DIGITO FINANCIAL TECHNOLOGY GROUP, LLC

PKI DISCLOSURE STATEMENT

Declaración de Divulgación de Prácticas (PDP)

Field	Detail
Document	PKI Disclosure Statement of Digito Financial Technology Group, LLC
Object Identifier (OID)	1.3.6.1.4.1.64999.6.2
Version	1.1
Date	10/27/2026
Location (Spanish)	https://digito.do/pds-es
Location (English)	https://digito.do/pds-en
Available languages	Spanish · English

This document provides an accessible summary of the conditions applicable to the trust services provided by **Digito Financial Technology Group, LLC**. It is structured in accordance with Annex A of ETSI EN 319 411-1 and is made available in compliance with requirement REQ-6.2-03 of ETSI EN 319 401. It is addressed to subjects, who are the subscribers of their certificates, to Affiliated Organisations and to relying parties, and is made available to them before they accept the service.

Its location is included in the *QcPDS* statement (OID 0.4.0.1862.1.5) of the qualified certificates issued by **DIGITO**, in accordance with ETSI EN 319 412-5.

This document does not replace DIGITO's Certificate Policies or the Certification Practice Statement, which are the reference documents and prevail in the event of discrepancy. All of them are published in DIGITO's repository. Among them, the applicable Certificate Policy prevails over the Certification Practice Statement.

This English version is provided in compliance with ETSI EN 319 412-5. In the event of discrepancy between language versions, the Spanish version shall prevail, as Spanish is the official language of the Dominican Republic and the language of the applicable legislation.

EMILY PEREZ GGT

1. Trust service provider and contact information

Field	Detail
Legal name	Digito Financial Technology Group, LLC
Taxpayer Registration Number (RNC)	1-32-46998-4
Registered office	Av. Gustavo Mejía Ricart No. 102, esq. Abraham Lincoln, Torre Corporativo 2010, Piso 13, Local 1302, Piantini, Santo Domingo
Website	https://digito.do
Contact e-mail	soporte@digito.do
Telephone	+1 809 920 8267
Policy Authority	pki@digito.do
Consumer and User Support Center	Same as above
Revocation requests (24 hours, 7 days)	DIGITO platform, after authentication (main channel; for certificates with institutional responsibility, also the Authorised Applicant through the organisation panel), or e-mail to soporte@digito.do. See Section 4.
Supervisory authority	Instituto Dominicano de las Telecomunicaciones (INDOTEL)
Authorisation number	115-2025

DIGITO operates as a Qualified Trust Service Provider authorised by the Dominican Institute of Telecommunications (INDOTEL), in accordance with Law No. 126-02 on Electronic Commerce, Documents and Digital Signatures, and with Resolution No. 067-2025 of the INDOTEL Board of Directors.

Enquiries, requests for information, complaints and technical support requests are handled through the Consumer and User Support Center, as set out in Section 8 of this document.

2. Certificate type, validation procedures and usage

DIGITO issues the following certificate types:

Certificate type	Identifier	Intended use
Qualified certificate for electronic signature of a natural person	1.3.6.1.4.1.64999.1.3.1	Qualified electronic signature by natural persons acting on their own behalf
Qualified certificate for electronic signature of a natural person with institutional responsibility	1.3.6.1.4.1.64999.1.3.4	Qualified electronic signature by natural persons associated with a legal person

DIGITO also provides a qualified time-stamping service, governed by the policy identified by OID 1.3.6.1.4.1.64999.1.3.2. This policy is based on the Best Practices Time-Stamp Policy of ETSI EN 319 421 (OID 0.4.0.2023.1.1). Before relying on a time-stamp, relying parties shall verify that it is correctly signed and that the time-stamping unit's key had not been compromised at the time of verification.

Natural person certificates are valid for thirty-six (36) months, and certificates with institutional responsibility for twelve (12) months, with mandatory re-verification of the affiliation and the role in the sixth month. Both are issued to the public under policy QCP-n-qscd of ETSI EN 319 411-2 and are Qualified Certificates for Electronic Signature under Article 38 of Resolution No. 067-2025. The private key is held in a qualified signature creation device (QSCD) managed by **DIGITO**, under the subject's sole control.

Identity verification

Before issuing any certificate, **DIGITO** verifies the identity of the subject through one of the following methods:

a) Automated. An unattended process in which the authenticity of the identity document is verified, a liveness check is performed, and the applicant's face is compared against the photograph on the document and against the records held by the Central Electoral Board (Junta Central Electoral). Where identity is evidenced by a passport, no comparison with the Central Electoral Board records applies; verification covers the authenticity of the document, including reading its chip where present, the liveness check and facial comparison against the document photograph.

b) Attended. A remote video session, by appointment, with an authorised **DIGITO** operator, in which the applicant presents the identity document and answers control questions.

c) In person. Identification before an authorised **DIGITO** operator, with physical presentation of the identity document.

Accepted identity documents: national identity and electoral card issued by the Central Electoral Board of the Dominican Republic, or a national or foreign passport.

For certificates with institutional responsibility, **DIGITO** additionally verifies the existence and validity of the legal person, by means of the Taxpayer Registration Number and the Commercial Registry or the constitutive document applicable to the type of entity, as well as the subject's institutional affiliation, the role to be included in the certificate and the authority of the Authorised Applicant. Only legal persons registered in the Dominican Republic are accepted.

Scope of certificates with institutional responsibility

The certificate attests to the identity of the subject and to the existence, as verified at the time of issuance, of an institutional affiliation with the legal person named in the certificate.

The certificate does NOT attest to the scope of the subject's powers of representation, nor to their capacity to legally bind the legal person towards third parties, nor to the continuation of the affiliation or role after issuance. The capacity in which the subject signs a given document derives from the declaration included in the signing act itself and from the applicable rules of representation. The title attribute is merely informative of the role verified at the time of issuance.

Prohibited uses

Certificates issued by **DIGITO** are not intended for encryption of information, session key establishment, or code signing. They may not be used after their expiry or revocation, nor for purposes other than those set out in the applicable Certificate Policy. Nor may they be used for unlawful or fraudulent acts. In particular:

- Natural person certificates do not attest to the representation of a legal person or to the subject's membership of an organisation.
- Certificates with institutional responsibility may not be used after the subject's institutional affiliation with the named legal person ends, or after the role stated in the certificate changes.

3. Reliance limits

Certificates issued under **DIGITO**'s Certificate Policies are intended exclusively for the creation of qualified electronic signatures (key usages digitalSignature and nonRepudiation), with the legal effects set out in Articles 9 and 10 of Law No. 126-02.

The following limits apply:

- The certificate may only be used during its validity period, as stated in the certificate itself.
- Use of the certificate for purposes other than those intended, or beyond the established limits, releases **DIGITO** from liability.
- **DIGITO** does not verify or warrant the content, accuracy or legal effects of the documents signed by the subject.
- **DIGITO** does not verify or warrant the subject's capacity or standing to perform the act being signed. For certificates with institutional responsibility, nor does it verify the scope of the powers conferred on the subject by the legal person.
- Registration information and event logs are retained for the periods set out in Section 7, and may be provided as evidence.

Operational limits of the signing platform

- PDF documents exceeding one hundred (100) MB are not accepted for the signing process.
- Natural person certificates: the signed document remains available for download for seven (7) calendar days. After that period it is deleted from the platform and cannot be recovered. Subjects are responsible for retaining a copy of the signed document.
- Certificates with institutional responsibility: the signed document remains available on the platform for as long as the agreement between DIGITO and the Affiliated Organisation remains in force, and for thirty (30) calendar days after its termination. After that period it is deleted from the platform and cannot be recovered.

DIGITO does not establish a monetary limit per certificate. Issued certificates do not include the QcLimitValue statement.

4. Obligations of subjects (subscribers) and Affiliated Organisations

Certificate acceptance

Acceptance requires an explicit, voluntary and unequivocal act by the subject: signing the Digital Certificate Use Agreement, expressly accepting the terms and conditions electronically on the registration portal, or voluntarily using the certificate once those conditions have been expressly accepted. Tacit acceptance is not admitted. For certificates with institutional responsibility, ratification by the Affiliated Organisation through its Authorised Applicant is also required.

Subject warranties and obligations

Upon accepting the certificate, the subject warrants that:

a) The electronic signature created using the certificate shall remain under their sole control.

b) No other person shall have access to the signature creation procedure.

c) The information contained in the certificate is true and corresponds to that provided to DIGITO.

The subject is further obliged to:

- Provide complete, accurate and truthful information, and keep it up to date.
- Safeguard their activation data and not disclose it to third parties. **DIGITO** cannot recover or reset activation data without a new identity verification.
- Use the certificate only for its intended purposes and during its validity period.
- Request revocation immediately, and in any case within twenty-four (24) hours, upon becoming aware of any circumstance giving rise to it, in particular the compromise or suspected compromise of their activation data.
- Keep their platform access credentials confidential and be accountable for all activity occurring in their account.
- Not allow third parties to use their private key. Any unauthorised use of the key is prohibited.
- Notify **DIGITO** without delay of any inaccuracy in, or change to, the information contained in the certificate.
- Permanently stop using the private key following its compromise or suspected compromise, or when informed that the certificate has been revoked or that the issuing Certification Authority has been compromised.
- Keep their contact details up to date on the platform and check there the validity status of their certificates. **DIGITO** does not send individual notice of upcoming expiry.

- For certificates with institutional responsibility, immediately notify **DIGITO** or the Affiliated Organisation of any change in their role and of the end of their institutional affiliation.

For certificates with institutional responsibility, the Affiliated Organisation is responsible for the authenticity of the documentation provided and for the validity of the institutional affiliation and of the role included in the certificate. It shall notify DIGITO within twenty-four (24) hours of any change affecting them, provide a six-monthly attestation of its subjects, affiliations and roles (failure to do so within fifteen (15) days of being requested is a ground for revocation), and shall not require the subject's activation data. It is liable for damage arising from any failure or delay in these notifications.

Failure to comply with the obligation to request revocation gives rise to liability towards good-faith third parties who relied on the certificate, in accordance with Article 49 of Law No. 126-02.

Certificate revocation

Revocation may be requested at any time (24 hours, 7 days) through the **DIGITO** platform or by e-mail to soporte@digito.do: by the subject, without giving reasons; for certificates with institutional responsibility, by the Affiliated Organisation through its Authorised Applicant; by **DIGITO** on its own initiative; or by INDOTEL or a competent authority. **DIGITO** publishes the revocation within twenty-four (24) hours. Revocation is irreversible; **DIGITO** does not suspend or renew certificates, and a new certificate requires a full new identity verification. For certificates with institutional responsibility, the end of the affiliation, a change of role or of the legal person's data, failure to complete the re-verification or the attestation, and termination of the agreement with the Affiliated Organisation are grounds for revocation (Section 4.9 of the applicable Certificate Policy).

5. Verification obligations of relying parties

Before relying on a certificate issued by **DIGITO,** the relying party shall:

a) Verify that the certificate was issued by a **DIGITO** Certification Authority, by validating the certification path up to the root certificate.

b) Check the revocation status of the certificate, using the online status service (OCSP) or the certificate revocation list, whose locations are stated in the certificate itself. The OCSP response is the preferred source. No effect shall be given to a certificate for which the service returns the status "unknown".

c) Verify that the certificate was valid at the time of signing. Where verification takes place after expiry, a qualified time-stamp evidencing the time of signing is required.

d) Check that the use of the certificate corresponds to that set out in the applicable Certificate Policy. For certificates with institutional responsibility, verify by appropriate means the subject's capacity for the specific act being signed.

e) Verify the signature on the response from the certificate status service and the validity of the responder certificate.

f) Take any other precautions set out in the Certificate Policy, the Certification Practice Statement and the applicable agreements.

g) Notify **DIGITO** of any incident detected in relation to an issued certificate.

Access to revocation status information is free of charge and requires no prior registration or authentication. The service is available on a continuous basis, twenty-four (24) hours a day, seven (7) days a week, with a service continuity rate of ninety-nine point seven per cent (99.7 %) measured annually, ninety-nine point five per cent (99.5 %) monthly on business days between 8:00 and 20:00, and ninety-nine point two per cent (99.2 %) at other times, in accordance with Article 48(c) of Resolution No. 067-2025. Scheduled maintenance interruptions are announced in the "Maintenance" section of DIGITO's website at least five (5) business days in advance and are preferably carried out at times of lower activity.

Certification Authority certificates and revocation lists are published in **DIGITO**'s repository (Certification Practice Statement, Section 2.1).

Failure to carry out these checks excludes the status of good-faith third party free from fault for the purposes of Article 49 of Law No. 126-02 and of DIGITO's limitations of liability.

6. Limited warranty, disclaimer and limitation of liability

DIGITO warrants that it provides its services in accordance with the Certificate Policies, the Certification Practice Statement and the applicable legislation, that the information in the certificate corresponds to that verified at the time of issuance, and that it revokes certificates and keeps status information available as described in this document. It gives no other warranty; in particular, it does not warrant the content or legal effects of the documents signed, the subject's capacity or powers for the act being signed, or the behaviour of third-party applications.

DIGITO is not liable for defects in the documentation provided that could not be detected by the established verification procedures; for any failure or delay by the subject or the Affiliated Organisation in requesting revocation or notifying changes; for use of the certificate beyond its limits; for damage resulting from the relying party's failure to carry out the checks in Section 5; or, for certificates with institutional responsibility, for the scope of the subject's powers of representation. These limitations do not affect **DIGITO**'s duty to revoke or any liability that cannot be excluded by law.

DIGITO maintains civil liability insurance with the minimum cover required by the applicable legislation. Subjects, Affiliated Organisations and relying parties shall hold **DIGITO** harmless against third-party claims arising from breach of their respective obligations.

7. Information retention periods

DIGITO retains information relating to issued certificates for the following periods, counted from the expiry or revocation of the certificate, whichever occurs first:

Information	Period
Register of issued certificates, certificates and revocation lists	Forty (40) years
Registration records and identity verification evidence	Twenty (20) years
Evidence of consent and acceptance of terms	Twenty (20) years
Lifecycle requests and decisions	Twenty (20) years
Documentation on the organisation, the institutional affiliation and the role; authority of the Authorised Applicant; periodic attestations; and contract with the Affiliated Organisation (certificates with institutional responsibility)	Twenty (20) years
Audit logs	Ten (10) years

The forty (40) year period derives from Article 52 of Law No. 126-02. The twenty (20) year period derives from Articles 14 and 17(h) of the Implementing Regulation of that Law.

Revocation status information remains available after certificates expire, so that signatures created during their validity period can still be verified.

8. Complaints and dispute resolution

DIGITO operates a Consumer and User Support Center which receives and handles enquiries and requests for information, complaints regarding the services provided, and technical support requests relating to document signing and to the use of the trust services. Disputes arising from the provision of the services shall first be submitted to this procedure.

Aspect	Applicable rules
Time limit for submitting a complaint	Thirty (30) calendar days from the event giving rise to it (Article 32 of Resolution No. 142-06)
DIGITO response time	Twenty (20) calendar days from submission (Article 37.1 of Resolution No. 142-06)
Form of response	Written notification to the complainant
Channels	E-mail to soporte@digito.do and other channels published in DIGITO's repository
Cost	Free of charge. Not subject to prior payment

Complainants are entitled to be informed at any time of the progress and status of their complaint, and to obtain copies of the documents in the case file.

DIGITO's decisions on complaints may be challenged by means of an Appeal (Recurso de Queja) before the Executive Directorate of INDOTEL within twenty (20) calendar days of notification of the decision or, if no response has been received, of the expiry of the time limit for issuing it (Articles 38 and 39 of Resolution No. 142-06), without prejudice to the right to bring the matter before the competent courts.

The Support Center is governed by Article 19 of Resolution No. 142-06 of the INDOTEL Board of Directors, as amended by Article 55.3 of Resolution No. 067-2025.

9. Applicable law and jurisdiction

The services provided by **DIGITO** are governed by the law of the Dominican Republic, and in particular by:

- Law No. 126-02 on Electronic Commerce, Documents and Digital Signatures, and its Implementing Regulation (Decree No. 335-03).

- Resolution No. 067-2025 of the INDOTEL Board of Directors, on Electronic Trust Services.
- Law No. 172-13 on the Protection of Personal Data.
- Resolution No. 142-06 on the Protection of Consumer and User Rights.

Disputes shall be submitted to the competent courts of the Dominican Republic, without prejudice to INDOTEL's supervisory powers.

References to ETSI technical standards and to IETF specifications are made for the technical purposes set out in Article 35 of Resolution No. 067-2025, and do not entail submission of **DIGITO** to the legal order of the European Union.

10. Authorisation, conformity assessment and audit

Aspect	Details
Supervisory authority	Instituto Dominicano de las Telecomunicaciones (INDOTEL)
Authorisation number	115-2025
Date of authorisation	3 November 2025
Conformity Assessment Body	INDOTEL
Reference standards	ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 and ETSI EN 319 421
Assessment scheme	ETSI EN 319 403, in accordance with Article 35 of Resolution No. 067-2025, by a Conformity Assessment Body accredited and recognised by INDOTEL
Assessment frequency	No more than twenty-four (24) months, and upon any substantial change or the addition of a new certificate type. Annual internal audit
Qualified signature creation device	Entrust nShield Connect XC, Common Criteria EAL4+ certified against Protection Profile EN 419 221-5 (certificate CSA_CC_21008, valid until 27/06/2027); signature activation module compliant with EN 419 241-2 (certificate CCN-CC-26/2025)

DIGITO publishes in its repository the current attestation of conformity, stating the issuing body, the scope of the assessment and its period of validity.

The Conformity Assessment Body is independent of **DIGITO**. **DIGITO** does not engage that body for consultancy services on the matters subject to assessment.

11. Personal data protection

The processing of personal data by **DIGITO** is governed by Law No. 172-13 on the Protection of Personal Data. **DIGITO** maintains a privacy policy, published in its repository which describes the data processed, the purposes, the retention periods and how to exercise data subject rights.

Information published in the certificate

The data included in the certificate is permanently and immutably embedded in every document signed by the subject, and is accessible to any third party verifying it. It comprises:

- For certificates of natural persons: given name, surname, e-mail address and identity document number, indicating the type of document and its issuing country.
- For certificates with institutional responsibility, additionally: legal name and identifier of the legal person, role of the subject, and institutional e-mail address.

This information remains accessible after the institutional affiliation ends, in respect of documents signed during the validity period of the certificate.

Information not published

The certificate does not include the subject's postal address or telephone number, the images, recordings and biometric data obtained during the identity verification process, copies of identity documents, or activation data. Such information is retained in the registration record with the applicable protection measures. For certificates with institutional responsibility, the documentation evidencing the organisation, the affiliation and the role, the Authorised Applicant's data and the content of the periodic attestations are not included either.

The subject gives express consent, which covers the processing of biometric data for identity verification and which, for certificates with institutional responsibility, cannot be given on the subject's behalf by the Affiliated Organisation or its Authorised Applicant. Identity proofing is performed on **DIGITO**'s behalf by an Identity Proofing Service Provider assessed against ETSI TS 119 461.

Subject rights

Subjects may exercise their rights of access, rectification, erasure, objection and restriction in accordance with Law No. 172-13, through the procedure published in **DIGITO**'s repository. The right of erasure does not extend to information whose retention is legally required under Section 7, nor to the content of certificates already issued.

DIGITO does not access subjects' private keys and has no mechanism enabling it to use them.

12. Refund policy

Fees are charged once the required verifications have been successfully completed and the certificate application has been approved.

DIGITO does not charge any fee for rejected applications, regardless of the reason for rejection.

DIGITO shall refund amounts paid where the certificate is not issued for reasons attributable to **DIGITO**, or where it must be revoked due to an issuance error attributable to **DIGITO**.

No refund shall be made where revocation is attributable to the subject or the Affiliated Organisation, or in the event of compromise or exposure of activation data as set out in Section 4.

Revocation, access to status information and access to the documents listed in this statement are free of charge. Refund complaints are handled in accordance with Section 8.

Applicable agreements and reference documents

Document	Identifier	Location
Certification Practice Statement	1.3.6.1.4.1.64999.6.1	https://cps.digito.do/
Certificate Policy for Natural Persons	1.3.6.1.4.1.64999.1.3.1	https://digito.do/politica-de-certificacion
Certificate Policy for Natural Persons with Institutional Responsibility	1.3.6.1.4.1.64999.1.3.4	https://digito.do/politica-de-certificacion
Terms and conditions of use	1.3.6.1.4.1.64999.6.3	https://digito.do/terminos-y-condiciones

Contract with the Affiliated Organisation (certificates with institutional responsibility)	—	Provided to the Affiliated Organisation before contracting
Privacy policy	—	https://digito.do/pol%C3%ADtica-de-privacidad

In the event of discrepancy between this document and the Certificate Policy or the Certification Practice Statement, the latter shall prevail and, between them, the applicable Certificate Policy. Changes that may affect acceptance of the service are notified at least thirty (30) calendar days in advance.

Version control

Version	Date	Description
1.0	10/12/2026	Initial version. Aligned with Certification Practice Statement v6.0, Certificate Policy for Natural Persons v7.0 and Certificate Policy for Natural Persons with Institutional Responsibility v1.0
1.1	10/27/2026	Signed document availability period differentiated by certificate class (Section 3). Status service continuity rate in accordance with Article 48(c) of Resolution No. 067-2025 and scheduled maintenance notice (Section 5). Grounds for revocation of certificates with institutional responsibility (Section 4) and correction of errata (registered address, RNC and date of authorisation). Aligned with Certification Practice Statement v6.1, Certificate Policy for Natural Persons v7.1 and Certificate Policy for Natural Persons with Institutional Responsibility v1.1.

Las firmas electrónicas a continuación cuentan con el respaldo de Digito Group, Entidad de Certificación y Proveedora de Servicios Electrónicos de Confianza autorizada por el INDOTEL mediante la Resolución Núm. 115-2025.

Esta lista solo incluye las firmas realizadas con Digito. Este documento puede contener firmas realizadas por otros medios o proveedores.

Documento firmado por 3/3 personas

Gregori Alejandro Polanco Capellan

Firma electrónica cualificada

Digito Group - Autoridad de certificación

Fecha de firma
27 de Octubre, 2026

Hora
13:15:42 GMT-4



Imagen de firma

Emily Altagracia Perez Trinidad

Firma electrónica cualificada

Digito Group - Autoridad de certificación

Fecha de firma
27 de Octubre, 2026

Hora
13:18:59 GMT-4



Imagen de firma

Gabriella Gisela Gomez Tolari

Firma electrónica cualificada

Digito Group - Autoridad de certificación

Fecha de firma
27 de Octubre, 2026

Hora
13:27:18 GMT-4

Imagen de firma

El documento ha sido protegido criptográficamente. Puedes verificar la integridad de sus firmas y contenido en el validador de Digito.

Escanea o visita
valida.digito.do