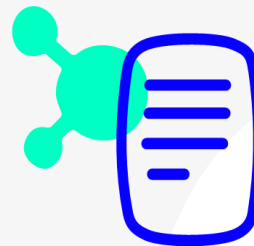


PKI Disclosure Text



Individual certificates

GENERAL INFORMATION

Type	PDS
Distribution	PUBLIC
Date	08/05/2023
Description	PKI Disclosure Text
Approved	CRS
Status	Published

CONTROL VERSION

VERSION	EXCHANGED PARTS	DESCRIPTION EXCHANGE	AUTHOR	DATE
1.0	All	Initial version	ASTREA	11/12/2017
1.1	1.1	Change of company name	DG	31/07/2018
1.2	1.1	Minor changes in denomination types of certificates	ASTREA	2/4/2019
	1.1	Inclusion of new types		
	1.1.14	Regulatory review		
	1.1.15	Inclusion of qualified services ReIDAS		
1.3	1.1.1	Change of address	DG	02/04/2019
1.4	All	Change of staff	ASTREA	27/02/2020
	1.1.1	Change of company name		
	1.1.4.2; 1.1.10.2	Change web domain .es to .com		
	1.1.2	Change of name certificates		
		Adaptation to Spanish Law 6/2020		21/04/2021
1.5		Deletion of certificates	ASTREA	08/05/2023

Index

1 Disclosure texts	4
1.1 Individual Certificates	4
1.1.1 Contact information	4
1.1.2 Types and certificate purposes	5
1.1.3 Issuing Certification Body	6
1.1.4 Limits on the use of the certificate	6
1.1.5 Obligations of the subscribers	8
1.1.6 Obligations of the signatories	9
1.1.7 Obligations of verifiers	10
1.1.8 LOGALTY's obligations	13
1.1.9 Limited warranties and disclaimer of warranties	15
1.1.10 Applicable agreements and CPS	16
1.1.11 Rules of trust for long-lasting firms	17
1.1.12 Privacy policy	17
1.1.13 Privacy Policy	18
1.1.14 Refund policy	18
1.1.15 Applicable law and competent jurisdiction	18
1.1.16 Accreditations and quality seals	19
1.1.17 Link to the list of providers	19
1.1.18 Severability of clauses, survival, full agreement and notification	19

1 Disclosure texts

a 1.1 Individual Certificates

This document contains the essential information to know about the certification service of the LOGALTY Certification Entity.

1.1.1 Contact information

- **Responsible organization**

The LOGALTY Certification Entity, hereinafter referred to as "LOGALTY", is an initiative of:

LOGALTY PRUEBA POR INTERPOSICIÓN SL

Calle Valportillo Primera, 22-24, Planta 1. Ed. Caoba.

28108 Alcobendas, Madrid (Spain)

PHONE: +34 915 145 800

FAX: +34 917 913 085

EMAIL: INFO.CA@LOGALTY.COM

1

If you have any questions, please contact:

LOGALTY PRUEBA POR INTERPOSICIÓN SL

Calle Valportillo Primera, 22-24, Planta 1. Ed. Caoba.

28108 Alcobendas, Madrid (Spain)

PHONE: +34 915 145 800

FAX: +34 917 913 085

EMAIL: INFO.CA@LOGALTY.COM

2

If you have any questions, please contact:

LOGALTY PRUEBA POR INTERPOSICIÓN SL

(LOGALTY TRUST SERVICES)

Calle Valportillo Primera, 22-24, Planta 1. Ed. Caoba.
28108 Alcobendas, Madrid (Spain)

EMAIL: revoke.ca@logalty.es

1.1.2 Types and certificate purposes

- **Natural Person HSM Cloud Qualified Certificate**

This certificate has the following OIDs:

In the Logalty certification hierarchy	1.3.6.1.4.1.30210.1.2.3
In accordance with the policy QCP-n	0.4.0.194112.1.0

These certificates are qualified certificates in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical regulation identified with the reference ETSI EN 319 411-2.

These certificates work with a qualified signature creation device, according to Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates are managed centrally.

These certificates guarantee the identity of the signatory and their link with the certification service subscriber, and allow the generation of the "**qualified electronic signature**", that is, the qualified electronic signature that is based on a qualified certificate and that has been generated using a qualified device, for which, in accordance with the provisions of Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, shall have a legal effect equivalent to a handwritten signature.

They can also be used in applications that do not require the electronic signature equivalent to a written signature, such as the applications listed below:

- a) Secure email signature.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents or data messages. In any case, LOGALTY shall not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows you to perform them:

- Digital signature (to perform the authentication function)
- Commitment to content (to perform the electronic signature function)

- b) The following statement appears in the "Qualified Certificate Statements" field:

- QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified
- QcSSCD (0.4.0.1862.1.4), as this certificate is used exclusively with a qualified signature creation device.

- c) The field "User Notice" describes the use of this certificate.

1.1.3 Issuing Certification Body

The certificates indicated are issued by LOGALTY, identified by the data indicated above.

1.1.4 Limits on the use of the certificate

- [Limits on use for subscribers](#)

The subscriber must use the certificate certification service provided by LOGALTY exclusively for the uses authorised in the contract signed between LOGALTY and the SUBSCRIBER, and which are reproduced below (section "obligations of the signatories").

Likewise, the subscriber undertakes to use the digital certification service in accordance with the instructions, manuals or procedures provided by LOGALTY.

The subscriber must comply with any laws and regulations that may affect its right to use the cryptographic tools it employs.

The subscriber may not take any measures to inspect, alter or reverse engineer LOGALTY's digital certification services, without prior express permission.

- **Use limits for verifiers**

The certificates are used for their own function and established purpose, without being able to be used for other functions and for other purposes.

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

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).

The certificates have not been designed, may not be used and are not authorised for use or resale as hazardous situation control equipment or for uses requiring fail-safe action, such as the operation of nuclear facilities, air navigation or communication systems, or weapons control systems, where failure could directly lead to death, personal injury or severe environmental damage.

The limits indicated in the various fields of the certificate profiles, visible on the LOGALTY website (<https://www.logalty.com/certificateauthority/>), must be taken into account.

The use of the digital certificates in operations that contravene this text of disclosure, or the contracts with the subscribers, is considered to be an improper use for the appropriate legal purposes, and

therefore LOGALTY is exempt, according to the legislation in force, from any responsibility for this improper use of the certificates by the signatory or any third party.

LOGALTY does not have access to the data on which the use of a certificate may be applied. Therefore, and as a consequence of this technical impossibility to access the content of the message, it is not possible for LOGALTY to make any assessment of such content. The subscriber, or the person responsible for the custody, assumes any responsibility arising from the content associated with the use of a certificate.

Likewise, the subscriber or the person responsible for the custody, will be responsible for any responsibility that could be derived from the use of the same outside the limits and conditions of use included in this text of disclosure, or in the contracts with the subscribers, as well as for any other improper use of the same derived from this section or that could be interpreted as such according to the legislation in force.

1.1.5 Obligations of the subscribers

- Key generation

The subscriber authorizes LOGALTY to generate the keys, private and public, for the identification and electronic signature of the signatories, and requests on his behalf the issuance of the certificate.

- Request for certificates

The subscriber undertakes to apply for the certificates in accordance with the procedure and, if necessary, the technical components supplied by LOGALTY, in accordance with the provisions of the Declaration of Certification Practice (DPC) and LOGALTY's operational documentation.

- Information obligations

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

The subscriber must immediately inform LOGALTY:

- Of any inaccuracies detected in the certificate once it has been issued.
- Of the changes that occur in the information provided and/or recorded for the issuance of the certificate.
- Of the loss, theft, subtraction, or any other loss of control of the private key by the signatory.
- Custody obligations

No policy requirement.

1.1.6 Obligations of the signatories

- Custody obligations

The signatory undertakes to safeguard the personal identification code or any technical support provided by LOGALTY, the private keys and, if necessary, the specifications owned by LOGALTY that are supplied to him, as well as the personal identification code (PIN) in safe custody.

In case of loss or theft of the certificate's private key, or in case the signatory suspects that the private key has lost its reliability for any reason, such circumstances must be immediately notified to LOGALTY by the subscriber.

- Obligations of correct use

The signatory must use the certificate certification service provided by LOGALTY, exclusively for the uses authorized in the CPS and in any other instruction, manual or procedure provided to the subscriber.

The subscriber must comply with any laws and regulations that may affect his right to use the cryptographic tools employed.

The subscriber may not take measures to inspect, alter or decompile the digital certification services provided.

The subscriber shall acknowledge:

- b) 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.
 - c) That it does not act as a certification body and, therefore, is obliged not to use the private keys corresponding to the public keys contained in the certificates for the purpose of signing any certificate.
 - d) That in case the private key is compromised, its use is immediately and permanently suspended.
- Prohibited transactions

The subscriber agrees not to use his private keys, certificates or any other technical support provided by LOGALTY in the performance of any transaction prohibited by applicable law.

The digital certification services provided by LOGALTY have not been designed nor do they allow their use or resale as equipment to control dangerous situations, or for uses that require error-proofing, 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.

1.1.7 Obligations of verifiers

- Informed decision

LOGALTY informs the verifier that it has access to sufficient information to make an informed decision when verifying a certificate and to rely on the information contained in the certificate.

In addition, the verifier shall acknowledge that the use of the LOGALTY Registry and Certificate Revocation Lists (hereinafter referred to as "CRLs" or "CRLs") is governed by the LOGALTY CPS and shall undertake to comply with the technical, operational and security requirements described in the said CPS.

- Requirements for the verification of electronic signatures

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

- It is necessary to use the appropriate software for the verification of a digital signature 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 electronic signature to be verified is based, since the electronic signature is verified using this chain of certificates.
- It is necessary to ensure that the chain of certificates identified is the most appropriate for the electronic signature being verified, since an electronic signature can be based on more than one chain of certificates, and it is up to the verifier to ensure that the most appropriate chain is used to verify it.
- It is necessary to check the revocation status of the certificates in the chain with the information supplied to the LOGALTY Registry (with LRCs, for example) to determine the validity of all the certificates in the chain of certificates, since an electronic signature can only be considered correctly verified if each and every one of the certificates in the chain is correct and in force.
- It is necessary to ensure that all the certificates in the chain authorize the use of the private key by the subscriber of the certificate and the signatory, since there is a possibility that some of the certificates may include usage limits that prevent the electronic signature being verified from being trusted. Each certificate in the chain has an indicator that refers to the applicable conditions of use, for review by the verifiers.
- It is necessary to technically verify the signature of all the certificates in the chain before relying on the certificate used by the signatory.

- Reliance on an unverified certificate

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

- Effect of verification

By virtue of the correct verification of the certificates, in accordance with this informative text, the verifier can rely on the identification and, where appropriate, public key of the signatory, within the corresponding limitations of use, to generate encrypted messages.

- Correct use and prohibited activities

The verifier agrees not to use any certificate status information or any other information provided by LOGALTY, in the performance of any transaction prohibited by the law applicable to such transaction.

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

In addition, the verifier undertakes not to intentionally compromise the safety of LOGALTY's public certification services.

The digital certification services provided by LOGALTY have not been designed nor do they allow the use or resale, as control equipment for dangerous situations or for uses that require error-proofing, such as the operation of nuclear facilities, air navigation or communication systems, air traffic control systems, or weapons control systems, where an error could cause death, physical damage or serious environmental damage.

- Indemnity clause

The third party who relies on the certificate undertakes to hold LOGALTY harmless from any damage arising from any action or omission resulting in liability, damage or loss, expense of any kind, including legal fees and representation incurred, by the publication and use of the certificate, when any of the following causes are present

- Failure to comply with the obligations of the third party relying on the certificate.
- Reckless confidence in a certificate, depending on the circumstances.
- Failure to check the status of a certificate, to determine that it is not suspended or revoked
- Failure to check all the insurance measures prescribed in the CPS or other applicable regulations.

LOGALTY shall not be liable under any circumstances for any loss of encrypted information that cannot be recovered.

LOGALTY will not be responsible for damages and losses caused in the terms indicated in article 11 of the Spanish Law *Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza*.

1.1.8 LOGALTY's obligations

- In relation to the provision of the digital certification service

LOGALTY undertakes to:

- a) 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 LOGALTY CPS.
- b) To carry out the services with the appropriate technical and material means, and with personnel who fulfil the conditions of qualification and experience established in the CPS.
- c) To comply with the quality levels of the service, in accordance with the provisions of the CPS, in the technical, operational and safety aspects.
- d) Notify the subscriber, prior to the expiry date of the certificates, of the possibility of renewing them, as well as the suspension, lifting of this suspension or revocation of the certificates, when these circumstances occur.

- e) Communicate to third parties who request it, the status of the certificates, in accordance with what is established in the CPS for the different certificate verification services.

- **In relation to the registry checks**

LOGALTY undertakes to issue certificates on the basis of the data supplied by the subscriber, and may therefore carry out any checks it deems appropriate regarding the identity and other personal and complementary information of the subscribers.

These verifications may include the documentary justification provided by the subscriber, and any other relevant document and information provided by the subscriber.

In the event that LOGALTY detects errors in the data to be included in the certificates or that justify these data, it may make the changes it considers necessary before issuing the certificate or suspend the issuing process and manage the corresponding incident with the subscriber. In the event that LOGALTY corrects the data without first managing the corresponding incident with the subscriber, it must notify the certified data to the subscriber.

LOGALTY 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.

- **Conservation periods**

LOGALTY archives the registers to the services provided in accordance with article 24.2 h) of Regulation (EU) N° 910/2014 of the European Parliament and of the Council of 23 July 2014, for at least 15 years from the expiration of the certificate or the completion of the service provided.

LOGALTY stores the information in the logs for a period of between 1 and 15 years, depending on the type of information recorded.

1.1.9 Limited warranties and disclaimer of warranties

- **LOGALTY guarantee for digital certification services**

LOGALTY guarantees the subscriber:

- That there are no factual errors in the information contained in the certificates, known or made by the Certification Body.
- That there are no errors of fact in the information contained in the certificates, due to a 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 CPS.
- That the revocation services and the use of the deposit comply with all the material requirements set out in the CPS.

LOGALTY guarantees the third party that it has confidence in the certificate:

- That the information contained or incorporated by reference in the certificate is correct, except where otherwise stated.
- In the case of certificates published in the repository, that the certificate has been issued to the subscriber identified therein and that the certificate has been accepted.
- That in approving the application for the certificate and in issuing the certificate all the material requirements established in the CPS have been fulfilled.
- Speed and security in the provision of services, especially revocation and deposit services.

In addition, LOGALTY guarantees the subscriber and the third party that it trusts the certificate:

- That the certificate contains the information that a qualified certificate must contain, in accordance with Annex I to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

- That, in the event that it generates the private keys of the subscriber its confidentiality is maintained during the process.
 - The responsibility of the Certification Body, with the limits established. Under no circumstances shall LOGALTY be liable for unforeseen circumstances or in cases of force majeure.
- **Exclusion of guarantee**

LOGALTY rejects any guarantee other than the above that is not legally enforceable.

Specifically, LOGALTY does not guarantee any software used by any person to sign, verify signatures, encrypt, decrypt, or otherwise use any digital certificate issued by LOGALTY, except where a written statement to the contrary exists.

1.1.10 Applicable agreements and CPS

- **Applicable agreements**

The agreements applicable to the certificates are as follows:

- Certification services contract, which regulates the relationship between LOGALTY and the certificate subscriber.
 - General conditions of service incorporated in the text of the certificate or PDS.
 - CPS, which regulate the issue and use of the certificates.
 - Certification policy (CP) for each of the certificates
- **CPS**

LOGALTY's certification services are technically and operationally regulated by LOGALTY's CPS, by its subsequent updates, as well as by complementary documentation.

The CPS and the transaction documentation are periodically amended in the Registry and can be consulted on the website: <https://www.logalty.com/certificateauthority/>

1.1.11 Rules of trust for long-lasting firms

LOGALTY informs certificate applicants that it does not offer a service that guarantees the reliability of the electronic signature of a document over time.

LOGALTY recommends, for the reliability of the electronic signature of a document over time, the use of the standards indicated in section II.7.3 (trust rules for long-lasting signatures) of the Application Guide for the Technical Standard for Interoperability "Policy on Electronic Signatures and Government Certificates".

The general considerations for long-lasting signature trust rules are set out in sub-section IV.3 of the NTI on electronic signatures.

1.1.12 Privacy policy

LOGALTY cannot disclose or be compelled to disclose any confidential information regarding certificates without a specific prior request from

a) The person in respect of whom LOGALTY has a duty to keep the information confidential, or

b) A judicial, administrative or any other order provided for in the legislation in force.

However, the subscriber accepts that certain information, personal and other, provided in the application for certificates, will be included in their certificates and in the mechanism for checking the status of the certificates, and that the information mentioned is not confidential, as required by law.

LOGALTY does not pass on the data provided specifically for the provision of the certification service to any person.

1.1.13 Privacy Policy

LOGALTY has a privacy policy in section 9.4 of the CPS, and specific privacy regulations regarding the registration process, the confidentiality of the registration, the protection of access to personal information, and the consent of the user.

The information referred to in section 1.1.8 is kept for the periods indicated, duly registered and with security and integrity guarantees.

1.1.14 Refund policy

LOGALTY will not refund the cost of the certification service under any circumstances.

1.1.15 Applicable law and competent jurisdiction

Relations with Logalty will be governed by the Spanish law on trustworthy services in force at any given time, as well as by civil and commercial legislation insofar as it is applicable.

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

In case of disagreement between the parties, the parties will try to reach an amicable resolution beforehand. To this end, the parties must send a communication to Logalty by any means that leaves a record to the contact address indicated under the point **1.1.1** of this PDS.

If the parties do not reach an agreement on this matter, either party may submit the dispute to civil jurisdiction, subject to the Courts of Logalty's registered office.

1.1.16 Accreditations and quality seals

LOGALTY is included in the list of trusted providers (TSL) in Spain

<https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx>

LOGALTY has "eIDAS-compliant" certification for the following services⁴:

- Service for issuing qualified electronic signature certificates
- Service for issuing qualified electronic certificates with electronic stamp
- Service for issuing qualified electronic certificates for website authentication
- Qualified electronic time stamp issuing service

LOGALTY has the following qualified extensions⁵ :

- ForeSignatures
- ForeSeals
- ForWebSiteAuthentication
- QCQSCDManagedOnBehalf

In accordance with EU Regulation 910/2014, LOGALTY will carry out compliance audits every 2 years.

1.1.17 Link to the list of providers

<http://www.minetur.gob.es/telecomunicaciones/eses/servicios/firmaelectronica/paginas/prestadores.aspx>

1.1.18 Severability of clauses, survival, full agreement and notification

The clauses in this disclosure text are independent of each other, which is why if any clause is considered invalid or inapplicable, the rest of the clauses in the PDS will continue to apply, unless the parties expressly agree otherwise.

The requirements contained in sections 9.6 (Obligations), 9.8 (Responsibility), 8 (Compliance Audit) and 9.3 (Confidentiality) of the LOGALTY Certification Practice Statement shall continue to apply after termination of service.

This text contains the complete will and all the agreements between the parties.

⁴ According to the website: <https://sedeaplicaciones.minetur.gob.es/Prestadores/Prestador.aspx>

⁵ According to the website: <https://webgate.ec.europa.eu/tl-browser/#/tl/ES/30/0>