CONFIRMATION OF CERTIFICATE APPLICATION DATA

CONFIRMATION OF CERTIFICATE APPLICATION DATA

Type of Certificate:

DNI/NIE: **Document Type:**

Name:

First Surname:

Second Surname:

Email:

Position/Others:

Type of Representation - Documentary Reference:

Pseudonym:

Department/Administrative Unit:

NIF of the Organization:

Organization Name:

Certificate/System Designation:

Organization Email:

By signing this document, you acknowledge that:

You have been informed of the circumstances relating to the processing of your personal data for the proper provision of the contracted certificate issuance service and the commercial relationship, in accordance with the Privacy Policy available at the following website: DIGITEL T.S.MK - Privacy Policies.

You have been informed of the content of the certificate and of the possibility of accessing the certificate's PKI Disclosure Statement (PDS) at the following electronic address: https://pki.digitelts.es/

You have been informed of the conditions governing the exercise of your right of withdrawal from the service, as well as the mandatory conditions for the use of the certificate, through contractual terms that you understand and accept, and which are included below as an inseparable part of this document.

TERMS AND CONDITIONS

Qualified Certificate Issuance Service

Prepared by:	Security Department
Reviewed by:	CRS
Approved by:	CRS **Date**: 23/07/2026
Code:	DIGITEL TS_T&C_Servicio_QCERT-EN
Version:	1.0
Date:	21/05/2026
Classification	Public
Status	Approved

Edit Control

Date	Version	Description	Author
21/05/2026	1.0	First version of the document applicable to all types of qualified certificates issued by DIGITEL TS	DIGITEL TS

CONTENTS

1. DEFINITIONS APPLICABLE TO THE CONTRACT

CONTRACT: all contractual documentation, these General Terms and Conditions, the Statement of Practices and Certification Policies of DIGITEL TS's Electronic Certificate Issuance Services and other documents that govern the relations between the Parties.

CERTIFICATION PRACTICES STATEMENT AND CERTIFICATE POLICIES (hereinafter, DPPC): set of practices and policies adopted by the DIGITEL TS Certification Authority for the issuance of electronic certificates where detailed information is found on its security system, support, administration and issuance of the Certificates, and on the relationship of trust between the Parties. It is published on the website of DIGITEL ON TRUSTED SERVICES S.L.U. https://pki.digitelts.es/

SPECIFIC POLICIES APPLICABLE TO CERTIFICATES: the Specific Certification Policies (CP) applicable to electronic certificates issued by DIGITEL TS, included in the Statement of Certification Practices and Policies (DPPC) that can be consulted on the website: https://pki.digitelts.es/. Specific Certification Policies (CPs) are incorporated into these Terms and Conditions by reference. In the event of any discrepancy, the meaning of the terms contained in these terms and conditions shall prevail over what is set out in the DPPC. The Certification Policy Identifiers (OIDs) applicable to each type of certificate are included in the certificate itself and are detailed in the DIGITEL TS DPPC, in accordance with the policies defined in ETSI EN 319 411-2 clause 5.3: QCP-n, QCP-l, QCP-n-qscd, QCP-l-qscd for qualified electronic signature and seal certificates.

PKI DISCLOSURE STATEMENT (PDS) FOR QUALIFIED CERTIFICATES: summary and presentation of the main points of the Statement of Certification Practices and Policies for all types of qualified Certificates in a more readable and understandable format for the benefit of subscribers and parties relying on the DIGITEL TS Certification Authority, in accordance with the requirements of Annex A of ETSI EN 319 411-1. It is published on the website of DIGITEL ON TRUSTED SERVICES, S.L.U. https://pki.digitelts.es/

DIGITEL ON TRUSTED SERVICES, S.L.U. (hereinafter DIGITEL TS): Qualified Trust Service Provider (QTSP), of Spanish nationality with registered office at Enrique Cubero 9, Edificio Madison Arena - 47014 Valladolid (Spain), with NIF B47447560, telephone +34 91 015 05 10 and contact email info@digitelts.com, which is subject to the statutory supervision of the Ministry for Digital Transformation and Civil Service. DIGITEL TS provides qualified trust services in accordance with Regulation (EU) 910/2014 of 23 July 2014, as amended by Regulation (EU) 2024/1183 of 11 April 2024, with regard to the establishment of the European Digital Identity Framework (hereinafter, eIDAS Regulation), and the ETSI EN 319 401 standards; ETSI EN 319 411-1; ETSI EN 319 411-2; ETSI TS 119 431-1 V1.3.1, in accordance with its Conformity Assessment Reports prepared by an accredited Conformity Assessment Body which can be found on its website: https://digitelts.es/certificados/ . In the provision of the requested service, DIGITEL TS acts as a Certification Authority (hereinafter the "CA") relating a certain public key to a natural person or a specific legal entity through the issuance of a digital certificate.

REGISTRATION AUTHORITY (hereinafter, the RA): entity in charge, among other functions, of verifying the identity of the APPLICANT for the certificate and, where applicable, of the other

circumstances associated with the certificate, as regulated in Section 1.3.2 of the DPPC of DIGITEL TS. All or part of the functions of AR may be assumed either directly by DIGITEL TS, or by a Delegated RA. The functions of registering subscribers are carried out by delegation and in accordance with the instructions of the Qualified Trust Services Provider DIGITEL TS, under the terms of Article 24 paragraphs 1 and 1 *bis* of Regulation (EU) 910/2014, and Article 7 of Law 6/2020, of 11 November, regulating certain aspects of electronic trust services, and under the full responsibility of the Qualified Trust Service Provider vis-à-vis third parties.

The SUBSCRIBER: natural person or organization that formalizes a contractual relationship with DIGITEL TS for the provision of certificate issuance services. Depending on the type of certificate, the subscriber may match the certificate holder. In corporate certificates, the subscriber may be an organisation with or without legal personality in which certificates are issued to natural persons linked to them.

THE APPLICANT: natural person who requests the issuance of a certificate for himself (with or without a relationship of representation or corporate link to an ENTITY) in which case he will assume the status of HOLDER/SIGNATORY (electronic signature certificates), or for an ENTITY in which case it is the latter who will assume the condition of HOLDER/SUBSCRIBER (electronic seal certificates). In all cases, the APPLICANT acts as the person responsible for the certificate.

THE ENTITY: the organization, with or without legal personality, linked to the HOLDER/SIGNATORY of a certificate through a representation relationship or corporate affiliation, or the HOLDER/SUBSCRIBER of the certificate in the case of electronic seal certificates issued to organizations with legal personality.

QUALIFIED CERTIFICATE or CERTIFICATE: a qualified certificate for electronic signature, electronic seal, or website authentication (depending on the contracted service) issued by a Qualified Trust Service Provider in accordance with the requirements of Regulation (EU) No 910/2014 of 23 July 2014 ("eIDAS Regulation").

QUALIFIED CERTIFICATE FOR ELECTRONIC SIGNATURE: a certificate certificate for electronic signature issued by a Qualified Trust Service Provider that complies with the requirements set out in Annex I of the eIDAS Regulation, providing the highest legal guarantees regarding the identification of the signatory and its unique link to the electronic signature, as well as the integrity and non-repudiation of the data associated with the electronic signature.

QUALIFIED ELECTRONIC SEAL CERTIFICATE: a certificate certificate for electronic seal issued by a Qualified Trust Service Provider that complies with the requirements set out in Annex III of the eIDAS Regulation, providing the highest legal guarantees regarding data integrity and the correctness of the origin of the data to which the electronic seal is linked.

RELYING PARTIES: natural persons or organizations that voluntarily rely on the certificate issued by the Certification Authority (CA) and, therefore, on the trust service supported by it.

QUALIFIED SIGNATURE OR SEAL CREATION DEVICE (QSCD): a qualified electronic signature or electronic seal creation device that complies with the requirements set out in Annex II of the eIDAS Regulation and is certified by a certification body designated in accordance with Article 30 of the eIDAS Regulation.

REMOTE SIGNATURE OR REMOTE SEAL: a qualified electronic signature or qualified electronic seal created using a qualified electronic signature or seal creation device remotely managed by

a Qualified Trust Service Provider on behalf of the signatory or seal creator, in accordance with Articles 29a and 39a of the eIDAS Regulation.

SIGNATURE ACTIVATION DATA (SAD): data required to activate the creation of an electronic signature or electronic seal within the qualified remote signature or seal creation device, which remains under the sole control of the signatory or under the control of the seal creator.

SERVER SIGNING APPLICATION SERVICE (SSAS): a trust service consisting of a server signing application and a QSCD/SCDev used to create a digital signature value on behalf of the signatory, in accordance with ETSI TS 119 431-1.

2. TYPES OF CERTIFICATES UNDER THESE GENERAL TERMS AND CONDITIONS

QUALIFIED CERTIFICATE FOR CITIZEN: identifies the HOLDER/SIGNATORY solely for acting in their own name. This type of certificate is issued either through a centralized Qualified Signature Creation Device (QSCD), generating a qualified signature, or without a QSCD, generating an advanced signature.

QUALIFIED CERTIFICATE FOR NATURAL PERSON ASSOCIATED WITH AN ENTITY: establishes the association relationship (employment, commercial, professional membership, etc.) between the HOLDER/SIGNATORY and the ENTITY, but not a legal or voluntary representation relationship. This type of certificate is issued either through a centralized Qualified Signature Creation Device (QSCD), generating a qualified signature, or without a QSCD, generating an advanced signature.

QUALIFIED CERTIFICATE FOR REPRESENTATIVES OF ENTITIES WITH OR WITHOUT LEGAL PERSONALITY: these certificates are representative certificates for persons acting as sole administrator, joint administrator, holder of full powers, or at least general specific powers to act before Spanish Public Administrations on behalf of the ENTITY. These certificates guarantee the identity of the SUBSCRIBER and the HOLDER/SIGNATORY and indicate a legal representation or general power-of-attorney relationship between the HOLDER/SIGNATORY and the ENTITY. This certificate includes a field specifying the document, public where legally required, that reliably proves the powers of the HOLDER/SIGNATORY to act on behalf of the ENTITY represented and, where registration is mandatory, the corresponding registry details.

This type of certificate is issued either through a centralized Qualified Signature Creation Device (QSCD), generating a qualified signature, or without a QSCD, generating an advanced signature.

QUALIFIED CERTIFICATE FOR ELECTRONIC SEAL FOR LEGAL PERSONS: these certificates guarantee the identity of the HOLDER/SUBSCRIBER and benefit from the presumption of data integrity and correctness of the origin of the data to which the qualified electronic seal is linked. This type of certificate is issued either through a centralized Qualified Signature Creation Device (QSCD), generating a qualified seal, or without a QSCD, generating an advanced seal.

QUALIFIED CERTIFICATE FOR PUBLIC EMPLOYEE: establishes the association relationship between the public employee HOLDER/SIGNATORY and the ENTITY (Public Administration), but not a legal or voluntary representation relationship. This type of certificate is issued either through a centralized Qualified Signature Creation Device (QSCD), generating a qualified signature, or without a QSCD, generating an advanced signature.

QUALIFIED CERTIFICATE FOR PUBLIC EMPLOYEE WITH PSEUDONYM: establishes the association relationship between the public employee HOLDER/SIGNATORY and the ENTITY (Public Administration), but not a legal or voluntary representation relationship. This type of certificate does not display any personal information, only a pseudonym and the relationship as a public employee with the ENTITY (Public Administration). It is issued either through a centralized Qualified Signature Creation Device (QSCD), generating a qualified signature, or without a QSCD, generating an advanced signature.

QUALIFIED CERTIFICATE FOR ELECTRONIC SEAL FOR PUBLIC ADMINISTRATIONS: these certificates guarantee the identity of the HOLDER/SUBSCRIBER (Public Administration) and benefit from the presumption of data integrity and correctness of the origin of the data to which the qualified electronic seal is linked. This type of certificate is issued either through a centralized Qualified Signature Creation Device (QSCD), generating a qualified seal, or without a QSCD, generating an advanced seal.

SECTION I
TERMS AND CONDITIONS APPLICABLE TO
ALL TYPES OF CERTIFICATES

3. PURPOSE

The issuance by the CA in favour of the APPLICANT of a Certificate of the type set out in the application form and the conditions of use by the APPLICANT of the certificate issuance service, in accordance with the terms set out in this contract, the Specific Policies, the Statement of Practices of Digitel TS, the eIDAS Regulation and local laws.

4. LEGAL FRAMEWORK FOR THE PROVISION OF THE SERVICE

The APPLICANT declares to be aware of the Certification Policies and Practices Statement (DPPC) and the PKI Disclosure Statement (PDS) for Qualified Certificates available on the DIGITEL TS website (https://pki.digitelts.es/). The terms and conditions of this document, together with the DPPC and the PDS, constitute the legal framework that will regulate the relationship between the parties, internally and vis-à-vis third parties, without prejudice to the provisions of current legislation.

5. DURATION OF THE CONTRACT

This contract will enter into force and will end up coinciding with the issue and expiry dates indicated in the Certificate, without prejudice to the causes for revocation provided for in the PDS and the DPPC, and may be renewed in accordance with the terms established in the DPPC.

The validity period of the certificate shall be determined in accordance with the applicable certification policies and shall be expressly stated on the certificate. The maximum duration of validity of the qualified certificates will be that established in the DPPC of DIGITEL TS.

6. CONSIDERATION

The price of the Certificate, which will include the consideration for the services of DIGITEL TS associated with it, is defined in the offer signed by the APPLICANT when requesting the Certificate and in the corresponding invoice.

This price must be paid by the APPLICANT or the ENTITY, to the CA or AR, prior to the delivery of the Certificate, unless otherwise agreed in the signed offer.

7. ACCEPTANCE OF THE CERTIFICATE

The APPLICANT expressly accepts the Certificate, confirming and assuming the accuracy of its content, with the consequent obligations arising from this towards the RA, the CA or any third party that in good faith relies on the content of the Certificate, by virtue of the DPC and/or current legislation. In the event that there is any difference between the data provided to the CA and the content of the Certificate, or the defect is detected, this must be immediately communicated to the CA or the RA by the APPLICANT or by the ENTITY, so that it can proceed to revoke it.

In the event that a HOLDER/SIGNATORY to whom a certificate has been issued ceases to be related to the SUBSCRIBER, said SUBSCRIBER undertakes to immediately request the revocation of the certificate.

8. OBLIGATIONS OF THE CA

a. To issue, deliver, administer, revoke and renew certificates in accordance with the provisions of its Statement of Certification Practices and Policies.
b. Notify the APPLICANT or the ENTITY of the revocation of their Certificate or for which they are responsible, when this occurs, explaining the reasons, the date and time at which the certificate will be null and void in accordance with the procedures defined in the DPPC. For security reasons, the CA may unilaterally and immediately revoke a certificate without the HOLDER/SIGNATORY or the ENTITY being able to claim any type of compensation for this fact. DIGITEL TS will replace the certificate with a valid one as long as the anomaly has been corrected.
c. Keep the database of valid certificates and revoked certificates updated.
d. Process requests for revocation of certificates as soon as possible.
e. Provide through the OCSP service information on the revocation status of certificates that have expired without a time limit after their expiration.
f. In the event of compromise of the CA's private key, DIGITEL TS will provide information on the revocation status of the certificates issued by the CA through the OCSP service of a new CA, in accordance with the provisions of its Statement of Certification Practices and Policies.
g. In the event of termination of the service provided by DIGITEL TS with the transfer of certificate management to another Qualified Trust Service Provider, DIGITEL TS will also transfer to the new Provider the obligation to provide information on the status of revocation of the certificates issued by the CA through the OCSP service of an MA of the new Provider, in accordance with the provisions of its Statement of Certification Practices and Policies.

h. In the event of termination of the service provided by DIGITEL TS without transfer of certificate management to another Qualified Trust Service Provider, the CA will issue the last CRL that will be kept in custody and available by another reliable party to which DIGITEL TS transfers this obligation, in order to continue providing through it the information on the status of revocation of the certificates, in accordance with the provisions of its Statement of Certification Practices and Policies.
i. To correctly identify, by means of the RA, the APPLICANT, in accordance with the procedures established in the DPPC.
j. If applicable, verify the data relating to the constitution and legal personality of the ENTITY and the APPLICANT's relationship of representation or corporate membership with it, in accordance with the procedures established in the DPPC.
k. To archive and keep the information relating to the data sent and received for 15 years from the expiration of the Certificate or the end of the service provided. This registration activity may be carried out by electronic means.
l. Proceed, by means of the RA, to deliver the Certificate to the APPLICANT in accordance with the conditions defined in the DPPC, once the above checks have been carried out.
m. To carry out the service with the appropriate technical and material means, and with personnel who meet the qualification and experience conditions established in the DPPC.
n. Comply with the levels of quality of service, in accordance with what is established in the DPPC, in the technical, operational and safety aspects.
o. Implement appropriate security procedures and mechanisms for cybersecurity risk management, in accordance with the NIS2 Directive and Implementing Regulation (EU) 2024/2690.
p. Notify the supervisory body of any change in the provision of its qualified trust services at least one month in advance, in accordance with Article 24(2)(a) of the eIDAS Regulation, or three months in the event of an intention to cease activity.
q. Have an updated termination plan to ensure continuity of service, in accordance with Article 24.2.i) of the eIDAS Regulation.
r. Have communication channels for customer and third party attention to requests, incidents, queries, complaints and claims and attend to them within a reasonable time.
s. Keep all the information associated with the provision of the service with the required levels of protection.
t. Have civil liability insurance to cover the risks arising from the service in accordance with Article 24.2 c) of the eIDAS Regulation and Article 9.3 b) of Law 6/2020.
u. Select service providers and subcontractors that provide cybersecurity guarantees in accordance with applicable law, and require them to propagate DIGITEL TS security requirements throughout their supply chain.
v. Carry out the necessary periodic audits, every two years, to ensure compliance with the applicable regulations, and inform the supervisory body at least one month before any planned audit, allowing its participation as an observer, in accordance with Article 20.1 bis of the eIDAS Regulation.

9. OBLIGATIONS OF THE APPLICANT AND THE HOLDER/SIGNATORY OF THE CERTIFICATE

a. Safeguard the Certificate and the secret keys, Password, pins or signature or seal activation data diligently, taking reasonable precautions to prevent their loss, disclosure,

modification or unauthorized use, maintaining exclusive control over the electronic signature creation data or control over the electronic seal creation data.

b. Request the revocation of the Certificate when any of the cases of revocation of certificates provided for in the DPPC and in current legislation are met.
c. Do not reveal the private key.
d. Provide all the required information and documentation, taking responsibility for its veracity and correctness.
e. Immediately notify the CA in the event that it detects that any incorrect or inaccurate information has been included or in the event that, unexpectedly, the information in the Certificate does not correspond to reality.
f. Immediately inform the CA of any situation that may affect the validity of the Certificate, or the security of the keys.
g. Use the Certificate in accordance with the Law and the limits set by the DPPC and the Certificate itself according to its type.
h. Use the key pair only for the purposes authorized by the type of certificate (electronic signature or electronic seal, as applicable),
i. Any other that derives from the content of the DPPC in relation to each type of certificate.

10. OBLIGATIONS OF THE SUBSCRIBING ENTITY

The obligations b., d., e., f., g. and h. of the APPLICANT shall also apply to the ENTITY, which may be exercised through its legal representative.

11. LIMITS OF USE ACCORDING TO THE PURPOSE OF THE CERTIFICATE

Each type of certificate is intended for a specific person (natural or legal person) and responds to its own functions that are defined in the DIGITEL TS DPC. To the extent that qualified certificates may contain specific attributes of the HOLDER/SIGNATORY or the HOLDER/SUBSCRIBER, the AR carries out the necessary checks prior to their issuance to reliably accredit these attributes (representation relationship, corporate membership, association, etc.). In the case of electronic signature certificates with the attribute of entity representation, the Certificate contains the references of the document on the basis of which it has been accredited to the HR that the powers of representation of the HOLDER/SIGNATORY are in accordance with the purpose of the Certificate. However, it is the responsibility of the HOLDER/SIGNATORY to make appropriate use of their certificate in accordance with its purpose and the powers of representation that have been granted to them, and it is the responsibility of the third parties who trust to verify the purpose of the certificate and its possible limitations in its use.

12. PROHIBITION OF TRADING WITH THE CERTIFICATE

The contracting of the certificate issuance service with DIGITEL TS only allows the use of the Certificate in the scope of activity of the APPLICANT or the ENTITY, according to the purpose of the type of certificate requested. Once the Certificate has been issued, the APPLICANT or the ENTITY may not, unless specifically agreed between the parties, make commercial use of the

Certificate. Commercial use of the Certificate is understood to be any action by which the APPLICANT or the ENTITY offers to third parties outside this contract, for consideration or free of charge, services that require the use of the Certificate issued.

The Digitel TS certificate issuance service has not been designed nor does it allow its use as control equipment for dangerous situations, or for uses that require error-proof actions, such as the operation of nuclear facilities, air navigation or communication systems, air traffic control systems or arms control systems. where an error could directly cause death, physical damage or serious environmental damage.

Failure to comply with this clause will entitle the CA to revoke the Certificate and to claim compensation for the damages caused by the breach, including loss of profit and indirect damages.

The AC does not accept liability for damages arising from the use of the service that exceed the limitations indicated in these terms and conditions, in accordance with article 13.2 of the eIDAS Regulation and ETSI EN 319 401 REQ-6.2-02 b).

13. RIGHT OF WITHDRAWAL

The provision of the Certificate to the APPLICANT or to the ENTITY, either by means of its delivery for download in software format, or by delivery in a centralised qualified signature creation device (QSCD), implies the beginning of the execution of the contract, with which, as permitted by the General Law for the Defence of Consumers and Users (RDL 1/2007) in such cases, the APPLICANT and the ENTITY lose their right of withdrawal.

14. RESPONSIBILITIES

The CA and, where appropriate, the AR will be responsible for the functions that correspond to them in accordance with the DPPC and, in particular, will assume full responsibility for the correct verification of the identity of the APPLICANT, and where appropriate of the ENTITY and other appropriate circumstances.

DIGITEL TS maintains sufficient financial resources and/or appropriate liability insurance, in accordance with applicable law, to cover liabilities arising from its operations and activities. The minimum insured coverage is 3,000,000 euros.

The CA and the RA shall not be liable for damages arising from or related to the non-execution or defective execution of the obligations of the APPLICANT, the ENTITY and/or Third Party users, nor for the incorrect use of the Certificates and keys, nor for any indirect damage that may result from the use of the Certificate or the information provided by the CA, in particular, loss of profit, loss of income or orders or loss of data, not giving rise to any type of right to compensation.

Neither the CA nor the RA will be liable to the HOLDER/SIGNATORY or HOLDER/SUBSCRIBER or to third parties for the improper or fraudulent use of the Certificate in the event that the HOLDER/SIGNATORY or HOLDER/SUBSCRIBER has assigned it or has authorized its use in favor of a third person, being the sole responsibility of the HOLDER/SIGNATORY or HOLDER/SUBSCRIBER to control the keys associated with their certificate.

Neither the CA nor the RA will be responsible for any inaccuracies in the Certificate resulting from the information provided by the APPLICANT, provided that they have always acted with the maximum diligence required.

Neither the CA nor the RA shall be liable for the failure to perform or delay in performance of any of the obligations under the DPPC if such failure to perform or delay results from or is the result of force majeure, acts of God or, generally, any circumstance over which the CA cannot have reasonable control and including, but not limited to: natural disasters, war, state of siege, disturbances of public order, transport strikes, power and/or telephone supply cuts, computer viruses, deficiencies in telecommunications services, security violations of the certification system or any damage arising from an event caused by an unforeseeable advance in technology.

Neither the CA nor the RA will be responsible for the content of those digitally signed or encrypted documents.

The CA and the RA shall not be responsible for the correct operation with applications that are not approved, and for damages generated by the impossibility of use with such applications.

Neither the CA nor the RA will be liable for damage or breakdowns in computer equipment or data for reasons not directly attributable to the use of the Certificates or the installation of the certificate, and provided that the APPLICANT does not act with the necessary diligence.

In any case and regardless of the nature of the declaration of will that is substantiated or the public or private status of the person who signs or trusts the certificates, as well as the amount of the damages that may be caused, the maximum amount for which DIGITEL TS will be liable in the event of negligent action in the fulfillment of the obligations assumed will be SIX THOUSAND EUROS (€6,000) per certificate, unless an upper limit has been expressly agreed.

15. MODIFICATIONS

The CA may modify this contract, as well as the DPPC or any of its clauses in the terms provided therein, notifying the APPLICANT or the SUBSCRIBER, when the change directly affects their rights and obligations, 15 days in advance, and must explain, in any case, the reasons for such decision. The APPLICANT or the SUBSCRIBER may choose between the termination of the contract or the novation of the contract in accordance with the new terms. The APPLICANT or the SUBSCRIBER will have a maximum of 15 days from the date of said communication to notify the CA of the acceptance of the subrogation or the modifications made. However, if after that period the CA has not received written communication from the APPLICANT or the SUBSCRIBER to the contrary, the subrogation and the modifications made will be understood as accepted.

16. SERVICE AVAILABILITY

Certificate status application and/or consultation is available 24 hours a day, 7 days a week, 365 days a year as outlined in sections 2.1 and 4.9.9 and 4.10.2 of the DPPC.

DIGITEL TS guarantees the availability of the certificate status query service (OCSP and CRL) at least 99% of the time, in accordance with the service levels established in the DPPC. The period

for which DIGITEL TS retains the service event logs is established in accordance with the DPPC and applicable legislation, being at least 15 years.

However, it may be temporarily interrupted for reasons of maintenance, updating or improvement of the system, after notifying the SUBSCRIBER with reasonable notice. In the event of an emergency or security incident, DIGITEL TS reserves the right to interrupt the service immediately to protect the integrity of the evidence and the safety of users.

17. COMPLAINTS AND SUGGESTIONS

Any party interested in making a suggestion, complaint or claim regarding the DIGITEL TS certificate issuance service, may do so through the info@digitelts.com email account or through the following url: https://digitelts.es/contacto/

In any case, DIGITEL TS has a maximum period of 30 days to deal with the complaint or claim made.

18. INFORMATION FOR TRUSTED PARTIES

Relying parties on certificates issued by DIGITEL TS should verify the validity of the Certificate by consulting the Health Check Services (OCSP or CRL) before relying on the Certificate. Certificate status information is available at the distribution points indicated on the certificate itself and in https://pki.digitelts.es/. Trusting parties must verify the entire certificate chain before trusting a digital signature or any of the certificates in the hierarchy.

Relying parties should be aware of any limitations on the use of the Certificate, whether contained in the Certificate itself or in these terms and conditions, as well as the validity period associated with the Certificate.

19. DATA PROTECTION

In accordance with the provisions of EU Regulation 2016/679 of 27 April 2016 on General Data Protection, and Organic Law 3/2018, we provide you with the following information regarding the processing of your personal data within the framework of the provision of the service of issuing certificates:

Data controller:

DIGITEL ON TRUSTED SERVICES, S.L.U.
NIF: B47447560
Postal address: C/ Enrique Cubero 9, Edificio Madison Arena - 47014 – Valladolid (Spain)
Phone: +34 91 015 05 10
Mail: dpo@madisonmk.com

Purpose of processing:

The processing of your personal data will serve the intended uses of the provision of the contracted trust service, which includes the reliable identification of the APPLICANT for the Certificate, the issuance of the requested Certificate and the conservation of the evidence generated by the service for the legally required period. They will also be used for the administrative, technical and contractual management of the service, including its invoicing.

DIGITEL TS obtains the personal data contained in the files by several procedures:

- By transfer of the data by the SUBSCRIBER through the APPLICANT, who must have obtained them legally, under the conditions provided for in the regulations on electronic signature and on the protection of personal data.
- Directly from the OWNER/SIGNATORY, when the registration of your data is carried out by the DIGITEL TS CA or by its authorized intermediaries.

For the certificate issuance service, the personal data will be included in the directory of electronic signature public keys necessary to verify the validity of the electronic certificate as well as in the directory of revoked certificates, so that they will be processed automatically so that they can be accessed for consultation by all users of the system. that is, the people who voluntarily trust and make use of the certificates, always in accordance with the provisions of the PDS and the DPPC of DIGITEL TS.

In accordance with the applicable regulation on electronic certification, the mechanics of the certification system and the internet require that users of the system can access their personal data from anywhere in the world, so you are informed that, if you contract the service, your data will be available for consultation by users of the system. DIGITEL TS is exonerated from any liability arising from improper use of the same by third parties.

No profiling will be created based on the information provided and no automated decisions will be made.

Within the framework of remote identity verification processes for certificate APPLICANTS, DIGITEL TS may use unassisted video identification. Consequently, it will require processing other personal data of the user, specifically biometric data. Prior to the verification of identity by this modality of the service, DIGITEL TS will make available to the APPLICANT of the certificate the information on the protection of personal data and will obtain their consent for the processing of the aforementioned data.

Storage Periods:

The data provided will be kept in electronic and/or paper format, for as long as the commercial relationship is maintained and for the years necessary to comply with the legal obligations of registration and access, in particular those defined in article 9.3 of Law 6/2020, regulating certain aspects of electronic trust services (15 years) and EU Regulation No. 910/2014.

Within the framework of remote identification by video-identification, DIGITEL TS will keep for 15 years the evidence of successful identification processes and for 5 years the evidence of those video identification processes that have failed in accordance with the provisions of Order ETD/465/2021, of May 6, which regulates the methods of remote identification by video for the issuance of qualified electronic certificates, amended by Order ETD/743/2022, of 26 July.

Legitimacy of processing:

The legal basis for the processing of your personal data is either in:

i. the contractual relationship established by virtue of the services contracted from DIGITEL TS according to the conditions of use that appear with the subscription of the services,
ii. the very purpose of the provision of issuance of electronic certificates that requires linking signature validation data with a natural person,
iii. the legal obligation imposed on Qualified Trust Service Providers issuing qualified trust service certificates to verify the identity and other attributes of the natural person to whom a qualified certificate is issued (Law 06/2020 and EU Regulation No. 910/2014) and to record and keep such data accessible for the stipulated legal period (15 years).
iv. The consent of the APPLICANT for his/her biometric personal data to be processed within the framework of remote identity verification processes by video-identification.

We would like to inform you that the contracting of our services obliges the customer to provide their personal data, even in the case of using a pseudonym, so if they do not consent to the processing of their personal data, the service cannot be provided.

Recipients (assignments and transfers):

To provide its certificate issuance services, DIGITEL TS may delegate registration tasks to a third party. This entity, in its capacity as Registration Authority within the DIGITEL TS certification system, will be considered a Data Processor by having access to the data it has provided to DIGITEL TS, for the sole and exclusive fulfillment of its registration tasks when these are necessary to provide the contracted service.

Your personal data will not be transferred to third parties unless legally obliged, nor will it be transferred to third countries or international organizations.

Rights of interested persons:

Persons who have provided their data have the right to:

- To know if your personal data is being processed by DIGITEL TS.
- Access your personal data and request its rectification or deletion, for example, if the data is no longer necessary for the purposes for which it was collected.
  In case of requesting the rectification or deletion of your personal data from our databases, you are informed that the electronic certificates issued in your name and in force at that time must be revoked by DIGITEL TS. DIGITEL TS will keep a copy of said data only for the purpose of complying with legal obligations regarding retention periods and for the exercise or defense of claims.
- Request the limitation of the processing of your data to the main purpose for which they were transferred to DIGITEL TS, withdrawing your consent to their processing for information or commercial prospecting purposes. Such a request will not affect the lawfulness of the prior processing based on the contractual need to process your data.
- Request the portability of your personal data in favor of another controller.

To exercise your rights, you can use one of two options:

- Electronically by sending an email to dpo@madisonmk.com with the subject "Data Protection".

- By post by sending a letter to "DPO" C/ Enrique Cubero 9, Edificio Madison Arena - 47014 Valladolid (Spain), with the Reference "Data Protection".

If they have not obtained satisfaction with the request to exercise their rights, they may file a complaint with the Data Protection Supervisory Authority, by contacting the Electronic Office of the Spanish Data Protection Agency.

Further details on how your personal data are processed can be found in the DIGITEL TS Privacy Policy available on the following website: DIGITEL T.S.MK - Privacy Policy

20.TERMINATION OF THE CONTRACT

Failure to comply with the stipulations contained in this contract and/or in the DPPC by either party will be cause for termination of this contract. In such a case, the non-defaulting party shall have the right to terminate the contract with immediate effect. Failure by the APPLICANT or the ENTITY will entitle the CA to revoke the Certificate, regardless of the damages that may be claimed.

The CA will have the right to revoke and not renew the Certificate prior to the established term of validity in the cases provided for in the DPPC. When the revocation is unjustified, the CA may compensate those APPLICANTS or ENTITIES that request it in writing within three months following the date of revocation. This compensation may not be higher than that paid by the APPLICANT himself for obtaining the aforementioned Certificate.

THE APPLICANT or the ENTITY may freely terminate this contract at any time by giving 30 days' written notice. In no case will this resolution give the right to a refund of the amounts paid for obtaining the Certificate.

If the exercise of the rights of opposition or cancellation of personal data hinders the provision of services subject to this contract, DIGITEL TS will be entitled to terminate this contract.

21. LEGISLATION AND JURISDICTION

This contract and the DPPC will be governed by the Spanish and European Law on the issuance of qualified certificates applicable at all times and according to which its content must be interpreted.

For the resolution of any conflict that may arise in relation to this contract, the parties, waiving any other jurisdiction that may correspond to them, submit to the jurisdiction of the Courts of the city of Valladolid (Spain).

SECTION II
TERMS AND CONDITIONS APPLICABLE TO
REMOTE ELECTRONIC SIGNATURE AND SEAL CERTIFICATES

The eIDAS Regulation regulates the possibility of entrusting qualified electronic signature and seal creation devices to a third party, provided that appropriate procedures and mechanisms are in place to ensure that the signatory has exclusive control over the use of their electronic signature creation data, that the seal creator is in control of the use of their electronic seal creation data, and that the use of the devices complies with the requirements of the qualified electronic signature and the qualified electronic seal. This makes it possible to create electronic signatures and seals remotely in an electronic signature and seal creation environment managed by a Qualified Trust Service Provider on behalf of the signatory or the creator of the seal, for which specific management and administrative security procedures are applied and reliable systems and products are used, including secure electronic communication channels to ensure that the e-signature and e-seal creation environment is reliable and used under the sole control of the signatory or under the control of the seal creator (Articles 29a and 39a *of the eIDAS Regulation*).

The DIGITEL TS remote electronic signature and seal creation service operates in accordance with the EUSPv2 (EU SSAS Policy v2) defined in ETSI TS 119 431-1, which includes the specific requirements of Regulation (EU) 2024/1183 regarding the management of remote QSCD. The OID for this policy is: 0.4.0.19431.1.1.4.

22. OTHER OBLIGATIONS OF THE CA

a. The CA shall implement specific management and administrative security procedures and use reliable systems and products, including secure electronic communication channels to ensure that the electronic signature and seal creation environment is reliable and used under the sole control of the signatory or under the control of the seal creator. The QSCD shall be operated in its configuration in accordance with the relevant certification documentation or in an equivalent configuration that achieves the same security objective. In any case, the CA's guarantee in this regard is limited to the correct functioning of the remote signature procedure and remote stamping in accordance with the level of service contracted.
b. The CA must safeguard the data for the creation of the electronic signature or electronic seal on behalf of the signatory or creator of the seal and protect them against any alteration, destruction or unauthorised access, as well as guarantee their continuous availability to the signatory or creator of the seal. The signer or stamp creator's signature keys will be generated and used only within a QSCD.
c. Due to its technical and usability characteristics, the remote certificate requires the use of APIRest services and/or specific applications for its use. Such add-ons will be provided to the user during the process of issuing the Certificate and are therefore part of the service.
   The CA may only duplicate electronic signature or electronic seal creation data for backup purposes, provided that: (i) the security of the duplicate datasets is of the same level as that of the original datasets; and (ii) the number of duplicate datasets does not exceed the minimum necessary to ensure continuity of service, in accordance with Article 29 bis 1.b) of the eIDAS Regulation.
   The CA shall comply with any requirements identified in the certification report of the specific qualified signature or remote seal device used.

23. OTHER OBLIGATIONS OF THE HOLDER/SIGNATORY AND THE HOLDER/SUBSCRIBER

a. The OWNER must safeguard his/her signature activation data (SAD) diligently and apply all appropriate measures aimed at avoiding damage to third parties as a result of the use of electronic signatures or electronic seals or authentication processes. The authentication tools for the activation of the remote signature or remote seal procedure are strictly personal, so the OWNER is required to protect the secrecy of such tools by not disclosing them to third parties in whole or in part and by storing them securely, maintaining exclusive control (in the case of electronic signature certificates) or control (in the case of electronic seal certificates) over the data signature activation.
b. In the event that the HOLDER assigns the use of his/her certificate in favour of another person based on the general rules of the legal business of the mandate or the rules governing the power of attorney and delegations of functions, the HOLDER will be solely responsible to third parties or to the ENTITY he/she represents if he/she is not duly authorised to do so, of the consequences that improper use of the Certificate may generate, without prejudice to actions against the person who may have exceeded the authorized limits of use.
c. The OWNER must update its hardware and software systems to comply with the security requirements required by applicable laws.
d. The HOLDER/SIGNATORY acknowledges that the qualified electronic signature generated through the remote signature service has legal effects equivalent to a handwritten signature, in accordance with article 25.2 of the eIDAS Regulation, provided that a certified QSCD has been used and the established requirements are met.
e. The OWNER expressly authorizes DIGITEL TS to generate and manage the data for the creation of an electronic signature or electronic seal on its behalf, as well as to duplicate said data solely for backup purposes under the terms established in these terms and conditions, in accordance with article 29 bis of the eIDAS Regulation.

SECTION III
TERMS AND CONDITIONS APPLICABLE TO
VIDEO IDENTIFICATION FOR THE ISSUANCE OF QUALIFIED SIGNING CERTIFICATES

24. TERMS AND CONDITIONS APPLICABLE TO UNATTENDED VIDEO IDENTIFICATION

The APPLICANT declares that he/she accepts the performance of the unassisted video identification process for the issuance of qualified certificates of the DIGITEL TS Certification Authority and will use the Unassisted Video Identification Service in accordance with the attached conditions and the Statement of Certification Practices and Policies of the DIGITEL TS Certification Authority and in accordance with Order ETD/465/2021, of 6 May, which regulates the methods of remote identification by video for the issuance of qualified electronic certificates and concordant standards, consenting to the full recording of your image and voice and the obtaining

of other evidence during the registration process, as well as the processing and conservation of special categories of personal data (biometric data) and the non-application of the right of withdrawal once the service has been completely executed, in accordance with the provisions of Royal Legislative Decree 1/2007, of 16 November, which approves the revised text of the General Law for the Defence of Consumers and Users and other complementary laws.

These terms and conditions are established in order to provide clear and understandable information to APPLICANTS about the unassisted video-identification service, the applicable security recommendations and privacy information, as established in the applicable rules. The APPLICANT, by accepting these conditions, grants express consent for the complete recording of the video and for the processing and conservation of special categories of data. By clicking on the Accept option, to carry out the identity verification process by means of unassisted video-identification to obtain a qualified electronic signature certificate, you are also accepting the privacy policy, information on data protection and these conditions of use. Failure to accept these conditions means that you will not be able to access the video-identification service.

DIGITEL TS, as a Qualified Trust Service Provider, informs you that there are other alternatives for identification that do not require the processing and storage of your image and biometric data, through physical presence before a DIGITEL TS Registry Office.

Since DIGITEL ON TRUSTED SERVICES S.L.U. and, where appropriate, the REGISTRATION AUTHORITY agree with the above, the APPLICANT or SUBSCRIBER reads, by himself, the entirety of this document and declares that he or she adheres to its content in its entirety, which is formalized by accepting the contract electronically, in accordance with the regulations in force on distance contracting.

Signed by the APPLICANT:

Signed by the SUBSCRIBER: