Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

PKI FNMT – RCM DISCLOSURE STATEMENT

"AC Components " Certificates

Ref. PDS_EN_components_v1.0

09/01/2017
FNMT – RCM

Index

Trust Service Provider contact info 2
Certificate type, validation procedures and usage 2
Reliance limits 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 4
Applicable law, complaints and dispute resolution 5
CA and repository licenses, trust marks and audit 5

Trust Service 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

Certificate type, validation procedures and usage

The "AC Components" Certification Authority issues the following types of electronic certificates with their specific scope of use:

- **Standard SSL Certificate**: To secure communications using the SSL / TSL protocol. This type of Certificate guarantees the identity of the domain where a web is located.

- **Wildcard SSL Certificate**: Ensures the security of an unlimited set of subdomains, from the third level, with a single SSL Certificate.

- **Multidomain SSL Certificate (SAN / UCC)**: Ensures the security of a set of independent domains with each other.

- **Qualified Seal certificate**: Certificate of legal person used for the automation of signature processes and authentication between computer components. In addition, the user is allowed to choose the extended use of Certificate keys (client authentication, email protection).

- **Qualified Certificate to be used in the FNMT-RCM Time Stamping Unit**: It is used by FNMT-RCM Time Stamping Authorities to provide the Qualified Time Service Sealing Service of the FNMT-RCM as a Qualified Trust Service Provider. In all matters relating to this service, the Policy and Practice Statement of the Time Stamping Service can be consulted at the following address: http://www.cert.fnmt.es/dpcs/

The qualified electronic certificates are issued 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 and repealing Directive 1999/93/EC.

Reliance limits

If any user part relies on a Component Certificate without carrying out the verification of the status of the Certificate, there will be no coverage of the Particular Certificate

Practice Statement applicable to this type of certificate and there will be no legitimacy whatsoever to claim or take legal action against the FNMT-RCM for damages or disputes arising from the use or reliance on a Certificate of Component.

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

The Particular CPS defines 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 Statements. 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 does not respond in the event of unforeseen circumstances, 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, in particular, those in the sections referring to the obligations and responsibility 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 Trust 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 Particular CPS and Policy from the "AC Components", accessible at http://www.ceres.fnmt.es/dpcs/, informs about the conditions and characteristics of the FNMT-RCM certification services as a Trust Services Provider. This document contains the obligations and procedures which agree to comply in regards to the issuing of the certificates of natural persons.

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

The FNMT - RCM has a refund policy that allows the refund request within the established withdrawal period, accepting that this fact will lead to the automatic revocation of the certificate. The procedure will be published in the electronic headquarters of the FNMT - RCM.

Applicable law, complaints and dispute resolution

Disputes shall be handled in accordance with the FNMT - RCM's complaints process, details of which can be obtained by applying to the Issuing Authority. Contact details are provided in the first section of this document.

All disputes may be resolved through mediation or other form of alternative dispute resolution if both parties so choose; however, nothing in this clause affects either party's rights or its ability to commence legal proceedings.

The provision of FNMT – RCM Certification Services shall be governed by Spanish law and all parties shall submit to the exclusive jurisdiction of the courts of the Spanish State in Madrid's Community.

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 Trust Services Provider, holds several accreditations and certifications, such as:

- For the seal certificates and the certificates used to provide Qualified Time Service Sealing Service of the FNMT-RCM: Issuance and administration of qualified electronic certificates in accordance with ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-2 ETSI EN 319 412-3 "Certificate profile for certificates issued to legal persons".
- The other certificates issued by the CA are in accordance with the European standard ETSI EN 319 411-1 "Policy and Security Requirements for Trust Services Providers issuing certificates- General Requirements"

This audit is conducted with the required frequency and by a Conformity Assessment Body accredited for such purpose.

The certificates issued by "AC Components" are 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.