DIGITELTS
by MADISON

# Electronic Certificate Issuance Services

PKI Disclosure Statement (PDS) for Qualified Certificates

## DOCUMENT CONTROL

| | |
|---|---|
| Name | PKI Disclosure Statement (PDS) for Qualified Certificates of DIGITEL TS Electronic Certificate Issuance Services |
| Distribution | **Public** |
| Version | V1.0 |
| Date | 21/05/2026 |
| Approved | Risk and Security Committee of DIGITEL TS Date 22/05/2026 |
| Status | Approved |

## CHANGE CONTROL

| VERSION | DATE | DESCRIPTION |
|---|---|---|
| V1.0 | 21/05/2026 | First version of the document applicable to all types of qualified certificates issued by DIGITEL TS |

## TABLE OF CONTENTS

# 1. INTRODUCTION

This document constitutes the PKI Disclosure Statement (hereinafter referred to as the "PDS") of the qualified trust service provider DIGITEL TS for all types of qualified certificates issued by its Certification Authority.

This PDS has been prepared in accordance with the PKI Disclosure Statement model defined in Annex A of the ETSI EN 319 411-1 standard and is intended to provide subscribers, signatories, seal creators, and relying parties with clear, simplified, and accessible information regarding the qualified certificate issuance services provided by DIGITEL TS, complementary to the Certification Practice Statement and Certification Policies (CPS/CP). This PDS is not intended to replace the CPS/CP or the certification policies contained therein.

DIGITEL TS provides its qualified certificate issuance services in accordance with the provisions of Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 regarding the establishment of the European Digital Identity Framework (hereinafter referred to as the "eIDAS Regulation").

In addition, DIGITEL TS in the provision of the services of issuance of qualified certificates complies with the provisions of the following regulations:

- Commission Implementing Regulation (EU) 2025/1943 of 29 September 2025 laying down detailed rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards for qualified electronic signature certificates and qualified electronic seal certificates
- Commission Implementing Regulation (EU) 2025/2530 of 16 December 2025 laying down detailed rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards requirements for qualified trust service providers providing qualified trust services.
- Law 6/2020, of 11 November, regulating certain aspects of electronic trust services.
- Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights.

For qualified certificates issued to representatives of legal persons and entities without legal personality, as well as to the staff and organizations of the Spanish Public Administrations (Administrations, bodies or entities of public law), DIGITEL TS also takes into account the stipulations of the document entitled "Electronic Certificate Profiles 2.0" of the Subdirectorate General of Information, Documentation and Publications of the Ministry of Finance and Public Administrations within the framework of Spanish Laws 39/2015 and 40/2015 and Royal Decree 203/2021.

For the remote video identification of applicants for qualified electronic signature and seal certificates covered by the DPPC, the requirements defined in Order ETD/465/2021, of 6 May, regulating the methods of remote video identification for the issuance of qualified electronic certificates, have been taken into consideration. amended by Order ETD/743/2022, of 26 July.

To ensure the cybersecurity and cyber resilience of the services covered by this PDS, Digitel TS has aligned its operations with the network and information security requirements set out in Directive (EU) 2022/2555 (NIS2 Directive) and its Implementing Regulation (EU) 2024/2690; as well as to the implementing regulations that are issued, including the regulations transposing it into the Spanish legal system.

Qualified certificates issued by DIGITEL TS are certificates issued to the public.

This PDS is available in PDF/A format in accordance with ISO 19005, and can be consulted at: https://pki.digitelts.es

## 2. CONTACT INFORMATION

- Company name: DIGITEL ON TRUSTED SERVICES S.L.U.
- Trade Name: DIGITEL TS Certification Authority
- NIF: B47447560
- Address. C/ Enrique Cubero 9, Edificio Madison Arena - 47014 Valladolid (Spain)
- Telephone. +34 91 015 05 10
- Web: https://www.digitelts.es
- Email. info@digitelts.com
- Request for revocation: The request for revocation of the electronic certificate can be made through the email address info@digitelts.com or the Registration Authority that issued the certificate in question, following the process described in the Statement of Certification Practices and Policies (DPPC).
- Mercantile Registry of Valladolid: Volume 891, Folio 38, Section 8, Page VA-11307

# 3. TYPES AND PURPOSES OF CERTIFICATES

DIGITEL TS has assigned OID 1.3.6.1.4.1.54225.10 for its trust services for the issuance of electronic certificates.

End-entity certificates issued by the DIGITEL TS Certification Authority shall include the standard policy OIDs for qualified European Union certificates issued to natural persons and legal entities in accordance with the provisions of ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-2 and 3, where applicable:

- Qualified advanced electronic signature certificates in accordance with the QCP-n policy defined in the ETSI EN 319 411-2 standard.
- Qualified certificates of qualified electronic signature in accordance with the QCP-n-qscd policy defined in the ETSI EN 319 411-2 standard.
- Qualified certificates of advanced electronic seal in accordance with the QCP-l policy defined in the ETSI EN 319 411-2 standard.
- Qualified electronic seal certificates in accordance with the QCP-l – qscd policy defined in the ETSI EN 319 411-2 standard.

In addition, DIGITEL TS has defined its own OIDs to identify the applicable policy for each certificate profile covered by the DPPC.

For certificates issued to representatives of legal persons and entities without legal personality, as well as to the staff and organizations of the Spanish public administration (Administrations, bodies or entities of public law), DIGITEL TS has also taken into account the OIDs established in the document entitled "Electronic Certificate Profiles 2.0" of the Subdirectorate General of Information, Documentation and Publications of the Ministry of Finance and Public Administrations within the framework of Spanish Laws 39/2015 and 40/2015 and Royal Decree 203/2021.

The types of qualified certificates issued by DIGITEL TS, their own DIGITEL TS object identifiers (OIDs), the applicable ETSI policy and, where applicable, the OID of the certificate profile of the Ministry of Finance and Public Administrations, the validation procedures and the restrictions on use of each of them are described below.

## 3.1 QUALIFIED CERTIFICATE FOR QUALIFIED ELECTRONIC SIGNATURE FOR CITIZENS [CENTRALISED]

DIGITEL TS OID: OID 1.3.6.1.4.1.54225.10.3.5. ETSI Policy: QCP-n-qscd (OID: 0.4.0.194112.1.2).

These certificates are qualified certificates for electronic signature in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 and comply with the provisions of the technical regulations identified with the ETSI reference EN 319 411-2.

These certificates work with a qualified electronic signature creation device (QSCD), in accordance with Annex II of Regulation (EU) 910/2014.

These certificates are managed centrally, i.e. the generation and management of the electronic signature creation data is carried out by the provider, on behalf of the signatory.

These certificates guarantee the identity of the signatory, and allow the generation of the "qualified electronic signature", with legal effect equivalent to that of a handwritten signature in accordance with Article 25.2 of Regulation (EU) 910/2014.

## 3.2 QUALIFIED CERTIFICATE FOR ADVANCED ELECTRONIC SIGNATURE FOR CITIZENS [SOFTWARE]

DIGITEL TS OID: OID 1.3.6.1.4.1.54225.10.3.1. ETSI Policy: QCP-n (OID: 0.4.0.194112.1.0).

These certificates are qualified certificates for electronic signature in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 and comply with the provisions of the technical regulations identified with the ETSI reference EN 319 411-2.

These certificates do not work with a qualified electronic signature creation device (QSCD).

These certificates are managed in a distributed way without the involvement of a centralized management tool.

These certificates guarantee the identity of the signatory, and allow the generation of the "advanced electronic signature" based on a qualified certificate for electronic signature.

## 3.3 QUALIFIED CERTIFICATE FOR QUALIFIED ELECTRONIC SIGNATURE FOR ASSOCIATED INDIVIDUALS [CENTRALIZED]

DIGITEL TS OID: 1.3.6.1.4.1.54225.10.3.15. ETSI Policy: QCP-n-qscd (OID: 0.4.0.194112.1.2).

These certificates are qualified certificates for electronic signature in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 and comply with the provisions of the ETSI EN 319 411-2 technical standard.

These certificates work with a qualified electronic signature creation device (QSCD), in accordance with Annex II of Regulation (EU) 910/2014.

These certificates are managed centrally, i.e. the generation and management of the electronic signature creation data is carried out by the provider, on behalf of the signatory.

These certificates guarantee the identity of the signatory and their relationship with the organisation subscribing to the certificate, and allow the generation of the "qualified electronic signature", with legal effect equivalent to that of a handwritten signature in accordance with Article 25.2 of Regulation (EU) 910/2014.

## 3.4 QUALIFIED CERTIFICATE FOR ADVANCED ELECTRONIC SIGNATURE FOR ASSOCIATED INDIVIDUALS [SOFTWARE]

DIGITEL TS OID: 1.3.6.1.4.1.54225.10.3.11. ETSI Policy: QCP-n (OID: 0.4.0.194112.1.0).

These certificates are qualified certificates for electronic signature in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 and comply with the provisions of the ETSI EN 319 411-2 technical standard.

These certificates do not work with a qualified electronic signature creation device (QSCD).

These certificates are managed in a distributed way without the involvement of a centralized management tool.

These certificates guarantee the identity of the signatory and their link with the organization subscribing to the certificate, and allow the generation of the "advanced electronic signature" based on a qualified electronic signature certificate.

## 3.5 QUALIFIED CERTIFICATE FOR QUALIFIED ELECTRONIC SIGNATURE FOR REPRESENTATIVES OF LEGAL ENTITIES [CENTRALIZED]

DIGITEL TS OID: 1.3.6.1.4.1.54225.10.3.25. ETSI Policy: QCP-n-qscd (OID: 0.4.0.194112.1.2). OID of the profile of the Ministry of Finance and Public Administration: 2.16.724.1.3.5.8.

These certificates are qualified certificates for electronic signature in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 and comply with the provisions of the ETSI EN 319 411-2 technical standard.

These certificates work with a qualified electronic signature creation device (QSCD), in accordance with Annex II of Regulation (EU) 910/2014.

These certificates are managed centrally, i.e. the generation and management of the electronic signature creation data is carried out by the provider, on behalf of the signatory.

They are certificates of representative of a legal entity, with full powers, sole or joint administrator of the organization subscribing to the certificate, or at least with specific general powers to act before third parties.

These certificates guarantee the identity of the organisation subscribing to the certificate and the signatory, indicate a relationship of legal representation or general power of attorney between the signatory and the organisation subscribing to the certificate, and allow the generation of the "qualified electronic signature", with legal effect equivalent to that of a handwritten signature in accordance with Article 25.2 of Regulation (EU) 910/2014.

These certificates include a field indicating the document, public if required, which reliably accredits the signatory's powers to act on behalf of the legal entity they represent and, if registration is mandatory, the registration data.

## 3.6 QUALIFIED CERTIFICATE FOR ADVANCED ELECTRONIC SIGNATURE FOR REPRESENTATIVES OF LEGAL ENTITIES [SOFTWARE]

DIGITEL TS OID: 1.3.6.1.4.1.54225.10.3.21. ETSI Policy: QCP-n (OID: 0.4.0.194112.1.0). OID of the profile of the Ministry of Finance and Public Administration: 2.16.724.1.3.5.8.

These certificates are qualified certificates for electronic signature in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 and comply with the provisions of the ETSI EN 319 411-2 technical standard.

These certificates do not work with a qualified electronic signature creation device (QSCD).

These certificates are managed in a distributed way without the involvement of a centralized management tool.

They are certificates of representative of a legal entity, with full powers, sole or joint administrator of the organization subscribing to the certificate, or at least with specific general powers to act before third parties.

These certificates guarantee the identity of the organization subscribing to the certificate and the signatory, indicate a relationship of legal representation or general power of attorney between the signatory and the organization subscribing to the certificate, and allow the generation of the "advanced electronic signature" based on a qualified electronic certificate of electronic signature.

These certificates include a field indicating the document, public if required, which reliably accredits the signatory's powers to act on behalf of the legal entity they represent and, if registration is mandatory, the registration data.

## 3.7 QUALIFIED CERTIFICATE FOR QUALIFIED ELECTRONIC SIGNATURE FOR REPRESENTATIVES OF ENTITIES WITHOUT LEGAL PERSONALITY [CENTRALIZED]

DIGITEL TS OID: 1.3.6.1.4.1.54225.10.3.35. ETSI Policy QCP-n-qscd (OID: 0.4.0.194112.1.2). OID of the profile of the Ministry of Finance and Public Administration: 2.16.724.1.3.5.9.

These certificates are qualified certificates for electronic signature in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 and comply with the provisions of the ETSI EN 319 411-2 technical standard.

These certificates work with a qualified electronic signature creation device (QSCD), in accordance with Annex II of Regulation (EU) 910/2014.

These certificates are managed centrally, i.e. the generation and management of the electronic signature creation data is carried out by the provider, on behalf of the signatory.

They are certificates of representative of an entity without legal personality, with full powers, sole or joint administrator of the organization subscribing to the certificate, or at least with specific general powers to act before third parties.

These certificates guarantee the identity of the organisation subscribing to the certificate and the signatory, indicate a relationship of legal representation or general power of attorney between the signatory and the organisation subscribing to the certificate, and allow the generation of the "qualified electronic signature", with legal effect equivalent to that of a handwritten signature in accordance with Article 25.2 of Regulation (EU) 910/2014.

These certificates include a field indicating the document, public if required, which reliably accredits the signatory's powers to act on behalf of the entity without legal personality that he or she represents and, if registration is mandatory, the registration data.

## 3.8 QUALIFIED CERTIFICATE FOR ADVANCED ELECTRONIC SIGNATURE FOR REPRESENTATIVES OF ENTITIES WITHOUT LEGAL PERSONALITY [SOFTWARE]

DIGITEL TS OID: 1.3.6.1.4.1.54225.10.3.31. ETSI Policy: QCP-n (OID: 0.4.0.194112.1.0). OID of the profile of the Ministry of Finance and Public Administration: 2.16.724.1.3.5.9.

These certificates are qualified certificates for electronic signature in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 and comply with the provisions of the ETSI EN 319 411-2 technical standard.

These certificates do not work with a qualified electronic signature creation device (QSCD).

These certificates are managed in a distributed way without the involvement of a centralized management tool.

They are certificates of representative of an entity without legal personality, with full powers, sole or joint administrator of the organization subscribing to the certificate, or at least with specific general powers to act before third parties.

These certificates allow the generation of the "advanced electronic signature" based on a qualified electronic certificate.

These certificates guarantee the identity of the organization subscribing to the certificate and the signatory, indicate a relationship of legal representation or general power of attorney between the signatory and the organization subscribing to the certificate, and allow the generation of the "advanced electronic signature" based on a qualified electronic certificate of electronic signature.

These certificates include a field indicating the document, public if required, which reliably accredits the signatory's powers to act on behalf of the entity without legal personality that he or she represents and, if registration is mandatory, the registration data.

## 3.9 QUALIFIED CERTIFICATE FOR QUALIFIED ELECTRONIC SEAL FOR GENERAL GOVERNMENT [CENTRALISED-HIGH LEVEL]

DIGITEL TS OID: 1.3.6.1.4.1.54225.10.2.15. ETSI Policy: QCP-l-qscd (OID: 0.4.0.194112.1.3). OID of the profile of the Ministry of Finance and Public Administration: 2.16.724.1.3.5.6.1.

These certificates are qualified certificates for electronic seal in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 and comply with the provisions of the ETSI EN 319 411-2 technical standard.

These certificates work with a qualified electronic seal creation device (QSCD), in accordance with Annex II of Regulation (EU) 910/2014.

These certificates are managed centrally, i.e. the generation and management of the electronic seal creation data is carried out by the provider, on behalf of the creator of the seal.

These certificates guarantee the identity of the creator of the seal (Public Administration) and allow the generation of the "qualified electronic seal", which will enjoy the presumption of data integrity and the correctness of the origin of the data in accordance with Article 35.2 of Regulation (EU) 910/2014.

## 3.10 QUALIFIED CERTIFICATE FOR ADVANCED ELECTRONIC SEAL FOR PUBLIC ADMINISTRATION [SOFTWARE-INTERMEDIATE LEVEL]

DIGITEL TS OID: 1.3.6.1.4.1.54225.10.2.11. ETSI Policy: QCP-l (OID: 0.4.0.194112.1.1). OID of the profile of the Ministry of Finance and Public Administration: 2.16.724.1.3.5.6.2.

These certificates are qualified certificates for electronic seal in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 and comply with the provisions of the ETSI EN 319 411-2 technical standard.

These certificates do not work with a qualified electronic seal creation device (QSCD).

These certificates are managed in a distributed way without the involvement of a centralized management tool.

These certificates guarantee the identity of the creator of the seal (Public Administration), and allow the generation of the "advanced electronic seal" based on a qualified electronic seal certificate.

## 3.11 QUALIFIED CERTIFICATE FOR QUALIFIED ELECTRONIC SIGNATURE FOR PUBLIC EMPLOYEES [CENTRALIZED-HIGH LEVEL]

DIGITEL TS OID: 1.3.6.1.4.1.54225.10.3.55. ETSI Policy: QCP-n-qscd (OID: 0.4.0.194112.1.2). OID of the profile of the Ministry of Finance and Public Administration: 2.16.724.1.3.5.7.1.

These certificates are qualified certificates for electronic signature in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 and comply with the provisions of the ETSI EN 319 411-2 technical standard.

These certificates work with a qualified electronic signature creation device (QSCD), in accordance with Annex II of Regulation (EU) 910/2014.

These certificates are managed centrally, i.e. the generation and management of the electronic signature creation data is carried out by the provider, on behalf of the signatory.

These certificates guarantee the identity of the signatory and his/her link as a public employee with the organisation subscribing to the certificate, and allow the generation of the "qualified electronic signature", with legal effect equivalent to that of a handwritten signature in accordance with Article 25.2 of Regulation (EU) 910/2014.

## 3.12 QUALIFIED CERTIFICATE FOR ADVANCED ELECTRONIC SIGNATURE FOR PUBLIC EMPLOYEES [SOFTWARE-INTERMEDIATE LEVEL]

DIGITEL TS OID: 1.3.6.1.4.1.54225.10.3.51. ETSI Policy: QCP-n (OID: 0.4.0.194112.1.0). OID of the profile of the Ministry of Finance and Public Administration: 2.16.724.1.3.5.7.2.

These certificates are qualified certificates for electronic signature in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 and comply with the provisions of the ETSI EN 319 411-2 technical standard.

These certificates do not work with a qualified electronic signature creation device (QSCD).

These certificates are managed in a distributed way without the involvement of a centralized management tool.

These certificates guarantee the identity of the signatory and his/her link as a public employee with the organization subscribing to the certificate, and allow the generation of the "advanced electronic signature" based on a qualified electronic signature certificate.

## 3.13 QUALIFIED CERTIFICATE FOR QUALIFIED ELECTRONIC SIGNATURE FOR PUBLIC EMPLOYEES WITH PSEUDONYM [CENTRALIZED-HIGH LEVEL]

DIGITEL TS OID: 1.3.6.1.4.1.54225.10.3.65. ETSI Policy: QCP-n-qscd (OID: 0.4.0.194112.1.2). OID of the profile of the Ministry of Finance and Public Administration: 2.16.724.1.3.5.4.1.

These certificates are qualified certificates for electronic signature in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 and comply with the provisions of the ETSI EN 319 411-2 technical standard.

These certificates work with a qualified electronic signature creation device (QSCD), in accordance with Annex II of Regulation (EU) 910/2014.

These certificates are managed centrally, i.e. the generation and management of the electronic signature creation data is carried out by the provider, on behalf of the signatory.

These certificates guarantee the identity of the signatory, by means of a pseudonym, and their link as a public employee with the organisation subscribing to the certificate, and allow the generation of the "qualified electronic signature", with legal effect equivalent to that of a handwritten signature in accordance with Article 25.2 of Regulation (EU) 910/2014.

## 3.14 QUALIFIED CERTIFICATE FOR ADVANCED ELECTRONIC SIGNATURE FOR PUBLIC EMPLOYEES WITH PSEUDONYM [SOFTWARE-MEDIUM LEVEL]

DIGITEL TS OID: 1.3.6.1.4.1.54225.10.3.61. ETSI Policy: QCP-n (OID: 0.4.0.194112.1.0). OID of the profile of the Ministry of Finance and Public Administration: 2.16.724.1.3.5.4.2.

These certificates are qualified certificates for electronic signature in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 and comply with the provisions of the ETSI EN 319 411-2 technical standard.

These certificates do not work with a qualified electronic signature creation device (QSCD).

These certificates are managed in a distributed way without the involvement of a centralized management tool.

These certificates guarantee the identity of the signatory, by means of a pseudonym, and his link as a public employee with the organization subscribing to the certificate, and allow the generation of the "advanced electronic signature" based on a qualified electronic signature certificate.

## 3.15 QUALIFIED CERTIFICATE FOR QUALIFIED ELECTRONIC SEAL FOR LEGAL ENTITIES [CENTRALIZED]

DIGITEL TS OID: 1.3.6.1.4.1.54225.10.2.5. ETSI Policy: QCP-l-qscd (OID: 0.4.0.194112.1.3).

These certificates are qualified certificates for electronic seal in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 and comply with the provisions of the ETSI EN 319 411-2 technical standard.

These certificates work with a qualified electronic seal creation device (QSCD), in accordance with Annex II of Regulation (EU) 910/2014.

These certificates are managed centrally, i.e. the generation and management of the electronic seal creation data is carried out by the provider, on behalf of the creator of the seal.

These certificates guarantee the identity of the creator of the seal and allow the generation of the "qualified electronic seal", which will enjoy the presumption of data integrity and the correctness of the origin of the data in accordance with Article 35.2 of Regulation (EU) 910/2014.

### 3.16 QUALIFIED CERTIFICATE FOR ADVANCED ELECTRONIC SEAL FOR LEGAL ENTITIES [SOFTWARE]

DIGITEL TS OID: 1.3.6.1.4.1.54225.10.2.1. ETSI Policy: QCP-l (OID: 0.4.0.194112.1.1).

These certificates are qualified certificates for electronic seal in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 and comply with the provisions of the ETSI EN 319 411-2 technical standard.

These certificates do not work with a qualified electronic seal creation device (QSCD).

These certificates are managed in a distributed way without the involvement of a centralized management tool.

These certificates guarantee the identity of the creator of the seal, and allow the generation of the "advanced electronic seal" based on a qualified electronic seal certificate.

## 4. VALIDITY PERIOD OF CERTIFICATES

The validity period will be as indicated on the certificate itself. However, DIGITEL TS issues all types of qualified electronic signature and electronic seal certificates valid for 3 years, 2 years and 48 hours.

# 5. CERTIFICATE USAGE LIMITS AND TRUST LIMITS

## 5.1 USAGE LIMITS FOR SIGNERS AND STAMP CREATORS

The signatory or the stamp creator must use the qualified certificate issuance service provided by DIGITEL TS exclusively for the uses authorized in the contract signed between DIGITEL TS and the subscriber, and which are reproduced below (section "obligations of signatories and stamp creators"). Likewise, the signatory or the creator of the seal undertakes to use the qualified service for the issuance of qualified certificates in accordance with the instructions, manuals or procedures provided by DIGITEL TS.

The signatory or creator of the seal must comply with any laws and regulations that may affect their right to use the cryptographic tools they employ.

The signatory or the creator of the seal may not adopt measures of inspection, alteration or reverse engineering of the services of issuance of qualified certificates of DIGITEL TS, without prior express permission.

Certificates issued in accordance with QCP-n-qscd and QCP-l-qscd policies require the use of a qualified electronic seal or signature creation device (QSCD). In centralised certificates, this device is managed by DIGITEL TS on behalf of the signatory or the creator of the seal.

## 5.2 USAGE LIMITS FOR VERIFIERS

Certificates are used for their own function and established purpose, and may not be used for other functions and for other purposes.

Similarly, certificates should be used only in accordance with applicable law, especially taking into account the import and export restrictions in place at any given time.

Except where expressly provided for in a procedure of the DIGITEL TS Certification Authority, certificates may not be used to sign requests for the issuance, renewal, suspension or revocation of certificates, or to sign public key certificates of any kind, or to sign certificate revocation lists (CRLs), without prejudice to the provisions of Article 24.1 bis letter b) of Regulation (EU) 910/2014.

The certificates have not been designed, cannot be used for and are not authorized for use or resale as hazardous situation control equipment or for uses that require fail-safe actions, such as the operation of nuclear facilities, air navigation or communications systems, or weapons control systems, where a failure could directly lead to death, personal injury or severe environmental damage.

The usage limits indicated in the fields and extensions of the certificate profiles should be taken into account, which do not include the encryption function of keys or other types of data. In any case, DIGITEL TS will not be liable for any loss of information encrypted with the public key contained in the certificates issued that cannot be recovered due to the loss of the private key or access to it by the holder of the certificate necessary to decrypt the information.

The use of the certificates in transactions that contravene this disclosure statement, the declaration of practices or the contracts with the subscribers, is considered improper use for the appropriate legal purposes, therefore exempting DIGITEL TS, according to current legislation, from any liability for this improper use of the certificates made by the signatory or any third party.

DIGITEL TS does not have access to the data on which the use of a certificate can be applied. Therefore, and as a consequence of this technical impossibility of accessing the content of the message, it is not possible for DIGITEL TS to issue any assessment on said content, therefore the subscriber or the person responsible for the use of the signature or electronic seal creation data of the certificate assumes any liability derived from the content associated with the use of the same. All this without prejudice to the regime applicable to information society services, when legally applicable.

Likewise, the subscriber or the person responsible for the use of the signature or electronic seal creation data of the certificate shall be responsible for any liability that may arise from the use of the same outside the limits and conditions of use set out in this disclosure statement, or in the contracts with the subscribers, as well as any other improper use of the same derived from this section or that may be interpreted as such in accordance with current legislation.

### 5.3 RELIANCE LIMITS

Qualified certificates issued by DIGITEL TS are intended for use with electronic signatures or electronic seals, as appropriate to the type of certificate, as well as for client authentication when accessing web services or TLS.

## 6. OBLIGATIONS OF SUBSCRIBERS

The obligations of the subscriber, as provided for in clause 6.3.5 (OVR-6.3.5-01 and OVR-6.3.5-02) of ETSI EN 319 411-1, include the following:

### 6.1 KEY GENERATION

The subscriber authorizes DIGITEL TS to generate the keys, private and public, for the identification and electronic signature of the signatories, and requests on their behalf the issuance of the certificate, and/or for the identification and electronic seal of the creator of the seal.

### 6.2 REQUEST FOR CERTIFICATES

The subscriber undertakes to make applications for certificates in accordance with the procedure and, if necessary, the technical components supplied by DIGITEL TS, in accordance with the provisions of the statement of certification practices and policies (DPPC) and in the DIGITEL TS operations documentation.

## 6.3 REPORTING OBLIGATIONS

The subscriber is responsible for ensuring that all information included in his/her certificate application is accurate, complete for the purpose of the certificate and is up to date at all times.

The subscriber must immediately inform DIGITEL TS:

- Any inaccuracies detected in the certificate once it has been issued.
- Any changes that occur in the information provided and/or registered for the issuance of the certificate.
- From the loss, theft, theft, or any other type of loss of control of the private key by the signer or the creator of the seal.

## 6.4 CUSTODY OBLIGATIONS

Where appropriate, the subscriber undertakes to safeguard all the information generated in its activity as a Registration Authority.

## 6.5 ADDITIONAL SUBSCRIBER OBLIGATIONS

In accordance with clause 6.3.5 (OVR-6.3.5-01 and OVR-6.3.5-02) of ETSI EN 319 411-1, additional obligations of the subscriber include:

a) Obligation for the key pair to be used exclusively in accordance with the limitations notified to the subscriber and the signatory or creator of the seal.
b) Prohibition of unauthorized use of the signer's or stamp creator's private key.
c) Obligation to promptly notify DIGITEL TS or the Registration Authority through which the certificate was issued if the private key has been compromised, if control over the activation data has been lost, or if inaccuracies in the content of the certificate are detected.
d) Obligation to immediately and permanently cease the use of the private key after its commitment.
e) Obligation to cease using the private key when the certificate has been revoked or when the issuing Certificate Authority has been compromised.

# 7. OBLIGATIONS OF SIGNATORIES AND CREATORS OF STAMPS

## 7.1 CUSTODY OBLIGATIONS

The signatory and the creator of the seal are obliged to safeguard the personal identification code or any technical support provided by DIGITEL TS, the private keys and, if necessary, the specifications owned by DIGITEL TS that are supplied to him/her.

The signer and the creator of the stamp are obliged to keep the personal identification code (PIN).

In the event of loss or theft of the certificate's private key, or in the event that the signatory or the creator of the seal suspects that the private key has lost reliability for any reason, such circumstances must be immediately notified to DIGITEL TS or to the Registration Authority through which the certificate was issued. directly or through the subscriber.

## 7.2 OBLIGATIONS OF CORRECT USE

The signatory and the creator of the seal must use the qualified certificate issuance service provided by DIGITEL TS, exclusively for the uses authorized in the DPPC and in any other instructions, manuals or procedures provided to the subscriber.

The signatory and the creator of the seal have to comply with any laws and regulations that may affect their right to use the cryptographic tools employed.

The signatory and the creator of the seal may not adopt measures to inspect, alter or decompile the digital certification services provided.

The signatory and the creator of the seal will recognize:

a) That when you use any certificate, and as long as the certificate has not expired or been suspended or revoked, you will have accepted that certificate and will be operational.
b) That it does not act as a Certificate Authority and, therefore, undertakes not to use the private keys corresponding to the public keys contained in the certificates for the purpose of signing any certificate.
c) That in the event of the private key being compromised, its use is immediately and permanently suspended.
d) For certificates issued in accordance with the QCP-n-qscd and QCP-l-qscd policies, the signer or seal creator is required to use the private key exclusively within the Qualified Signature or Seal Creation Device (QSCD).

## 7.3 PROHIBITED TRANSACTIONS

The signatory and the creator of the seal undertake not to use their private keys, certificates or any other technical support provided by DIGITEL TS in the performance of any transaction prohibited by applicable law.

The services for the issuance of qualified certificates provided by DIGITEL TS have not been designed and do not allow their use or resale 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 weapons control systems, where an error could directly cause death, physical damage or serious environmental damage.

# 8. OBLIGATIONS OF VERIFIERS

In accordance with clause 6.3.5 (OVR-6.3.5-03) of ETSI EN 319 411-1, the obligations of the parties relying on the certificates are as follows:

## 8.1 INFORMED DECISION

DIGITEL TS informs the verifier that it has access to sufficient information to make an informed decision at the time of verifying a certificate and to rely on the information contained in such certificate.

In addition, the verifier shall acknowledge that the use of the Certificate Revocation Lists (hereinafter referred to as the CRLs) and the DIGITEL TS OCSP service are governed by the DIGITEL TS DPPC and shall undertake to comply with the technical, operational and security requirements described in the aforementioned DPPC.

## 8.2 DIGITAL SIGNATURE VERIFICATION REQUIREMENTS

The check will normally be carried out automatically by the verifier's software and, in any case, in accordance with the DPPC, with the following requirements:

- It is necessary to use the appropriate software for the verification of a digital signature (electronic signature or electronic seal) with the algorithms and key lengths authorized in the certificate and/or to execute any other cryptographic operation, and to establish the chain of certificates on which the digital signature to be verified is based, since the digital signature is verified using this chain of certificates.
    - It is necessary to ensure that the identified chain of certificates is the most suitable for the digital signature being verified, since a digital signature can be based on more than one chain of certificates, and it is the decision of the verifier to ensure the use of the most appropriate chain to verify it.
    - It is necessary to check the revocation status of the certificates in the chain with the information provided by DIGITEL TS (CRL or OCSP service) to determine the validity of all the certificates in the certificate chain, since an electronic signature can only be considered correctly verified if each and every one of the certificates in the chain is correct and current.
    - It is necessary to ensure that all certificates in the chain authorize the use of the private key by the signer or the creator of the seal, since there is a possibility that some of the certificates include usage limits that prevent trusting the digital signature being verified. Each certificate in the chain has an indicator that refers to the applicable conditions of use, for review by verifiers.
- It is necessary to technically verify the digital signature of all certificates in the chain before trusting the certificate used by the signer.

## 8.3 TRUST IN AN UNVERIFIED CERTIFICATE

If the verifier relies on an unverified certificate, he will assume all the risks arising from this action.

## 8.4 EFFECT OF VERIFICATION

By virtue of the proper verification of certificates, in accordance with this disclosure statement, the verifier may rely on the identification and, where applicable, the public key of the signatory or the creator of the seal, within the corresponding limitations of use

## 8.5 PROPER USE AND PROHIBITED ACTIVITIES

The verifier undertakes not to use any type of information on the status of the certificates or any other type that has been provided by DIGITEL TS, in the performance of any transaction prohibited by the law applicable to the aforementioned transaction.

The verifier undertakes not to inspect, interfere with or reverse engineer the technical implementation of the public certification services of DIGITEL TS, without prior written consent.

In addition, the verifier undertakes not to intentionally compromise the security of the public services for the issuance of qualified DIGITEL TS certificates.

The services for the issuance of qualified certificates provided by DIGITEL TS have not been designed and do not allow the use or resale, as hazardous situation control equipment 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 weapons control systems, where a mistake could cause death, physical harm or serious environmental damage.

## 8.6 INDEMNITY CLAUSE

The third party relying on the certificate agrees to hold DIGITEL TS harmless from any damage arising from any action or omission resulting in liability, damage or loss, expenses of any kind, including legal and legal representation expenses that may be incurred, due to the publication and use of the certificate, when any of the following causes occur:

- Failure to comply with the obligations of the third party relying on the certificate.
- Reckless reliance on a certificate, in the light of the circumstances.
- Failure to check the status of a certificate, to determine that it is not suspended or revoked.
- Failure to verify all the security measures prescribed in the DPPC or other applicable regulations.

DIGITEL TS will not be liable in any case for any loss of encrypted information that cannot be recovered. DIGITEL TS will not be liable for damages caused in the terms indicated in article 11 of Law 6/2020, of 11 November, regulating certain aspects of electronic trust services.

# 9. OBLIGATIONS OF DIGITEL TS

In relation to the provision of the services of issuance of qualified certificates, DIGITEL TS undertakes to:

- To issue, deliver, administer, suspend, revoke and renew certificates, in accordance with the instructions provided by the subscriber, in the cases and for the reasons described in the DPPC of DIGITEL TS.
- To carry out the services with the appropriate technical and material means, and with personnel who meet the qualification and experience conditions established in the DPPC.
- Comply with the levels of quality of service, in accordance with what is established in the DPPC, in the technical, operational and safety aspects.
- Notify the subscriber, prior to the expiration date of the certificates, of the possibility of renewing them.
- Notify the signatories and creators of stamps of the revocation of the certificates, when this circumstance occurs.
- Communicate to third parties who request it, the status of the certificates, in accordance with what is established in the DPPC for the different certificate verification services.

In relation to registration checks

DIGITEL TS is obliged to issue certificates based on the data provided by the subscriber, for which it may carry out the verifications it deems appropriate regarding the identity and other personal and complementary information of the subscribers and, when appropriate, of the signatories.

These checks may include the documentary justification provided by the signatory through the subscriber, if DIGITEL TS deems it necessary, and any other relevant documents and information provided by the subscriber and/or the signatory.

In the event that DIGITEL TS detects errors in the data that must be included in the certificates or that justify this data, it may make the changes it deems necessary before issuing the certificate or suspend the issuance process and manage the corresponding incident with the subscriber. In the event that DIGITEL TS corrects the data without prior management of the corresponding incident with the subscriber, it must notify the subscriber of the finally certified data.

DIGITEL TS reserves the right not to issue the certificate, when it considers that the documentary justification is insufficient for the correct identification and authentication of the subscriber and/or the signatory.

The above obligations will be suspended in cases where the subscriber acts as Registration Authority and has the technical elements corresponding to the generation of keys, issuance of certificates and recording of corporate signature devices.

## 9.1 RETENTION PERIODS

DIGITEL TS keeps the information relating to the services provided in accordance with Article 24.2.h) of Regulation (EU) 910/2014, and Article 9.3 letter a) of Law 6/2020, for at least 15 years from the expiry of the certificate or the end of the service provided.

DIGITEL TS stores log information for a period of between 1 and 15 years, depending on the type of information recorded.

# 10. LIMITED WARRANTIES AND DISCLAIMERS OF WARRANTIES

DIGITEL TS Warranty for Digital Certification Services

**DIGITEL TS guarantees the subscriber:**

- That there are no factual errors in the information contained in the certificates, known or made by the Certification Authority.
    - That there are no factual errors in the information contained in the certificates, due to lack of due diligence in the management of the certificate application or in the creation of the certificate.
- That the certificates comply with all the material requirements established in the DPPC.
- That the revocation services comply with all the material requirements established in the DPPC.

**DIGITEL TS guarantees the third party relying on the certificate:**

- That the information contained or incorporated by reference in the certificate is correct, except where otherwise indicated.
- That the certificate has been issued to the subscriber and signatory identified therein and that the certificate has been accepted.
- That in the approval of the certificate application and in the issuance of the certificate, all the material requirements established in the DPPC have been met.
- The speed and security in the provision of services, especially revocation and deposit services.

**In addition, DIGITEL TS guarantees the subscriber and the third party that relies on the certificate:**

- That the certificate contains the information that a qualified certificate must contain, in accordance with Annex I (signature certificates) or Annex III (seal certificates) of Regulation (EU) No. 910/2014, as amended by Regulation (EU) No. 2024/1183.
- That, in the event that it generates the private keys of the subscriber or, where appropriate, of the natural person identified in the certificate (signatory), its confidentiality is maintained during the process.
- The responsibility of the Certification Authority, with the limits that are established. In no case will DIGITEL TS be liable for fortuitous events and in case of force majeure.

## 10.1 EXCLUSION OF WARRANTY

DIGITEL TS rejects any other guarantee different from the previous one that is not legally enforceable. Specifically, DIGITEL TS does not warrant any software used by any person to sign, verify signatures, encrypt, decrypt, or otherwise use any digital certificate issued by DIGITEL TS, except in cases where there is a written statement to the contrary.

## 10.2 LIMITATIONS OF LIABILITY

DIGITEL TS will be liable for the damage caused to the subscriber and/or signatory or any person who in good faith relies on the certificate, provided that there is intent or gross negligence, in accordance with the provisions of Article 13 of Regulation (EU) 910/2014 and Article 11 of Law 6/2020, of 11 November, regulatory of certain aspects of electronic trust services. The maximum amount for which DIGITEL TS will be liable in the event of negligent action in the fulfilment of the obligations assumed will be six thousand euros (€6,000) per certificate.

## 10.3 INSURANCE COVERAGE

DIGITEL TS has a guarantee of sufficient civil liability coverage, through professional civil liability insurance that complies with the provisions of Article 24.2.c) of Regulation (EU) 910/2014 and Article 9.3.b) of Law 6/2020, with a minimum insured of 3,000,000 euros.

# 11. APPLICABLE AGREEMENTS, DPPC, AND CERTIFICATION POLICY

## 11.1 APPLICABLE AGREEMENTS

The agreements applicable to the Digitel TS qualified certificate issuance service are as follows:

- Qualified certificate issuance services contract, which regulates the relationship between the DIGITEL TS Certification Authority and the Certificate Applicant/Subscriber.
- General Terms of Service incorporated into this disclosure statement (PDS) and the Certification Policy and Practices Statement (DPPC).

## 11.2 DPPC

The DIGITEL TS Certification Authority's qualified certificate issuance services are technically and operationally regulated by the DIGITEL TS Certification Authority's DPPC, for their subsequent updates, as well as for complementary documentation.

The DPPC and the operations documentation are regularly amended and can be consulted on the following websites: https://pki.digitelts.es

## 12. PRIVACY POLICY

DIGITEL TS has a privacy policy in place at the DPPC, and specific privacy regulation in relation to the registration process, confidentiality of registration, protection of access to personal information, and user consent, as required by Regulation (EU) 2016/679 (General Data Protection Regulation) and Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights.

The information referred to in the section on retention periods is kept for the periods indicated, duly recorded and with guarantees of security and integrity.

In particular, registration information is retained for at least 15 years from the expiration of the certificate or the termination of the service provided. The following information is kept confidential: applications for certificates, approved or denied, as well as any other personal information obtained for the issuance and maintenance of certificates; private keys generated and/or stored by the certification service provider; and transaction logs, including full logs and audit logs of transactions.

## 13. REFUND POLICY

DIGITEL TS will not reimburse the cost of the certification service under any circumstances.

## 14. GOVERNING LAW, CLAIMS, AND DISPUTE RESOLUTION

Relations with the DIGITEL TS Certification Authority will be governed by Spanish law on trust services in force at all times, as well as by civil and commercial legislation as applicable.

The competent jurisdiction is that indicated in Law 1/2000, of 7 January, on Civil Procedure.

In the event of a discrepancy between the parties, the parties shall attempt a prior amicable settlement. To this end, the parties must send a communication to the Certification Authority of DIGITEL TS by any means that is recorded at the contact address indicated in point 1 of this document.

If the parties do not reach an agreement in this regard, either of them may submit the dispute to civil jurisdiction, subject to the Courts of the registered office of the DIGITEL TS Certification Authority.

DIGITEL TS establishes, in the subscriber agreement and in this PDS, the applicable mediation and dispute resolution procedures, in accordance with the ETSI EN 319 411-1 standard.

# 15. ACCREDITATIONS, QUALITY SEALS AND CONFORMITY AUDITS

The DIGITEL TS Certification Authority is included in the Spanish list of trusted providers (TSL) https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx

DIGITEL TS is a company committed to the safety and quality of its services by obtaining and maintaining ISO/IEC 27001:2022 certification.

In accordance with the provisions of Regulation (EU) 910/2014, the DIGITEL TS Certification Authority will carry out compliance audits every 2 years and follow-up audits in the intervening years. Within the framework of these audits, DIGITEL TS verifies compliance with the controls defined in the Implementing Regulations of the eIDAS Regulation applicable to qualified certificate issuance services,

The qualified certificates issued by DIGITEL TS conform to the following technical standards:

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
- ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
- ETSI TS119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev.