

169. See the relevant section in the *GCPS*.

5.1.1. Site location and construction

170. See the relevant section in the *GCPS*.

5.1.2. Physical access

171. See the relevant section in the *GCPS*.

5.1.3. Power and air conditioning

172. See the relevant section in the *GCPS*.

5.1.4. Water exposures

173. See the relevant section in the *GCPS*.

5.1.5. Fire prevention and protection

174. See the relevant section in the *GCPS*.

5.1.6. Media storage

175. See the relevant section in the *GCPS*.

5.1.7. Waste disposal

176. See the relevant section in the *GCPS*.

5.1.8. Off-site backup

177. See the relevant section in the *GCPS*.

5.2. PROCEDURAL CONTROLS

178. See the relevant section in the *GCPS*.

5.2.1. Trusted roles

179. See the relevant section in the *GCPS*.

5.2.2. Number of persons required per task

180. See the relevant section in the *GCPS*.

5.2.3. Identification and authentication for each role

181. See the relevant section in the *GCPS*.

5.2.4. Roles requiring separation of duties

182. See the relevant section in the *GCPS*.

5.3. PERSONNEL CONTROLS

183. See the relevant section in the *GCPS*.

5.3.1. Qualifications, experience, and clearance requirements

184. See the relevant section in the *GCPS*.

5.3.2. Background check procedures

185. See the relevant section in the *GCPS*.

5.3.3. Training requirements

186. See the relevant section in the *GCPS*.

5.3.4. Retraining frequency and requirements

187. See the relevant section in the *GCPS*.

5.3.5. Job rotation frequency and sequence

188. See the relevant section in the *GCPS*.

5.3.6. Sanctions for unauthorized actions

189. See the relevant section in the *GCPS*.

5.3.7. Independent contractor requirements

190. See the relevant section in the *GCPS*.

5.3.8. Documentation supplied to personnel

191. See the relevant section in the *GCPS*.

5.4. AUDIT-LOGGING PROCEDURES

192. See the relevant section in the *GCPS*.

5.4.1. Types of events recorded

193. See the relevant section in the *GCPS*.

5.4.2. Frequency of processing log

194. See the relevant section in the *GCPS*.

5.4.3. Retention period for audit log

195. See the relevant section in the *GCPS*.

5.4.4. Protection of audit log

196. See the relevant section in the *GCPS*.

5.4.5. Audit log backup procedures

197. See the relevant section in the *GCPS*.

5.4.6. Log collection systems

198. See the relevant section in the *GCPS*.

5.4.7. Notification to event-causing subject

199. See the relevant section in the *GCPS*.

5.4.8. Vulnerability assessments

200. See the relevant section in the *GCPS*.

5.5. RECORDS ARCHIVAL

201. See the relevant section in the *GCPS*.

5.5.1. Types of records archived

202. See the relevant section in the *GCPS*.

5.5.2. Retention period for archive

203. See the relevant section in the *GCPS*.

5.5.3. Protection of archive

204. See the relevant section in the *GCPS*.

5.5.4. Archive backup procedures

205. See the relevant section in the *GCPS*.

5.5.5. Requirements for time-stamping of records

206. See the relevant section in the *GCPS*.

5.5.6. Log collection systems

207. See the relevant section in the *GCPS*.

5.5.7. Procedures to obtain and verify archive information

208. See the relevant section in the *GCPS*.

5.6. CA KEY CHANGEOVER

209. See the relevant section in the *GCPS*.

5.7. COMPROMISE AND DISASTER RECOVERY

210. See the relevant section in the *GCPS*.

5.7.1. Incident and compromise handling procedures

211. See the relevant section in the *GCPS*.

5.7.2. Computing resources, software, and/or data are corrupted

212. See the relevant section in the *GCPS*.

5.7.3. Entity private key compromise procedures

213. See the relevant section in the *GCPS*.

5.7.4. Business continuity capabilities after a disaster

214. See the relevant section in the *GCPS*.

5.8. TRUST SERVICE PROVIDER TERMINATION

215. See the relevant section in the *GCPS*.

6. TECHNICAL SECURITY CONTROLS

216. See the relevant section in the *GCPS*.

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key pair generation

6.1.1.1 CA key pair generation

217. As for the CA *Key* generation FNMT-RCM needs to carry out its activity as *Trust Service provider,* see the relevant section in the *GCPS*.

6.1.1.2 RA key pair generation

218. No stipulation.

6.1.1.3 Subscriber key pair generation

219. *Private Keys* associated with the *Judicial Career Certificates in QSCD* are generated and kept in a *Qualified signature creation device* that meets the requirements listed in Annex II of the eIDAS Regulation.

220. *Private keys* associated with *Judicial Career Centralised Certificates* are generated and held securely by FNMT-RCM's signature activation module, so that those *Keys* are accessed by means reliably guaranteeing exclusive control by the *Signatory*.

6.1.2. Private key delivery to the subscriber

221. There is no Private key delivery in the issuance of *Certificates* under these *Certification Policies and Practices*.

222. The *Private keys* associated with *Judicial Career Centralised Certificates* are generated in a signature creation device exclusively controlled by the *Signatory*, where they will be held securely for use. The *Private key* is not therefore delivered to the *Signatory* in this case.

223. In any case, if FNMT-RCM or any registration office should become aware of unauthorised access to the *Signatory's Private key*, the *Certificate* associated with that *Private key* will be revoked.

6.1.3. Public key delivery to certificate issuer

224. The *Public key* generated with the *Private key* on a key generation and custody device is delivered to the Certification Authority sending a certification request.

6.1.4. CA public key delivery to relying parties

225. Véase el apartado correspondiente en la *DGPC*.

6.1.5. Key sizes and algorithms used

226. The algorithm used is RSA with SHA-256.

227. As for key size, depending on each case, that is:

- Root FNMT CA keys: 4096 bits.
- Subordinate Public Sector CA Keys*:* 4096 bits.
- *Judicial Career Centralised Certificate's keys:* 2048 bits.

6.1.6. Public key parameters generation and quality checking

228. See the relevant section in the *GCPS*.

6.1.7. Key usage purposes (KeyUsage field X.509v3)

229. FNMT *Certificates* include the extension Key Usage and, as appropriate, Extended Key Usage, indicating *Key* usage purposes.

230. The root FNMT CA *Certificate Key* usage purposes are to sign/seal Subordinate FNMT CA *Certificates* and ARLs.

231. The *Certificate* usage purpose of Subordinate FNMT CAs issuing *Judicial Career Centralised Certificates* is exclusively to sign/seal end-entity *Certificates* and CRLs.

232. The usage purpose of *Judicial Career Centralised Certificates* is exclusively use of signature.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic module standards and controls

233. See the relevant section in the *GCPS*.

6.2.2. Private key (n out of m) multi-person control

234. See the relevant section in the *GCPS*.

6.2.3. Private key escrow

235. Copying, safeguarding or recovery of FNMT-RCM Certification Authority *Private keys* is exclusively controlled by authorised personnel, using at least dual control and in a secure environment.

236. *Private Keys* associated with the *Judicial Career Certificates in QSCD* are generated and kept in a *Qualified signature creation device* that meets the requirements listed in Annex II of the eIDAS Regulation.

237. The *Private keys* of *Judicial Career Centralised Certificates* issued to end users (*Signatories*) are held safely in FNMT-RCM's systems so that only *Signatories* may access their *Private key*. Access is guaranteed through the use of *Signatories'* identification credentials and their signature password (only known to *Signatories*), plus a second authentication factor consisting of a single-use password.

6.2.4. Private key backup

238. See the relevant section in the *GCPS*.

6.2.5. Private key archival

239. See the relevant section in the *GCPS*.

6.2.6. Private key transfer into or from a cryptographic module

240. See the relevant section in the *GCPS*.

6.2.7. Private key storage on cryptographic module

241. See the relevant section in the *GCPS*.

6.2.8. Activating private keys

242. Certification Authority *Private keys* are generated and held securely by a cryptographic device meeting the FIPS PUB 140-2 Level 3 security requirements.

243. The Certification Authority's *Private keys* are activated and used based on management and operation role segmentation implemented by FNMT-RCM, including multi-person access based on cryptographic cards and related PINs based on an M out of N (2 out of 5) simultaneous use pattern.

244. End-entity *Centralised Signature Certificate Private key* activation and use is based on use by *Signatories* of their identification credentials and signature password (known only to them), plus a second authentication factor in the form of a single-use password.

6.2.9. Deactivating private keys

245. See the relevant section in the *GCPS*.

6.2.10. Destroying private keys

246. FNMT-RCM will destroy or appropriately store the Trust Service Provider's Keys when their validity period is over, in order to prevent their inappropriate use.

247. End-entity *Judicial Career Centralised Certificates Private keys* will be destroyed once their period of use is over or when the *Signatories'* relationship with FNMT-RCM terminates. In any case, private key destruction shall be preceded by revocation of the *Centralised Certificate*.

6.2.11. Cryptographic module capabilities

248. See the relevant section in the *GCPS*.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public key archival

249. See the relevant section in the *GCPS*.

6.3.2. Certificate operational periods and key pair usage periods

250. Operational periods for the *Certificates* and their associated *Keys*:

- Root FNMT CA *Certificate* and Key pair: until 1 January 2030.
- *Certificate* of the Subordinate CA issuing *Electronic Signature and Electronic Seal Certificates* and Key pair: until 31 December 2029.
- *Judicial Career Centralised Certificates* and Key Pair: not in excess of 4 years.

6.4. ACTIVATION DATA

6.4.1. Activation data generation and installation

251. Key activation data generation for both the root FNMT CA and the subordinate CA issuing *Judicial Career Certificates* takes place during those *Certification Authorities'* Key generation ceremony.

252. Key activation data for *Public Employee Centralised Certificates* is generated by the signature activation module in the same manipulation-proof environment as the *Trust Service Provider's* signature creation device, guaranteeing that such generation can only be carried out under the future *Signatory's* exclusive control.

6.4.2. Activation data protection

253. The *Certification Authority's Private key* activation data is protected, as described in section "6.2.8 Activating private keys" above, with multi-person access based on cryptographic cards and related PINs based on an M out of N (2 out of 5) simultaneous use pattern.

254. The password protecting access to the *Judicial Career Centralised Certificate's Private key* is confidential, personal and non-transferable. *Signatories*, who also need a second authentication factor to activate their *Private key*, are therefore responsible for protecting their activation data.

6.4.3. Other aspects of activation data

255. No stipulations.

6.5. COMPUTER SECURITY CONTROLS

256. See the relevant section in the *GCPS*.

6.5.1. Specific computer security technical requirements

257. See the relevant section in the *GCPS*.

6.5.2. Computer security rating

258. See the relevant section in the *GCPS*.

6.6. LIFE CYCLE TECHNICAL CONTROLS

259. See the relevant section in the *GCPS*.

6.6.1. System development controls

260. See the relevant section in the *GCPS*.

6.6.2. Security management controls

261. See the relevant section in the *GCPS*.

6.6.3. Life cycle security controls

262. See the relevant section in the *GCPS*.

6.7. NETWORK SECURITY CONTROLS

263. See the relevant section in the *GCPS*.

6.8. TIME-STAMPING

264. See the relevant section in the *GCPS*.

6.9. OTHER ADDITIONAL CONTROLS

265. See the relevant section in the *GCPS*.

6.9.1. Control of the ability to provide services.

266. See the relevant section in the *GCPS*.

6.9.2. Control of systems development and computer applications

267. See the relevant section in the *GCPS*.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

268. *Judicial Career Certificates* are issued as "qualified" *Certificates* in accordance with European standards ETSI IN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" and ETSI IN 319 412-2 "Certificate profile for certificates issued to natural persons".

7.1.1. Version number

269. *Judicial Career Certificates* conform to standard X.509 version 3.

7.1.2. Certificate extensions

270. The document describing the profile of *Judicial Career Certificates* issued under this policy, including all extensions, is published at http://www.cert.fnmt.es/dpcs/.

271. All certificates issued under this *CP* shall contain a non-critical extension qcStatements using the predefined qcStatement-2 in RFC 3739, where all values in sematicsInformation shall be:

• semanticsIdentifier: id-etsi-qcs-semanticsId-Natural

• nameRegistrationAuthorities: https://poderjudicial.es (URI type generalName) Algorithm object identifiers

7.1.3. Algorithm object identifiers

272. The corresponding object identifier (OID) for the cryptographic algorithm used (SHA-256 with RSA Encryption) is 1.2.840.113549.1.1.11.

7.1.4. Name forms

273. *Judicial Career Certificates* encoding is based on the RFC 5280 recommendation "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Except where otherwise indicated in the relevant fields, the fields defined in the *Certificate* profile use UTF8String encoding.

274. The document describing the profile of *Judicial Career Certificates* issued under this policy, including all extensions, is published at http://www.cert.fnmt.es/dpcs/.

275. The semantics of the field serialNumber shall be as follows:

JU:ES-JXXXXXXXXXR,

where "xxxxxxxxx" is a personal, unique and non-transferable code given to each member of the Judiciary by the Integrated Management System for Judicial Bodies and the Judicial Professions (SIGOC) and "R" a control character.

7.1.5. Name constraints

276. The distinguished name (*DN*) assigned to the *Subject* of the *Certificate* under this *SPPS* shall be unique and be composed as defined in the *Certificate* profile.

7.1.6. Certificate policy object identifier

277. The *Judicial Career Centralised Certificate's* policy object identifier (OID) is defined in section "1.2 Document name and identification" above.

7.1.7. Usage of policy constraints extension

278. The root CA *Certificate* "Policy Constraints" extension is not used.

7.1.8. Policy qualifiers syntax and semantics

279. The "Certificate Policies" extension includes two "Policy Qualifier" fields:

- CPS Pointer: contains the URL where the *Certification Policies* and *Trust Service Practices* applicable to this service are posted.
- User notice: contains wording that may be displayed on the *Certificate* user's screen during verification.

7.1.9. Processing semantics for the critical certificate policies extension

280. The "Certificate Policy" extension includes the policy OID field, which identifies the policy associated with the *Certificate* by FNMT-RCM, as well as the two fields referred to in the preceding section.

7.2. CRL PROFILE

7.2.1. Version number

281. The CRL profile conforms to standard X.509 version 2.

7.2.2. CRL and CRL entry extensions

282. The CRL profile has the following structure:

Table 3 – CRL profile

Fields and extensions	Value
Version	V2
Signature algorithm	Sha256WithRSAEncryption
CRL number	Incremental value
Issuer	Issuer DN
Issuance date	UTC issuance time.
Date of next upgrade	Issuance date + 24 hours
Authority key identifier	Issuer key hash
Distribution point	Distribution point URLs and CRL scope
ExpiredCertsOnCRL	CA NotBefore value
Revoked Certificates	Certificate revocation list, containing at least serial number and revocation date for each entry

7.3. OCSP PROFILE

7.3.1. Version number

283. See the relevant section in the GCPS.

7.3.2. OCSP extensions

284. See the relevant section in the GCPS.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

285. The *Certificate* issuance system is audited on a yearly basis in conformity with European standards ETSI EN 319 401 “General Policy Requirements for Trust Service Providers” and ETSI EN 319 411-1 “Policy and security requirements for Trust Service Providers issuing certificates”.

286. Likewise, since Certificates are considered as qualified, audit ensures compliance with the requirements established in European standards ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates".

287. An independent auditor shall annually assess the CA's compliance with the requirements and practices established in this CPS.

288. Audit plans will be regularly prepared, covering at least the following actions:

i. Audit of the Information Security Management System in accordance with UNE-ISO / IEC 27001 “Information Security Management Systems. Requirements”.

ii. Audit of the Privacy Information Management System in accordance with UNE-ISO/ IEC 27701 “Privacy Information Management Systems Requirements”.

iii. Audit as ruled in the National Security Scheme (Royal Decree 311/2022, of May 3, which regulates the National Security Scheme in the field of Electronic Administration).

iv. Audit of the Quality Management System according to ISO 9001.

v. Audit of the Social Responsibility Management System in correspondence with IQNet SR10.

vi. Audit of the Business Continuity Plan according to ISO 22301.

vii. Audit in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/, and Organic Law 3/2018, of December 5th, on the Protection of Personal Data and guarantee of digital rights (RGPD / LOPD-GDD).

289. Risk analysis is also carried out, in accordance with the dictates of the Information Security Management System.

290. The *Certification Authority* issuing the *Judicial Career Certificates* is subject to regular audits, respectively in accordance with European standard ETSI IN 319 401 “General Policy Requirements for Trust Service Providers”, ETSI IN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates” and ETSI IN 319 412-2 “Certificate profile for certificates issued to natural persons”.

291. The ETSI audits mentioned in the previous section are carried out on a yearly basis by an external accredited firm.

292. The frequency of the remaining additional audits shall be in accordance with the relevant regulations in force.

8.2. QUALIFICATIONS OF ASSESSOR

293. See the relevant section in the *GCPS*.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

294. See the relevant section in the *GCPS*.

8.4. TOPICS COVERED BY ASSESSMENT

295. See the relevant section in the *GCPS*.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

296. See the relevant section in the *GCPS*.

8.6. COMMUNICATION OF RESULTS

297. See the relevant section in the *GCPS*.

8.7. AUTOEVALUATION

298. See the relevant section in the *GCPS*.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

299. See the relevant section in the *GCPS*.

9.1.1. Certificate issuance or renewal fees

300. See the relevant section in the *GCPS*.

9.1.2. Certificate access fees

301. No stipulation.

9.1.3. Revocation or status information access fees

302. FNMT-RCM offers CRL or OCSP certificate status information services free of charge.

9.1.4. Fees for other services

303. See the relevant section in the *GCPS*.

9.1.5. Refund policy

304. FNMT-RCM has a refund policy whereby a refund request may be made within the set withdrawal period, and accepts that this will result in automatic revocation of the certificate. The procedure is published at the FNMT-RCM website.

9.2. FINANCIAL RESPONSIBILITY

305. See the relevant section in the *GCPS*.

9.2.1. Insurance coverage

306. See the relevant section in the *GCPS*.

9.2.2. Other assets

307. See the relevant section in the *GCPS*.

9.2.3. Insurance or warranty coverage for end-entities

308. See the relevant section in the *GCPS*.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

309. See the relevant section in the *GCPS*.

9.3.1. Scope of confidential information

310. See the relevant section in the *GCPS*.

9.3.2. Information not within the scope of confidential information

311. See the relevant section in the *GCPS*.

9.3.3. Responsibility to protect confidential information

312. See the relevant section in the *GCPS*.

9.4. PRIVACY OF PERSONAL INFORMATION

313. See the relevant section in the *GCPS*.

9.4.1. Privacy plan

314. See the relevant section in the *GCPS*.

9.4.2. Information treated as private

315. See the relevant section in the *GCPS*.

9.4.3. Information not deemed private

316. See the relevant section in the *GCPS*.

9.4.4. Responsibility to protect private information

317. See the relevant section in the *GCPS*.

9.4.5. Notice and consent to use private information

318. See the relevant section in the *GCPS*.

9.4.6. Disclosure pursuant to judicial or administrative process

319. See the relevant section in the *GCPS*.

9.4.7. Other information disclosure circumstances

320. See the relevant section in the *GCPS*.

9.5. INTELLECTUAL PROPERTY RIGHTS

321. See the relevant section in the *GCPS*.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA representations and warranties

322. FNMT-RCM's representations and warranties as *Trust Service Provider* to the person associated with the *Certificate*, who acts as *Signatory*, and to the other members of the *Electronic Community*, shall be mainly set out in the document containing the terms of use or the *Certificate* issuance agreement, and, secondarily, in this *Certification Policy and Practice Statement*.

323. FNMT-RCM meets the technical requirements for qualified *Certificate* issuance specified in standard ETSI EN 319 411 and agrees to continue complying with that standard or any replacement standards.

324. The rights and obligations of Administrations, agencies, public entities and FNMT-RCM shall be governed by the relevant agreement or arrangement regulating the provision of the trust

services. These agreements or arrangements may establish the *Issuance Law* governing these *Certificates* with the content and for the purpose referred to in this Statement.

325. See the relevant section in the *GCPS.*

9.6.2. RA representations and warranties

326. In addition to the participants' representations and warranties set out herein and in the *GCPS*, *Registration Offices* and/or the *Registration Operations Officer* have the following obligations:

- To thoroughly check the information as to identity and status as a *member of the Judiciary* of the *Certificate Holder*.
- The *Trust Service Provider*, through the *Registration Operations Officer*, will make sure that the procedures approved by FNMT-RCM to identify Certificate Applicants are fulfilled and will inform *Certificate* users how to use them properly, in accordance with the terms of use, the Certification Policies and Practices and the applicable laws.
- Not to register or process applications by employees serving in an entity other than the entity for which they are acting, or with respect to which the Registration Office has no power or authority to act as such, without prejudice to centralised Registration Offices being created or agreements being entered into between administrations for registrations to be made.
- Not to register or process applications for Certificates issued under these policies and where the Applicant has not been authorised by the *Registration Operations Officer.*
- Not to process Pseudonym Certificates, other than for use in actions implemented by electronic means affecting classified information, public safety and security, national defence or other actions where anonymity is justified by law.
- To request revocation of the *Certificate* forthwith upon learning of any of the trigger events specified in section 4.9.1 of this SPPS.

327. See the relevant section in the *GCPS.*

9.6.3. Subscriber and signatory representations and warranties

328. In addition to the participants' representations and warranties set out in the *GCPS*, *members of the Judiciary*, as the *Certificate Signatory*, have the following obligations:

- Not to use the *Certificate* where any of the information as to office, job, employment or any other information is inaccurate or incorrect or does not reflect or define the relationship with the body, agency or entity where the *member of the Judiciary* is employed, or where security reasons so advise.
- Shall use and store the Certificate in a proper way, according to the purposes and functionalities it was issued for.
- To notify the *Registration Operations Officer* of any of the trigger events specified in section 4.9.1 of this SPPS, in order to start processing revocation of the *Certificate*.

329. The natural person associated with the *Centralised Certificate* acting as *Signatory* shall also comply with the security rules regarding custody and use of the signature password, as confidential, personal and non-transferable information that guarantees access to the *Signatory's Private keys*. That *Signatory* must therefore observe the following precautions in relation to the signature password,:

- To hold it in confidence, and not to disclose it to third parties.
- To memorise it and not to write it down on any physical or electronic document.
- To change it forthwith upon suspecting that a third party may know it.
- To notify FNMT-RCM of any possible loss of control over the Private key, in order for the *Centralised Certificate* and associated Keys to be revoked.
- Not to choose a password that may be easily inferred from the *Signatory's* personal information or a predictable password (date of birth, telephone, consecutive number series, same character repetitions, etc.).
- To observe FNMT-RCM's security policy with respect to password composition, regular password change, etc.
- Digital signatures are only created by a QSCD device.

330. The *Signatory* and *Subscriber* will be responsible for informing FNMT-RCM of any change to the status or information recorded in the *Certificate*, in order for the *Certificate* to be revoked and re-issued.

331. In any case, the *Signatory* shall not use the *Signature Creation Data* or private keys associated with the *Signatory's Certificate* where its validity period has expired or the Provider's *Signature / Seal Creation Data* may be under threat and/or compromised and the *Signatory* has been so advised by the Provider or, as the case may be, is aware, suspects or has learned of any such circumstances. The *Signatory's* breach of this requirement shall make the *Signatory* liable for the consequences of acts, documents or transactions signed in any such circumstances, and for any costs, damages and losses arising for FNMT-RCM or third parties if the *Certificate* is used beyond its validity period.

332. In addition, the *Signatory* shall be liable to the members of the *Electronic Community* and other *User entities* or, as the case may be, third parties for *Certificate* misuse, or for any misrepresentations therein contained, or acts or omissions resulting in damages and losses for FNMT-RCM or third parties.

333. The *Subscriber* shall be liable, in any case, to the FNMT-RCM, user entities, and, where applicable, to third parties, for any falsehoods or errors in the statements made during the certificate application process, as well as for any acts or omissions that cause damage or harm to the FNMT-RCM or third parties.

9.6.4. Relying party representations and warranties

334. See the relevant section in the *GCPS*.

9.6.5. Representations and warranties of other participants

335. No stipulation.

9.7. DISCLAIMER OF WARRANTIES

336. No stipulation.

9.8. LIMITATIONS OF LIABILITY

337. In addition to the liabilities set out in the *GCPS,* the *Trust Service provider*:

- Shall not be liable for the use of the *Certificates* issued under this policy where the *Certificate Subscriber's* representatives or *members of the Judiciary* do things for which they have no authority or acting ultra vires.
- The public body or entity of the Public Administration, *Subscrib*er of the *Certificate,* and/or the *members of the Judiciary* and its relations with the FNMT-RCM shall be conducted at all times through the *Registration Office* and the officer responsible therefor.

338. See the relevant section in the *GCPS*.

9.9. INDEMNITIES

339. See the relevant section in the *GCPS*.

9.9.1. CA indemnity

340. No stipulation.

9.9.2. Subscribers indemnity

341. No stipulation.

9.9.3. Relying parties indemnity

342. No stipulation.

9.10. TERM AND TERMINATION

9.10.1. Term

343. This *Certification Policy and Practice Statement* shall enter into force upon being published.

9.10.2. Termination

344. This *Certification Policy and Practice Statement* shall be repealed when a new version of the document is published. The new version shall fully supersede the previous document. FNMT-RCM agrees to review that Statement on a yearly basis.

9.10.3. Effect of termination and survival

345. For valid *Certificates* issued under a previous *Certification Policy and Practice Statement*, the new version will prevail over the previous version to the extent not in conflict therewith.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

346. See the relevant section in the *GCPS*.

9.12. AMENDMENTS

9.12.1. Procedure for amendment

347. See the relevant section in the *GCPS*.

9.12.2. Notification mechanism and period

348. See the relevant section in the *GCPS*.

9.12.3. Circumstances under which OID must be changed

349. See the relevant section in the *GCPS*.

9.13. DISPUTE RESOLUTION PROVISIONS

350. See the relevant section in the *GCPS*.

9.14. GOVERNING LAW

351. See the relevant section in the *GCPS*.

9.15. COMPLIANCE WITH APPLICABLE LAW

352. FNMT-RCM declares that it complies with the applicable law.

9.16. MISCELLANEOUS PROVISIONS

353. See the relevant section in the *GCPS*.

9.16.1. Entire agreement

354. See the relevant section in the *GCPS*.

9.16.2. Assignment

355. See the relevant section in the *GCPS*.

9.16.3. Severability

356. See the relevant section in the *GCPS*.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

357. See the relevant section in the *GCPS*.

9.16.5. Force Majeure

358. See the relevant section in the *GCPS*.

9.17. OTHER PROVISIONS

359. See the relevant section in the *GCPS*.