Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

PKI FNMT – RCM DISCLOSURE STATEMENT

Electronic signature certificates for the Public Sector

Ref. PDS_EN_SP_v1.3

19/01/2026
FNMT – RCM

Contents

Trust Services Provider contact info 2
Certificate types, validation procedures and usage 2
Obligations of subscribers 3
Certificate status checking obligations for the relying parties 3
Limitation of liability 3
Applicable agreements, CPS, CP 4
Privacy policy 4
Refund policy 5
Applicable law, complaints and dispute resolution 5
CA and repository licenses, trust marks and audit 6

Trust Services Provider contact info

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

C/ Jorge Juan, 106

28009 Madrid

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

Contact: ceres@fnmt.es

FNMT-RCM provides Subscribers, Relying Parties, Application Software Suppliers, and other third parties through the web site https://www.sede.fnmt.gob.es/ with clear instructions for reporting suspected private key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to certificates for website authentication.

Certificate types, validation procedures and usage

The Certification Authority “AC Sector Público” and “AC Sector Público G2” issue the following types of electronic certificates, with their specific scopes of application:

1) Certificate of electronic signature for the personnel in the service of the Public Administration and Justice Administration, which confirms:

    - the identity of the staff in the service of the these Administrations, and
    - the subscriber of the certificate, which is the body, agency or entity of the Public Administration or of the Justice Administration, where such personnel provide their services, or develop their activity.

2) Judicial Career Centralised Certificate 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. It is a Centralised Signature Certificate which can be used for identification and electronic signature within the exercise of Judicial Authority.

These certificates are qualified according to the Regulation (EU) No 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.

These certificates can be validated through the certificate validation service provided by the FNMT - RCM through the OCSP protocol, available at the location specified in the certificate itself.

Limits of use

Use of these certificates is limited to:

- For Judicial Career Centralised Certificates: can be used for authentications and electronic signatures required, exclusively, in the Judicial sphere.

- For Certificates of Electronic Signature: the use is limited to the different powers and functions of the subscribing Public Administrations, acting, as the case may be, through the personnel at their service as signatory, according to their title, employment and authorization conditions.

The FNMT-RCM shall file those important events that are necessary to verify the activity of the Certification Authority for a period of no less than 15 years, according to the current legal regulations.

Obligations of subscribers

At the corresponding Certification Policies and Practices for Public Sector or Certification Policies and Practices for the Judicial Career Certificates are defined the obligations of all the parties that act in relation to the use of these certificates.

Certificate status checking obligations for the relying parties

If a relying party is to reasonably rely upon a certificate it shall:

- Ensure that reliance on certificates issued under Certificate Policy is restricted to appropriate uses (see corresponding CP document).
- Verify the validity by ensuring that the certificate has not expired.
- Ensure that the certificate has not been suspended or revoked by accessing current revocation status information available at the location specified in the certificate to be relied upon.
- Determine that such certificate provides adequate assurances for its intended use.

Limitation of liability

The FNMT-RCM shall only be liable for deficiencies in the procedures that correspond to its activity as a Trust Services Provider, and pursuant to the terms of these Certification Practices and Policies. In no other case will it be liable for the actions or losses incurred by applicants, representatives, represented entities, user entities, or in such case, third parties involved, that are not due to errors that can be attributed to the FNMT-RCM in the aforementioned issuing procedures and/or management of the certificates.

The FNMT-RCM shall not be liable in the case of acts of God, force majeure, terrorist attacks, illegal strikes, as well as in the cases that involve actions that constitute a crime or omission that affect its supplier infrastructure, except in the case of gross negligence by the entity.

The FNMT-RCM shall not be liable to persons whose behavior in the use of the Certificates has been negligent. For these purposes and in any case shall be considered negligence, the failure to observe the provisions set forth in the Certification Practices Statements, and especially in the stipulations in the sections referring to the obligations and liability of the parties.

In any case, and with the condition of penal clause, the quantity that the FNMT-RCM must pay for the concept of damages as ordered by the court to the harmed third parties

or members of the Electronic Community, in the absence of specific regulation in the contracts or agreements, is limited to a maximum of SIX THOUSAND EUROS (6,000€).

In the event of termination of the activity as Certification Services Provider, the FNMT-RCM shall be governed by that stated in the electronic signature regulations. In any case, will inform this event, duly and sufficiently in advance, to the holders of the certificates, as well as the users of the affected services. The FNMT-RCM will transfer, with the express consent of the holders, those certificates which continue in force on the effective date of the cessation of the activity, to another Trust Services Provider which accepts them. If this transfer is not possible, the certificates shall be extinguished.

Applicable agreements, CPS, CP

The documents of Certification Policies and Practices for Public Sector and Certification Policies and Practices for the Judicial Career Certificates, inform about the conditions and characteristics of the certification services and services for the issuing of electronic certificates by the FNMT-RCM as a Trust Services Provider. These documents contains the obligations and procedures which agrees to comply in regards to the issuing of the certificates.

The activities that can be outsourced by FNMT-RCM in order to develop its activity as a Trust Services Provider are carried out according with the FNMT-RCM Certification Policies and Practices and the contracts/agreements signed with entities that perform such activities. In these cases, access to FNMT-RCM information by third parties follow the protocol defined in the Security Policy of this company, in terms of identifying risks, establishing security controls to protect access to information and formalization of the corresponding confidentiality agreements. If applicable, will be signed a contract for the treatment of personal data in compliance with current regulations.

Privacy policy

Basic information on the personal data collected. This information is made in two layers on the basis of European regulation (articles 13 and 14 of REGULATION (EU) 2016/679 - General Regulation of Data Protection) and Organic Law 3/2018, of December 5, of Protection of Personal Data and guarantee of digital rights

RESPONSABLE: FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA, E.P.E., M.P. (FNMT-RCM)

PURPOSE: management of the provision of trusted services and other services of the electronic administration and information society, related and foreseen in the purpose of the Entity and in the current regulations. To manage the provision of the above service in all phases of their development and execution. Quality Management, surveys and opinion polls related to the trust services.

LEGITIMATION: the consent of the interested party. Law 6/2020, of November 11, regulating certain aspects of electronic trust services.

DATA COMMUNICATION: Public Administrations, agencies and related or dependent entities, within the scope of article 81 of Law 66/1997, of December 30, 1997, and all

other cases contemplated in European and national regulations having the force of Law. Data communications will occur when the certificate serial number is included in the list of revoked certificates. In addition, the use of the certificate enables third parties to access data that you have provided us (name, surname and ID). Communications to the State Security Forces and Corps and judicial authority. No international transfers are made outside the EU.

RIGHTS: you can access, rectify, delete the data and exercise the other rights, as reported in **https://www.fnmt.es/politica-privacidad**

SOURCE: unequivocal consent of the interested party. From companies and organizations where services are provided by those affected.

SECURITY MEASURES: Esquema Nacional de Seguridad. Further information on the link below.

DATA CATEGORY: Identifying data: NIF/DNI, Passport (full content), name and surname, address, phone number, age, date of birth, email, position, company name or business name, IP, NICC (Central Consular Identification Number). Electronic certificate data: public authentication key, private key for cloud signature, certificate serial number, certificate request code. Social circumstances data: attributes related to capacity and power of representation. Commercial information data: web address (URL)

You may consult additional and detailed information about this treatment in: **https://www.fnmt.es/politica-privacidad (DATA PROCESSING Nº 13)**

The interested parties authorize the FNMT-RCM to include the certificate serial number in the list of revoked certificates (data communication) so that it may be viewed by any user, whether or not the user has an electronic certificate, in both the public and private areas. We also inform you, and you agree that the use of the certificate for identification purposes or if you perform an electronic signature, entails the possibility that third parties may access the data you have provided to us that are included in the certificate.

Refund policy

It does not apply to these types of certificates.

Applicable law, complaints and dispute resolution

Provision of trusted services of the FNMT - RCM will be governed by the provisions of the Laws of the Kingdom of Spain.

In general, members of the Electronic Community and Users of the trust services of the FNMT-RCM accept that any litigation, discrepancy, question or claim resulting from the execution or interpretation of the Policies and / or Declarations of Service Practices Trust and Electronic Certification or related to them, directly or indirectly, will be resolved in accordance with what is established in the corresponding contracts, general conditions and / or assignments or agreements, in the terms set forth in the Bylaw of the entity, approved by RD 51 /2023, of January 1 (BOE nº 27 of February 1, 2023).

In the event that contracts, general conditions and / or parcels or agreements do not specify conflict resolution systems, all parties submit to the exclusive jurisdiction of the courts of the Spanish State in the city of Madrid.

Likewise, mediation or arbitration procedures may be agreed upon, subject to the approval of the competent bodies of the FNMT-RCM, in accordance with the applicable legislation.

CA and repository licenses, trust marks and audit

The FNMT – RCM has a long history in performing its industrial activities, as well as backing from the State. Since the entry in force of article 81 of the Fiscal, Administrative and Social Order Measures Act 66/1997, of 30th December, and its modifications, the FNMT-RCM has contributed to promoting the extension of the services to which it is authorized and has gained the recognition in the private environment in the sector of electronic certification and the data communications networks, becoming a significant player in the provision of certification services.

FNMT-RCM, as a Trusted Services Provider, holds several accreditations and certifications, such as:

- Issuing qualified certificates according to ETSI EN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates”, ”ETSI EN 319 412-2 “Certificate profile for certificates issued to natural persons”. This audit is performed on an annual basis by an Accredited Conformity Assessment Body.

Certificates issued by “AC Sector Público” and “AC Sector Público G2”, are issued as qualified certificates under the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, concerning electronic identification and trust services for electronic transactions in the internal market. Inclusion in the list of trusted certification service providers (TSL) of Spain can be seen through the link https://sedediatid.mineco.gob.es/Prestadores/.