Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

PKI FNMT – RCM DISCLOSURE STATEMENT

Electronic certificates of identification, seal and signature of the Public Administration

Ref. PDS_EN_AP_v1.1

13/09/2017
FNMT – RCM

Contents

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 Administración Pública" issues three 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) Certificate for Website Authentication to ensure secure communication and linking of the website to the Public Administration, body, public body or entity of public law to whom the certificate is issued.

3) Certificate of Electronic Seal of Public Administration, body, public body or entity of public law, as a system of identification and for automated administrative action and for automated judicial action, which allows to authenticate documents or any digital asset.

The Certificates of electronic signature and Electronic Seal of Public Administration cited above 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 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 Certification Practice Statements 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 CA CPS 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 Statement, 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 specific document of Certification Practices and Policy of Certificates of representatives of legal entities from the "AC Administración Pública", accessible at http://www.ceres.fnmt.es/dpcs/, 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. This document contains the obligations and procedures which agrees to comply in regards to the issuing of the certificates of representatives of legal entities, certificates of representatives of institutions with no legal entity and representative certificates for sole and joint administrators.

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

The FNMT – RCM adopts the technical and organizational security measures in order to guarantee the security of the personal data and avoid its unauthorized alteration, processing or access, in accordance with that set out in Royal Decree 1720/2007, of 21st December, which passes the Regulations which develop Constitutional Act 15/1999. The files shall be publicly owned and their creation, modification or deletion shall be performed under general regulations published in the Official State Gazette. Likewise, FNMT – RCM shall destroy or return all personal data object of processing once the relations ends for whatever reason with the FNMT-RCM, except that data which the legislation states must be kept for at least fifteen (15) years.

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 1.114 / 1999, of June 25 (BOE nº 161 of July 7).

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” and ETSI EN 319 412-3 “Certificate profile for certificates issued to legal persons”. This audit is performed on an annual basis by an Accredited Conformity Assessment Body.

Certificates of Electronic signature for the personnel in the service of the Public Administration and Electronic Seal, 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://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl.