Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CATALOGUE OF DIGITAL SERVICES

INNOVATION IN CITIZEN SERVICES

Contents

Introduction

The aim of this Digital Services Catalogue is to disseminate the services made available to the public, Public Administrations and private companies by the Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM).

The FNMT-RCM is a Public Business Entity (PBE) and In-House Supplier (IHS) of the General State Administration, in accordance with its Statutes and Law 40/2015, of 1 October, on the Legal Regime of the Public Sectorand of Regions and Local Entities, in accordance with RD - law 11/2020 of 31 March.

The FNMT-RCM, as a Trusted Service Provider via CERES (CERtificación ESpañola), has implemented a series of applications that allow the Administration, citizens and Spanish companies to carry out their administrative procedures online in a totally secure way.

As an extension of these pioneering services, the new digital identity authentication and certification solutions included in this Catalogue make all electronic transactions valid and secure.

The most popular digital services offered by the FNMT-RCM are listed below, although they are by no means the only ones.
The Entity offers the possibility of analysing, designing and deploying digital services tailored to the Administrations and Organisations that request them.

Electronic identification and signature means

01. CERTIFICATES FOR CITIZENS

02. CERTIFICATE FOR LEGAL ENTITY REPRESENTATIVES

03. CERTIFICATE FOR PUBLIC EMPLOYEES

The identification and signature processes can be carried out thanks to electronic certificates and the private keys associated with them. The FNMT-RCM issues recognised digital certificates for different types of end entities: citizens, legal entity representatives and public employees.

Electronic identification and signature means

01.

CERTIFICATES FOR CITIZENS

FNMT User Certification Authority

The digital certificate issued by the FNMT-RCM for Natural Persons is an electronic declaration that links its subscriber with signature verification data and confirms their identity.

This type of certificate, also known as a Citizen's Certificate, is an electronic document that contains, among other information, the subscriber's identity (name, surname and ID number), allowing them to identify themselves securely to third parties online, and to sign electronic documents through the use of an electronic signature.

These are recognised certificates pursuant to Regulation (EU) No 910/2014 of the European Parliament and of the Council

WHO CAN OBTAIN A NATURAL PERSON DIGITAL CERTIFICATE?

Any person of Spanish or foreign nationality, who is of legal age or is a legally emancipated minor and in possession of their Spanish ID or NIE tax identification number, may request and obtain their electronic certificate free of charge in order to sign electronically and/or securely certify their identity telematically.

WHAT IS IT FOR?

Thanks to the digital certificate issued by the FNMT-RCM, you can avoid unnecessary journeys and waiting times. The Natural Person Digital Certificate allows you to carry out procedures securely with different public administrations and private entities online, such as, for example:

- Tax filing and settlement
- Submitting appeals and complaints
- Consulting the municipal register
- Requesting information on employment history
- Enquiries regarding traffic fines
- Enquiries and procedures regarding grant applications
- Enquiries regarding polling station allocation
- Enquiries regarding actions not needing specific technical approval
- Electronic signature for official documents and forms

FOR FURTHER INFORMATION PLEASE VISIT

https://www.sede.fnmt.gob.es/certificados/persona-fisica

Electronic means of identification and signature

02.

CERTIFICATE FOR LEGAL ENTITY REPRESENTATIVES

Certification Representation Authority

The FNMT-RCM issues three types of proxy certificates that are recognised in accordance with 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 domestic market.

These types of certificates are issued to natural persons acting as entity representatives and companies that obtain a certificate for use in their relations with the Public Administrations, Public Entities and Bodies, either linked to or dependent on them.

CERTIFICATES FOR SOLE OR JOINT ADMINISTRATORS

This type of certificate can be obtained by: public limited companies (A) and private limited companies (B) if the company representative is a sole or joint administrator correctly registered with the Commercial Register.

CERTIFICATES FOR LEGAL ENTITIES

This type of certificate may be obtained by persons representing an entity or company that is a legal entity.

CERTIFICATES FOR UNINCORPORATED ENTITIES

This type of certificate can be obtained by persons who represent an entity or company that has the status of an entity without legal personality (residents' associations, associations, etc.).

FOR FURTHER INFORMATION PLEASE VISIT

https://www.sede.fnmt.gob.es/certificados/certificado-de-representante

Electronic identification and signature means

03.

CERTIFICATE FOR PUBLIC EMPLOYEES

Public Sector Certification Authority

These are recognised certificates issued by the FNMT-RCM, pursuant to Regulation (EU) No 910/2014 of the European Parliament and of the Councilas well as in accordance with laws 40/2015 and 18/2011.

These confirm the identity of the Signatory (Public Administration employee) as well as the identity of the Administration, Body or Entity under public law where the Signatory provides their services or carries out their activity.

The FNMT-RCM issues three types of certificates with these characteristics

RECOGNISED CERTIFICATE FOR PUBLIC ADMINISTRATION EMPLOYEES

This certificate links its holder with signature verification data and confirms the holder's identity, the identity of the Entity where they provide their services and, where applicable, personal identification number, position and job title. This certificate can be supported by software or on a cryptographic card.

PUBLIC EMPLOYEE CERTIFICATE WITH PSEUDONYM

A digital certificate issued by the FNMT-RCM to Administration employees, whereby the signatory is identified by means of a pseudonym.

RECOGNISED CERTIFICATES OF CENTRALISED SIGNATURES FOR PUBLIC ADMINISTRATION EMPLOYEES.

"CLOUD CERTIFICATE" (ACCESSIBLE FROM MOBILE DEVICES)

A digital certificate issued by the FNMT-RCM to the Administration's personnel, which is focused on remote or server signatures. The generation of public and private keys is generated and stored in a secure environment belonging to the FNMT-RCM, as are electronic certificates, thus guaranteeing the signatory exclusive control over the use of these keys at all times. Access to this storage is secure thanks to the use of different access keys and passwords.

FOR FURTHER INFORMATION PLEASE VISIT

https://www.sede.fnmt.gob.es/certificados/administracion-publica/obtener-certificado

Website authentication

The FNMT-RCM issues two types of certificates in order to secure websites.

Recognised e-Office certificates for the Public Administration, which validate the identity of the e-Office, guaranteeing the privacy, identity and security of communications between citizens and the e-Office.

SSL certificates are designed to secure communication with a website with the same guarantees of integrity and confidentiality.

01. RECOGNISED E-OFFICE CERTIFICATES

02. SSL/TLS QUALIFIED CERTIFICATES

- 02.1. SSL/TLS STANDARD CERTIFICATE
- 02.2. WILDCARD CERTIFICATE
- 02.3. SAN CERTIFICATE

Website authentication

01.

RECOGNISED E-OFFICE CERTIFICATES

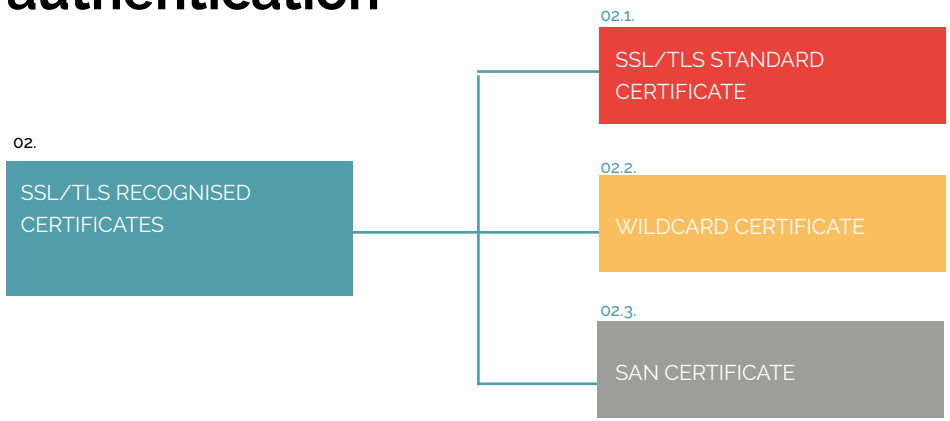
Secure Server Certification Authority

These certificates are issued according to the provisions of Law 40/2015, of 1 October, on the Legal Regime of the Public Sector.

Digital site certificates issued by the FNMT-RCM link signature verification data to the identification data of an e-Office, guaranteeing at all times the identification of the Entity that owns the site.

For these certificates, the subscriber is the Administration, Body or public Entity that owns the electronic address and domain through which the e-office is accessed.

Website authentication



These certificates enable communication with clients using SSL or TLS technology (protocols that provide data encryption and authentication between applications and servers), which are the standards for secure communication on the Web.

The server identifies clients with the name of the domain where their web service is located, as well as guaranteeing the integrity and confidentiality of communications.

The FNMT-RCM issues these certificates through the Secure Servers CA, under two types of characteristics:

EV Certificates
EV (extended validation) certificates confirm the existence of the entity, the legal representation of the entity and the domain ownership. These certificates are currently issued for a period of one year.

OV Certificates
OV (organisation validation) certificates confirm the existence of the entity and the domain ownership.

All types of certificates can be installed on as many machines as required. They are currently issued for a period of one year.

SSL/TLS STANDARD CERTIFICATE 02.1.

This type of certificate guarantees the identity of the domain name where the Web service is located. They can be either EV or OV. In most cases, this is the most suitable.

WILDCARD CERTIFICATE 02.2.

A wildcard certificate secures, with a single certificate, an unlimited set of subdomains associated to a main domain. For example, the wildcard certificate issued to "*.example.co.uk" guarantees the identity of domains such as "shopping.example.co.uk", "sales.example.co.uk" and "registrations.example.co.uk". They may be type OV

SAN CERTIFICATE 02.3.

The SAN type certificate (Subject Alternative Name), also known as a multi-domain certificate, UCC or Unified Communications Certificate, makes it possible to secure up to twelve different domains with a single certificate. They can be either EV or OV.

Automated asset identification and administrative/ judicial action

01.

ELECTRONIC SEAL

Electronic seal certificates link signature verification data with the identification and authentication data of a specific Administration, Body or Entity and its respective organisational units (unit that carries out the automated administrative action).

These certificates are issued through the Public Sector (AC SP CA), in accordance with the provisions of Law 40/2015, of 1 October, on the Legal Regime of the Public Sector.

02.

ENTITY SEAL

Certificate enabling the automation of signature and authentication processes between IT components

These certificates are valid for three years.

Qualified time-stamping service

When carrying out transactions online, time acknowledgement is important, and asking a trusted third party to provide a record of dates and times is essential in order to provide evidence, guarantee the time source used, and ensure the integrity of the data stamped.

Time stamping is a method of proving that a set of data existed before a given point in time and that none of this data has been modified since then.
Qualified time stamping provides added value to the use of digital signatures as the digital signature alone does not provide any information about when the signature was created and, in the case that the signatory did include it, it would have been provided by one of the parties, whereas it is advisable that the time stamp be provided by a trusted third party.
The FNMT-RCM has the necessary technical infrastructure to carry out qualified electronic time-stamping services and has extensive experience in the sector, subject to the provisions of current legislation as a trusted third party.
The time-stamping service offered by the FNMT-RCM is based on the provisions of 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 (eIDAS), as well as on the specifications of the IETF-PKIX RFC-3161 standard.

SECURE TIME SOURCE

To associate the data with a specific moment in time it is necessary to use a Qualified Time Stamp Authority (QTSA) as a trusted third party.
Said moment shall be obtained from a secure time source, which in the case of the FNMT-RCM is that of the Royal Naval Observatory, which provides the basis for the legal time throughout the national territory (R. D. 23 October 1992, no. 1308/1992).
Once the timestamp is received, it is distributed to the Digital Dating Authority, making use of the Network Time Protocol (NTP) with an accuracy of up to several microseconds.
Thanks to the agreement between the FNMT-RCM and the ROA by which the synchronism between the atomic clocks of both Entities is maintained, this service offers technical and legal guarantees.

LEGAL BASIS

The FNMT-RCM developed its time-stamping service in 1998, and since then this service has been operational for public and private entities, providing reliable proof of the time at which a transaction is carried out.
This service demonstrates the capabilities of the FNMT-RCM, which, after developing the service, nominated its collaborators as drafters of the ISO standard on time stamping and, in October 2002, succeeded in having this standard unanimously approved as international standard ISO/IEC 18014.
Since then, the service has undergone technological upgrades to meet new usage and regulatory requirements.
For the scope of Public Administrations, law 9/2017, of 8 November, on Public Sector Contracts, specifies the need for public Entities to disseminate their contracting party profile via the Internet and that the computer system that supports this profile must have a device that allows for reliable accreditation of the time at which the dissemination of the information begins.
To comply with this law and its technical requirements implies that only seals issued by a recognised Certification Service Provider can offer the reliability required by the law.

FOR FURTHER INFORMATION PLEASE VISIT

Digital certificate validation services

One of the uses of digital certificates by third parties is the verification of electronic signatures made by the certificate holder.

However, even if the electronic signature of a given document is verified and is correct, the certificate's validity period may have expired, or the holder may have invalidated that certificate prior to the execution of that signature.

Whenever a signature is verified, the validity of the signatory's certificate must be checked.

Digital Onboarding Remote identity certification

The FNMT-RCM offers its new Onboarding service, allowing users to be certified in order to obtain our recognised certificates, while maintaining the guarantees of appearing in person at an accreditation office.

The FNMT-RCM offers this platform in the cloud, allowing us to provide this service to those organisations that need to use digital Onboarding for any of their procedures.

The platform offers additional functions. It presents all biometric services to make use of them in other developments for identity verification, user authentication, document authenticity verification, etc.

The system features anti-fraud controls to prevent a user being certified with more than one identity, thus providing the platform with a high level of security that can be transferred to the applications of the organisations that integrate this system into their user identification platforms.

Finally, the versatility of the Onboarding platform makes it possible to offer additional services such as video calls in which the interlocutor is reliably identified, thus making it possible to replace the need for a face-to-face appointment.

The platform complies with all security requirements demanded by the National Cryptographic Centre, pursuant to the specifications set out in Law 6/2020, of 11 November, regulating certain aspects of electronic trust services, developed in part via Ministerial Order ETD/465/2021, of 6 May, regulating remote video identification methods for issuing qualified electronic certificates.

Electronic identification credentials and attributes

Issuance of digital identification credentials, as an evolution of the current electronic certificates.

Issuance of electronic credentials, after identification with an ID, to access the electronic administration.

Blockchain Laboratory

FNMT-RCM infrastructure made available to Public Administrations for multiple uses: proof of concept, for development and/or pre-production environments, to create, host and manage their Blockchain production platform, etc.

Exploiting knowledge about the European network (EBSI) and use cases.

Promotion of government projects on Blockchain technology, rationalisation of public sector resources and alignment with European requirements and standards (guarantee of interoperability).

Digital evidence safekeeping system.

We securely store all the data that clients wish to keep as evidence of any business process, applying the applicable conservation rules.

FNMT Cloud in the service of Public Administrations

Advanced FNMT-RCM infrastructure for hosting Public Sector services.

Rationalisation of the administration's DPC (data processing centre) resources.

Technical solution, located on Spanish territory and geographically distributed, where the ownership of the infrastructure, management, storage technology, computing capacity and the interests it protects are public.

Safekeeping evidence, documents and files

Application of FNMT-RCM digitisation and safekeeping solutions to the services required by the Public Sector, such as:

- Single electronic file (finalised files) and transformation of paper files into digital format.
- Electronic documents, files or information structures associated with a business process.
- Management of records stored under specific business rules (encryption, sealing, secure deletion, etc.)

In addition, we offer SaaS solutions involving the management of electronic signatures**(signature holders)** or the management of the archive**(electronic files in the archiving phase)**.

ADVANTAGES OF FNMT-RCM CERTIFIED DIGITISATION

Service level: Reliability, quality and security.

Public ownership: The Administration's own supplier.

Experience. Experience in transport, management, handling, destruction and safekeeping chain traceability.

Infrastructure and assets. Facilities, processes and qualified staff to provide services with logical and physical security.

Know-how. Experience acquired in the digitisation and OCR of over 7 million documents.

Standardisation: Present on Committees and in Working Groups that regulate e-Administration: access to information and active participation.

Scope: 4 service areas available: Digitisation, Metadata, Verification and Administration.

System for traceability and authenticity of the logistics chain origins

This allows the establishment of traceability systems that provide reliability and make it easier for the end consumer to check the security measures and the authenticity of product origins by simply scanning a QR code from a mobile device.

Application of emerging technologies, such as Blockchain, in the agri-food and fisheries supply chain.

Other services

The FNMT-RCM has carried out many pilot projects in all kinds of digital projects.

Tell us your idea and what you need, then let us help you bring your project to life.

servicios.digitales@fnmt.es

OTHER SERVICES AVAILABLE

Product traceability: Establishment of markers to trace the movements of any product, as well as authentication of its origin. Our experience with the traceability system developed in tobacco products with over 2.5 billion identifiers per year is our best guarantee.

IoT projects: IoT has the potential to transform almost every aspect of the way we live, work and interact, both locally and globally. FNMT-RCM experts can help you carry out your IoT project.

Electronic invoicing: With more than 3,850,000 invoices issued, we have offered this service since 2016.

Mobile Apps. We have developed numerous apps for most public Entities (state, regional and local) with identification via e-ID

Consultancy: Consultancy in product traceability projects by means of unique electronic identifiers, in identification projects and in all projects in which security is essential.

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA

Calle Jorge Juan nº 106,
Madrid 28009
+34 91 566 666.
servicios.digitales@fnmt.es
www.fnmt.es