Disclosure text - PDS (PKI Disclosure Statement) for Electronic Seal Certificate

Docuten

Index

1. Disclosure text applicable to electronic seal certificates

This document contains the essential information in connection with the certification service of the Trustworthy Electronic Service Provider of DOCUTEN.

1.1 Contact information

1.1.1. Responsible organisation

The Trustworthy Electronic Service Provider of DOCUTEN, from now on 'DOCUTEN', is the result of:

DOCUTEN TECH, S.L. RÚA GAMBRINUS, NÚMERO 7, 1ºA A CORUÑA 15008 TELEPHONE: +34 981 269 685 EMAIL: ATENCIONALCLIENTE@DOCUTEN.COM

1.1.2. Contact

For inquiries, please contact:

DOCUTEN TECH, S.L. Email: ATENCIONALCLIENTE@DOCUTEN.COM Telephone: +34 981 269 685

1.1.3. Trustworthy Electronic Services Provider issuer

The certificate described in this document is issued by UANATACA, as mentioned previously.

1.1.4. Revocation proceedings contact

For inquiries, please contact:

DOCUTEN TECH, S.L.

Email: ATENCIONALCLIENTE@DOCUTEN.COM
Telephone: +34 981 269 685

1.2. Types of Certificates

The following certificates have been issued by UANATACA. They are qualified according to Article 38 and with the Annex I of the Regulation (UE) 910/2014 of the European Parliament and Board, 23rd July of 2014 and have complied with the identified technical standards with the reference ETSI EN 319 411-2. UANATACA has assigned to each certificate an object identifier (OID), for its identification on the applications. They are as follow:

Number OID	Type of certificates
	Sello Electrónico
1.3.6.1.4.1.56098.1.5.1	Certificado cualificado de Sello Electrónico en HSM centralizado
1.3.6.1.4.1.56098.1.5.2	Certificado cualificado de Sello Electrónico en QSCD centralizado

1.3. Purpose of the certificates

1.3.1. Qualified certificate for Electronic Seal on HSM Centralised

This certificate has the OID 1.3.6.1.4.1.56098.1.5.It is a certificate issued in according with the certification statement QCP-l with the OID 0.4.0.194112.1.1. The electronic seal certificates are qualified certificates issued as stated in Article 38 of the Regulation (UE) 910/2014 eIDAS.

These certificates guarantee the identity of the subscribing entity, and where relevant, the representative of the organisation who is responsible for managing the seal

The information of uses in the certificate's profile indicates the following:

The "key usage" field is activated and therefore it allows us to perform the following functions:

a. Digital Signature, for authentication
b. Content commitment, for electronic signature
c. Key Encipherment

1.3.2. Qualified certificate for Electronic Seal on QSCD Centralised

This certificate has the OID 1.3.6.1.4.1.56098.1.5.2. It is a qualified certificate, which it is issued in accordance with the certification statement QCP-l-qscd with the OID 0.4.0.194112.1.3. The electronic seal certificates are qualified and issued as stated in Article 38 of the Regulation (EU) 910/2014 eIDAS.

The electronic seal certificates on centralized QSCD guarantee the identity of the organization included in the certificate.

These certificates guarantee the identity of the subscribing entity, and where relevant, the responsible person who manage the seal. The information of uses in the certificate's profile indicates the following:

The "key usage" field is activated and therefore it allows us to perform the following functions:

a. Digital Signature, for authentication
b. Content commitment, for electronic signature
c. Key Encipherment

1.4. Limits of use of the certificate

1.4.1. Limits of use targeted to the signers

The signer can use the certification service of electronic seal certificates provided by DOCUTEN, only for authorised uses in the contract signed between DOCUTEN and the SUBSCRIBER, which are reproduced later (section 'obligations of the signers').

Likewise, the signer binds to use the digital certification service in accordance with the instructions, manuals or procedures provided by DOCUTEN.

The signer must comply any law or regulation that may affect his right of use of the cryptographic tools used.

The signer cannot take actions of inspection, alteration or reverse engineering of the digital certification services of DOCUTEN, without prior express permission.

1.4.2. Limits of use targeted to the verifiers

Certificates are used for its own function and established purpose, without being able to be used in other functions and other purposes.

Similarly, certificates can only be used in accordance with the applicable law, specially taking into account the existing import and export restrictions at all times.

Certificates cannot be used to sign requests of public key certificates of any type, or Certificate Revocation List (CRL).

Certificates have not been designed, cannot be assigned and its use or resale as control equipment for dangerous situations is not authorised nor for uses that require fail- safe actions, such as operations of nuclear installation, navigation systems, air communications, or weapons control systems, where a failure could lead directly to death, personal injury or severe environmental damage.

There must be taken into account the limits indicated in the various fields of the certificates profiles, visible in the web of DOCUTEN (https://www.docuten.com).

The use of the digital certificates in operations that violate this Certification Practice Statement, the binding legal documents with each certificate, or the contracts with the Registration Authorities or their signers/subscribers, is considered to misuse the legal purposes, exempting therefore to DOCUTEN, according to the current legislation, of any liability for this misuse of the certificates made by the signer or any third party.

DOCUTEN does not have any access to the data on which the use of the certificate can be applied. Therefore, as a result of this technical impossibility to access to the content of the message, DOCUTEN can't issue any valuation about the mentioned content, being the subscriber, the signer or the person responsible of the custody, the one who will assume any responsibility arising from the content rigged to the use of a certificate.

Likewise, any responsibility that could result from the use of the custody out of the limits and conditions of use included in this Certification Practice Statement, the binding legal documents with each certificate, or the contracts or agreements with the registration authorities or with their subscribers, and any other misuse thereof derived from this section or may be interpreted as such according to the law, will be attributable to the subscriber, signer or the responsible of it.

1.5. Subscribers' obligations

1.5.1. Key generation

The subscriber authorises DOCUTEN to generate keys, private and public for the signers, and requests on behalf the issuance of certificates in accordance to the certification policies of DOCUTEN electronic signatures.

1.5.2. Certificates request

The subscriber is obliged to request the qualified certificates in accordance with the procedure and, if necessary, the technical components supplied by DOCUTEN, in accordance with what it is established in the certification practice statement (CPS) and DOCUTEN's operations documentation.

1.5.3. Reporting obligations

The subscriber is responsible for all information included in the application for the certificate is accurate, complete for the purpose of the certificate and updated at all times.

The subscriber must immediately inform DOCUTEN of:

- Any inaccuracies detected in the certificate once issued.
- The changes that occur in the information provided and/or registered to issue the certificate.
- The loss, theft, subtraction or any other type of control loss of the private key by the signer.

1.6. Signers' obligations

1.6.1. Custody obligations

The signer binds to custody the personal identification code or any other technical support delivered to DOCUTEN, the private keys and, if necessary, DOCUTEN properties specifications that are supplied.

In case of loss or theft of the certificate private key, or if the signer suspects that the private key has lost reliability for any reason, such circumstances must be notified immediately to DOCUTEN by the subscriber.

1.6.2. Obligations of proper use

The signer must use the electronic seal certificates certification service provided by DOCUTEN, only for authorized uses in the CPS and in any other instruction, manual or procedure supplied to the subscriber.

The signer must comply any law and regulation that may affect their right of use the cryptographic tools used.

The signer will not be able to adopt the inspection, alteration or decompiling measures of the digital certification services provided.

The signer will recognise that:

a. When using any certificate, and while the certificate has not expired or been suspended or has been revoked, the certificate will be accepted and will be operative.

b. It does not act as certification authority and, therefore, agrees not to use the corresponding private key to the public key contained in the certificate for the purpose of signing any certificate.
c. In case the private key is compromised, its use is immediately suspended and proceeds according to this document.

1.7. Verifiers obligations

1.7.1. Informed decision

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

In addition, the verifier will recognize that the use of the Registry and the Certificates Revocation Lists (hereinafter "the CRLs") of DOCUTEN are governed by the CPS of DOCUTEN and will compromise to comply the technical, operational and security requirements, described in the mentioned CPS.

1.7.2. Electronic signature verification requirements

The check is normally performed automatically by the software verifier and, in any case, according to 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 perform any other cryptographic operations, and establish the certificate chain based on electronic signatures to verify, since the electronic signature is verified using this certificate chain.
- It is necessary to ensure that the identified certificates chain is the most suitable for the electronic signature to verify, since an electronic signature may be based on more than one certificate chain, and it's up to the verifier make sure of the most appropriate chain for verification.
- It is necessary to check the revocation status of the certificates chain with the information provided to DOCUTEN Registry (with CRLs, for example) to determine the validity of all certificates in the certificate chain, since an electronic signature can only be considered properly verified if each and every certificate in the chain are correct and are in force.
- It is necessary to ensure that all certificates in the chain authorize the private key use by the certificate subscriber and the signer, since there is the possibility that any of the certificates include use limits that prevent rely on the electronic signature to verify. Each certificate in the chain has an indicator that refers to the conditions of applicable uses, to review by the verifiers.
- It is necessary to technically verify all certificates signature in the chain before relying on the certificate used by the signer.

1.7.3. Trusting a certificate not verified

If the verifier trusts a certificate not verified, he/she will assume all risks from that action.

1.7.4. Verification effect

Under proper verification of electronic seal certificates of natural person issued on QSCD, in accordance with this disclosure text, the verifier can rely on the identification and, where appropriate, on the signer's public key, within the limitations of appropriate use, to generate encrypted messages.

1.7.5. Proper use and prohibited activities

The verifier agrees not to use any certificates status information or any other type that has been supplied by DOCUTEN, in performing a prohibited transaction by the applicable law of that transaction.

The verifier agrees not to inspect, interfere or perform any reverse engineer of the technical implementation of certification public services of DOCUTEN without prior written consent.

In addition, the verifier binds not to intentionally compromise the security of certification public services of DOCUTEN.

Digital certification services provided by DOCUTEN haven't been designed and its use or resale as control equipment for dangerous situations is not authorized nor for uses that require fail-safe actions, such as the operation of nuclear installation, navigation systems, air communications, or weapons control systems, where a failure could lead directly to death, personal injury or severe environmental damage.

1.7.6. Indemnity clauses

The relying third party in the certificate agrees to indemnify DOCUTEN of any damage from any action or omission that results in liability, damage or loss, expenses of any kind, including court and legal representation that may be incurred by the publication and use of the certificate, when any of the following causes occurs:

- Breach of the obligations of the relying third party in the certificate.
- Reckless confidence in a certificate, along with the circumstances.
- Lack of checking of the certificate status, to determine that it is not suspended or revoked.
- Lack of checking of all security measures prescribed in the CPS or other applicable regulations.

1.8. DOCUTEN obligations

1.8.1. Regarding the digital certification services provision

DOCUTEN undertakes:

a. Issue, deliver, manage, suspend, revoke and renew certificates, according to the instructions provided by the subscriber, in the cases and for the reasons described in DOCUTEN CPS.
b. Perform the services with technical media and suitable materials, and with personnel that meet the qualification conditions and experience established in the CPS.
c. Comply the quality service levels, in accordance with what is established in the CPS, in the technical, operational and security aspects.
d. Notify the subscriber and the signer, prior the certificates expiration date, the possibility of renewal and suspension, lifting of this suspension or revocation of certificates, when such circumstances occur.
e. Communicate to third parties who request the status of certificates, according to what is established in the CPS for different certificate verification services.

1.8.2. Regarding the registry checks

DOCUTEN undertakes to issue certificates based on the data supplied by the subscriber, so can perform the checks it deems appropriate regarding the identity and other personal and supplementary information from subscribers and, where appropriate, of the signatories.

These checks may include the documentary justification provided by the signer by the subscriber and any other documents and relevant information provided by the subscriber and/or the signatory.

In case DOCUTEN detects errors in the data to be included in the certificates or justify these data, will be able to make the necessary changes before issuing the certificate or suspend the issuance process and manage with the subscriber the corresponding effect. In case DOCUTEN corrects the data without prior management of relevant incident with the subscriber, it must notify the data finally certified to the subscriber.

DOCUTEN reserves the right to not issue the certificate if considers that the documentary justification is insufficient for the correct identification and authentication of the subscriber and/or the signatory.

The foregoing obligations shall be suspended in cases where the subscriber is acting as Registration Authority and has the technical elements corresponding to the key generation, certificate issuance and recording devices of corporate signature.

1.8.3. Periods of retention

DOCUTEN holds the corresponding issuance and revocation certificates requests logs for at least 15 years.

DOCUTEN holds the logs information for a period of between 1 to 15 years, depending on the type of information recorded, according to its policies and procedures.

1.9. Limited guarantees and guarantees rejection

1.9.1. DOCUTEN guarantees by the digital certification services

DOCUTEN guarantees to the subscriber:

- That there are not factual errors in the information in the certificates, known or made by the Certification Authority.
- That there are not factual errors in the information in the certificates, due to lack of diligence due to the management of the certificate request or creation of it.
- That the certificates comply with the material requirements established in the Certification Practice Statement (CPS).
- That the revocation services and the use of the Deposit comply with all material requirements established in the Certification Practice Statement (CPS).

DOCUTEN guarantees the relying third party on the certificate:

- That the information contained or incorporated by reference in the certificate is accurate, except where indicated the opposite.
- In case of certificates published in the Deposit, the certificate has been issued to the subscriber identified in it and the certificate has been accepted.
- That in the approval of the certificate request and in the certificate issuance all the material required established in the Certification Practice Statement (CPS) has been accomplished.
- The rapidity and security in the certification services provision, especially in the revocation services and Deposit.

In addition, DOCUTEN guarantees to the subscriber and the relying third party in the certificate:

- That the qualified certificate has the information that a qualified certificate must have, in accordance with Article 38 of the Regulation (UE) 910/2014 eIDAS, in compliance with the certification statement ETSI EN 319 411-2.
- That, in case of private keys generated by the subscriber or, where appropriate, the natural person identified on the certificate, his confidentiality is preserved during the process

- The responsibility of the Certification Authority, with the limits established. DOCUTEN will not be responsible for fortuitous event or force majeure.

1.9.2. Guarantee exclusion

DOCUTEN rejects any other different guarantee to the previous that is not legally enforceable.

Specifically, DOCUTEN does not guarantee any software used by anyone to sign, verify signatures, encrypt, decrypt, or use any digital certificate in any other way issued by DOCUTEN, except in cases where a written declaration to the contrary exists.

1.10. Applicable agreements and CPS

1.10.1. Applicable agreements

Applicable agreements to the certificates are the followings:

- Certification services contract, which regulates the relation between DOCUTEN and the subscribing certificates Company.
- Service general terms incorporated in this document
- CPS regulates the certificates issuance and use.

1.10.2. Certification practice statement (CPS)

DOCUTEN certification services are technically an operationally regulated by the CPS of DOCUTEN, for its subsequent updates, as well as the additional documents.

The CPS and the operations documentation is changed periodically in the Registry and can be consulted on the website: https://www.docuten.com.

1.11. Rules of trust for long-term signatures

DOCUTEN informs the certificates' applicants that do not offer a service that guarantees the reliability of the electronic signature of a document over time.

1.12. Intimacy policy

DOCUTEN cannot disclose or may be required to disclose any confidential information regarding certificates without prior specific request coming from:

a. The person with respect to which DOCUTEN has a duty to keep information confidential, or

b. Judicial, administrative or any other order provided in the current legislation.

However, the subscriber accepts that certain information, personal and any other type, provided in the certificate request, is included on the certificates and in the certificates status checking mechanism, and that the above information is not confidential, by legal imperative.

DOCUTEN does not give the data provided specifically for the certification services provision to anyone.

1.13. Privacy policy

DOCUTEN has a privacy policy under Section 9.4 of the CPS, and a specific regulation of the privacy related to the registration process, registration confidentiality, personal data protection, and the user consent.

Likewise, it is contemplated that the supporting documentation for the request approval must be preserved and properly registered with guarantees of security and integrity for a period of 15 years from the certificate expiration, even in case of early loss of effect for revocation.

1.14. Refund policy

DOCUTEN will not reimburse the cost of certification service under any circumstance.

1.15. Applicable law and competent jurisdiction

DOCUTEN relations are governed by the Regulation (UE) 910/2014 eIDAS, by the Spanish law, and in particular by the legislation that complies with its policy.

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

1.16. Linking with the list of Qualified Providers of Trusted Electronic Services

https://sedeaplicaciones.minetur.gob.es/Prestadores/

1.17. Severability, survival, entire agreement and notification clauses

The clauses of this disclosure text are independent of each other, that's why, if any clause is held invalid or unenforceable, the remaining clauses of the PDS will still be applicable, except expressly agreed by the parties.

The requirements contained in sections 9.6.1 (Obligations and liability), 8 (audit of conformity) and 9.3 (Confidentiality) of the CPS of DOCUTEN shall continue in force after the service termination.

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

The parties mutually notify the facts by sending an email to the following addresses:

- atencionalcliente@docuten.com, by DOCUTEN
- Email, indicated by the subscriber in the contract with DOCUTEN.