TERMS AND CONDITIONS FOR REMOTE VIDEO IDENTIFICATION FOR THE ISSUANCE OF QUALIFIED ELECTRONIC SIGNATURE CERTIFICATES BY THE ROYAL MINT OF SPAIN (FNMT-RCM).

The *Applicant* and future *Signatory* states that he/she accepts performance of the process of remote video verification and identification for the issue of qualified certificates by the Royal Mint of Spain (Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)) and will use the *Remote Video Identification Service* in accordance with the attached conditions, the Specific Policy and Certification Practices for the Certificates applied for and the General Statement of Certification Practices of the FNMT-RCM and, in accordance with "Order ETD/465/2021, of 6 May, which regulates the methods of remote video identification for the issuance of qualified electronic certificates" and related rules, also accepting the FNMT-RCM's policy on privacy and data protection information, consenting to the full recording of his/her face and voice and the obtaining of other forms of proof during the registration process, and also the processing and keeping of special categories of personal data (biometric data) and the non-application of the right of withdrawal once the service has been fully executed, in accordance with the provisions of Royal Legislative Decree 1/2007, of November 16, 2007, which approves the revised text of the General Law for the Defense of Consumers and Users and other complementary laws.

The *Applicant's* acceptance of these terms and conditions applies to the whole content thereof, and he/she may not restrict their application and states responsibly that his/her ability to enter into a contract with this Organisation is not limited in any way.

Conditions of Use

These terms and conditions are drawn up in order to provide clear and comprehensible information to the *Applicants*, *Signatories* and users about the remote video identification process, the applicable security recommendations and the information on privacy, as set out in the applicable rules. By accepting these terms and conditions, the *Applicant* gives explicit consent for the full video recording and for the processing and keeping of special categories of personal data. When you press the Accept option, to carry out the process of remote video identification to obtain a qualified electronic signature certificate, you are also accepting the privacy policy, the policy on data protection information and these conditions of use. If you do not accept these conditions, you will not be able to gain access to the video identification service.

The FNMT-RCM, as a Trust Service Provider, informs you that there are other alternatives for identification that do not require the processing and keeping of your image and your biometric data, either by physically attending a Registry Office, with personnel qualified for the procedure, with which the FNMT-RCM has signed an agreement or which is covered by an administrative ruling or decision; or by using an electronic signature Certificate that confirms the applicant's identity.

Access to the Service

1) The method of remote video identification that will be performed is unassisted (asynchronous), with no online interaction between an operator and the *Applicant* and subsequent review by an operator appointed by the FNMT-RCM. To initiate the FNMT-RCM video identification verification process, the user must first have applied for the Certificate and obtained the corresponding application code. The user must also accept in advance the privacy policy, data protection policy and these conditions of use, in addition to the website cookies policy.

2) Once the video identification option is selected, the system will guide you through different steps and actions that the *Applicant* must carry out to obtain the proofs establishing the accreditation of identity with an appropriate level of security, according to the approved standards. The verification of identity will be based on facial recognition using biometric procedures, a voice recording and proof of life via video and the presentation of a valid identity document.

Click on this link to consult the instructions for carrying out the full video identification process.

3) Once the process of obtaining proofs is completed, the FNMT-RCM, either directly or through qualified agents contracted by it, will review the recorded identification process and will check the proofs generated by the system to accept or reject their validity. The authenticity, validity and physical and logical integrity of the identification document used will be verified, ensuring that the holder of the document is the same person as the *Applicant*. Measures will be taken to reduce to a minimum the risk that the identity of the applicant does not coincide with the claimed identity, considering the risk of lost, stolen, suspended, revoked or expired documents.

The identification process will be interrupted or will not be deemed valid when any of the following circumstances occurs:

a) There are indications of falsification, manipulation or invalidity of the identification document.

b) There are indications that the document holder and the applicant are not the same person.

c) The quality of the image or the sound prevent or make it difficult to verify the authenticity and the integrity of the identification document and to verify that the holder of the document and the applicant are the same person.

d) The conditions, security or the quality of the communication make it impossible or difficult to complete the process with the appropriate reliability.

e) There are indications of the use of pre-recorded files.

f) There are indications that more than one device has been used to transmit the video.

g) There are indications that the video has not been transmitted in real time or that the process has not been carried out as a single act.

h) There are indications that the applicant is being coerced or intimidated.

i) Any other circumstance in which there is a reasonable doubt about the security of the process being carried out.

If the FNMT-RCM, through the technical systems implemented, interrupts the identification process or deems it not to be valid, the reason will be given and there will be a verifiably documented record of this in the system.

The registry agent that reviews the proofs obtained in the registration process will base their decision to approve or deny the application for issue of a certificate on the review of all the proofs collected in the identification process, including, at least, the video, the checking of random characters sent to the applicant, the existence of security elements in the identity document extracted from it during the identification process and the biometric comparison carried out.

Appropriate measures will be taken to detect a possible manipulation of the video image, of the identity document or the applicant's document, guaranteeing their proof of life. These will include, at least, the following:

a) Procedural measures that make said manipulation evident with the entering of a unique, random and unpredictable single-use code generated for the purpose and sent to the applicant. The code will consist of a minimum of six characters or system with equivalent entropy. The service provider will check that the mobile device to which the code is sent is in the user's possession during the identification process.

b) In the case of unassisted remote video identification, the system will require the applicant to actively carry out physical interactions and actions, which will include both common and random and differentiated actions.

4) The FNMT-RCM, as Trust Service Provider, informs you that the recording and obtaining of proofs is performed under the following conditions:

a) The video will be recorded in full and without interruptions.

b) There will be a verifiably documented record of the date and time of the recording using a qualified time stamp.

c) A copy of the recording of the video will be kept for a minimum of fifteen years from the moment the validity of the certificate obtained by this method expires.

d) Photos or screenshots of the applicant and the identity document used, in which both the person and the front and back of the identity document are clearly recognisable, will be kept for a minimum of fifteen years.

e) The automatic result of the verification carried out by the application, and the assessment and observations made by the agent together with their decision to approve or reject the identification, will be kept for a minimum of fifteen years.

f) All the proofs from the incomplete identification processes that have not been completed because of suspected attempted fraud will be kept for a period of 5 years from the performance of the identification process, specifying the reason why they were not completed.

g) The integrity, authenticity and confidentiality of the recording, and of the other proofs obtained during the remote identification process, will be guaranteed through the use of qualified trust services. To keep the data, they will be blocked as provided for in article 32 of Organic Law 3/2018, of 5 December, on Personal Data Protection and guarantee of digital rights.

h) The recording and the images obtained during the identification process will meet the conditions of sufficient quality and clarity to guarantee their use in subsequent investigations and analyses.

i) The images obtained during the identification process can be used to introduce technical improvements in the video identification tool and establish references on which to make measurements.

5) During the registration process, when the applicant presents their National Identity Document (DNI), the applicant's identity data are checked using the document number, through the intermediation platform of the Data Verification and Consultation Service of the Secretary of State for Digitalisation and Artificial Intelligence. In the case of technical problems associated with the verification platform that are beyond the service provider's control, at least three query attempts will be made, and the responses received will be kept.

The accreditation will be carried out respecting the valid regulations on personal data protection at all times, and the privacy and data protection policy must be accepted prior to processing. The personal data collected during the verification of identity will be stored by the FNMT-RCM for the time periods established by the specifically applicable regulations.

Applicant Obligations

The natural person video identification *Applicant* must:

- Provide true, accurate and complete information to perform the registration.
- Provide valid, exclusive identity documents.
- Be familiar with and comply with these conditions of use, the Specific Policy and Certification Practices for the Certificates applied for and the General Statement of Certification Practices of the FNMT-RCM.
- Hold the FNMT-RCM harmless from any complaint or claim related to the fraudulent use of identity documents or the provision of false, distorted or incomplete data in the remote video identification process. Any attempted or suspected identity theft or fraudulent action on the part of the *Applicant* in the video identification process will be communicated to the competent Law Enforcement Bodies and/or the Public Prosecutor.

Obligations on verification of the status of third-party certificates

The members of the Electronic Community, the user organisations and third parties that trust in the *Certificates*, issued by means of certified video identification, and in the electronic signatures generated with them, must be familiar with the Specific Policy and Practices for Certification of Certificates – which are documents approved and published on the FNMT-RCM website, accessible using the Certificate itself – and comply with the following obligations, exonerating the Trust Service Provider (FNMT-RCM) from any liability should any of them not be met:

- Verify, prior to trusting in the *Certificates*, the advanced electronic signature or the electronic stamp of the Trust Service Provider that issued the *Certificate*.
- Verify that the *Certificate* is still valid.
- Verify the status of the *Certificates* in the certification chain, by consulting the FNMT-RCM's "Information and consultation service on the validity status of the certificates" included in the *Certificate* itself or in the System.
- Check the restrictions on use applicable to the *Certificate* being verified.
- Inform the FNMT-RCM, or any Registry Office, of any anomaly or information relating to the *Certificate* that may be considered a reason for revocation thereof, and provide all the available elements of proof.

Limitations of liability

The FNMT-RCM is only liable for the correct issuance and management of the Certificates, based on the video identification of the *Applicant* and future *Signatory*, and for incorporating these data into a *Certificate*. This personal identification is carried out through a process of video identification (*On Boarding*), using remote identification systems and the subsequent verification thereof. For the guarantees, obligations and responsibilities to apply, the event must have occurred within the scope of the Electronic Community (agents involved in the activities leading to the issuance and use of the certificates).

The FNMT-RCM shall only be liable for shortcomings in the procedures inherent in its activity as Trust Service Provider, and in accordance with the Specific Policy and Practices for Certification of Certificates or with the Law. Under no other circumstances shall it be liable for any actions or losses incurred by the holders, *Signatories*, user Organisations, registry offices or third parties involved, which are not due to errors that may be attributed to the FNMT-RCM in the procedures for issuance and/or management of the Certificates.

FNMT-RCM shall not be liable in cases of force majeure, unforeseeable circumstances, terrorist attacks or wildcat strikes, or in those cases concerning actions constituting an offence or breach affecting its service provider infrastructures, unless the organisation is found to have committed gross negligence. In any event, in the corresponding contracts and/or agreements, the FNMT-RCM may implement liability limitation clauses. In any event, the amount that the FNMT-RCM may be required by the courts to pay in damages to harmed third parties, and/or members of the associated electronic Community in operations affecting the issuance and use of the Certificate, when there is no specific regulation in the contracts or agreements, is limited to a maximum of SIX THOUSAND EUROS (€6,000).

The FNMT-RCM shall not be liable with regard to *Applicants* that fail to comply with these conditions and with persons whose behaviour when using the Certificates has been careless or negligent; in this regard, and in any event, negligence must be considered to be a failure to observe the terms of the Specific Policy and Practices for Certification of Certificates and, in particular, the provisions in the sections referring to the parties' obligations and responsibilities.

The FNMT-RCM shall not be liable for any software that it has not provided directly. This notwithstanding, the FNMT-RCM shall implement appropriate protection measures to protect its systems and applications against Malware and other systems that are harmful to or attack its infrastructures, and shall keep them up to date in order to cooperate with users in preventing the damage that may be caused by this type of software.

The FNMT-RCM cannot guarantee the video identification systems, even if they are certified, or the cryptographic algorithms, and shall not be liable for any harm caused by successful external attacks on the system and/or cryptographic algorithms used, if it exercised due diligence in accordance with the current state of the art, regulations and certification and proceeded in accordance with the terms of the Specific Policy and Practices for Certification of Certificates and with the Law.

Return Policy

The return policy adopted by the FNMT-RCM for the commercialization of the remote video verification and identification process for the issuance of qualified certificates establishes that, due to the nature of the video-identification service for the issuance of qualified certificates, once the accreditation of identity is approved by our qualified agents, the service will have been fully executed, and the right of withdrawal is not applicable to the Applicant, in accordance with the provisions of article 103. a) of the Royal Legislative Decree 1/2007, of November 16, which approves the revised text of the General Law for the Defense of Consumers and Users and other complementary laws.

Applicable law, complaints and dispute resolution

The provision of trust services by the FNMT-RCM will be governed by the Laws of the Kingdom of Spain. In general, members of the Electronic Community and Users of FNMT-RCM trust services accept that any litigation, discrepancy, issue or claim resulting from the implementation or interpretation of the Policies and/or Statements of Trust Service and Electronic Certification Practices or related thereto, directly or indirectly, will be resolved in accordance with the provisions of the relevant contracts, general conditions and/or commissions or agreements, in the terms of the entity's By-laws, approved by RD 51/2023 of 31 January (Official State Gazette No. 27 of February 1).

In the event that contracts, general conditions and/or commissions or agreements do not specify any conflict resolution arrangement, all the parties submit to the exclusive jurisdiction of the courts of the Spanish State in the city of Madrid. In addition, mediation or arbitration procedures may be agreed, subject to the approval of the competent bodies of the FNMT-RCM, in accordance with applicable legislation.

Licences and repository, trusted trademarks and auditing

The FNMT-RCM has a lengthy track record in the performance of its industrial activities, as well as the backing of the Central Government as a Public Business Entity attached to the Ministry of Finance and Civil Service. Since the entry into force of Article 81 of Law 66/1997 (30 December) on tax, administrative and social measures and amendments thereto, it has contributed to encouraging the extension of the services for which it is authorised and has obtained the recognition of private business in the electronic certification and open electronic networks sector, achieving a significant position in the provision of trust services.

The procedures and methods of remote video identification for the issuance of qualified electronic certificates by the FNMT-RCM, as Trust Service Provider, have been certified in the framework of 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 in the framework of Law 6/2020 and Order ETD/465/2021 which regulates the methods of electronic video identification for the issuance of qualified electronic certificates.

The FNMT-RCM's authorisation to use video identification for the issue of qualified certificates can be verified using https://sedeaplicaciones.minetur.gob.es/Prestadores/Inicio.aspx

DATA PROTECTION.

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: Procedures for identification and verification of identity using online (remote) procedures to obtain products or the provision of services that require it.

LEGITIMATION: Necessary processing for the execution of a contract in which the data subject is a party. Consent given by the data subject. Art. 6.1(a) and Art. 9.2(a) of the GDPR (for the processing of biometric data). Compliance with a legal obligation applicable to the data controller. Art. 6.1(c) of the GDPR: Law 6/2020, of November 11, regulating certain aspects of trust electronic services. Order ETD/465/2021, of May 6, regulating remote video identification methods for the issuance of qualified electronic certificates.

DATA COMMUNICATION: Public administrations, bodies and associated or dependent organisations, within the scope of article 81 of Law 66/1997, of 30 December and the remaining cases covered by European and domestic regulations with the force of Law. Communications to the State Law Enforcement Bodies and judicial bodies. No international transfers outside the EU are made.

SOURCE: You can access, rectify, delete the data and exercise the other rights, as reported in https://www.fnmt.es/en/politica-privacidad (MAIN PAGE)

RESPONSABLE: Unequivocal consent of the interested party.

SECURITY MEASURES: Esquema Nacional de Seguridad. More information in the lower link

DATA CATEGORY: DNI or Passport (full content), name and surname, address, phone number, age, email, photograph, and video of the data subjects (proof of life). Personal characteristics data: public authentication key, private key for cloud signature, biometric data (facial recognition, voice).

You may consult additional and detailed information about this treatment in: https://www.fnmt.es/politica-privacidad (DATA PROCESSING Nº21st)

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.