PKI DISCLOSURE STATEMENT

(PDS)

CLAVE (QUALIFIED CERTIFICATES OF CENTRALISED SIGNATURE CITIZEN)

PKI DISCLOSURE STATEMENT (PDS)

TABLA DE CONTENIDOS

Pág.

1. PROVIDER'S CONTACT DATA

DATA	CONTENT
Name	Dirección General de la Policía (Ministerio del Interior)
E-mail address	certificados@dnielectronico.es
Postal Address	C/Miguel Ángel 5 MADRID (España)
Telephone number	+34913223400
Fax	+34913085774

2. TYPES OF CERTIFICATES, VALIDATION PROCEDURES AND USE CONDITIONS

2.1 TYPES OF CERTIFICATES

The service for issuing qualified electronic certificates for centralised citizen signatures.

- Qualified Centralized Signature Certificate
  - OID: 2.16.724.1.2.2.2.29
  - Key Usage: contentCommitment

2.2 VALIDATION CERTIFICATES

Validation Authority(ies)(VA) have as function to check the status of other certificates issued for Spanish and Foreign citizens ID cards, following the protocol *Online Certificate Status Protocol* (OCSP). It determines the current status of an electronic certificate upon a Third-Party request without requesting access to lists of certificates repudiated by the same. FNMT-RCM will provide end-user partitioned CRLs.

This consultation service must be provided as established by the Law 6/2020, of 11 November, Regulating Certain Aspects of Trusted Electronic Services and pursuant Article 24 of the 910/2014 EU Parliament and Council "Regulation on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC" (commonly referred as "eIDAS" Regulation).

The initial scenario of Validation Authorities (that fulfils the universality and redundancy targets) is the following:

- **"Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda" (Spanish Royal Mint, FNMT-RCM)**, that would provide universally its validation/authentication services to citizens, business and Public Administration Entities.

The agreements governing the relationship between the PSC (DGP) and the Validation Authorities are outside the scope of this document. However, the provisions of current legislation for Qualified Trust Service Providers will apply to entities that provide the validation service.

The revocation status information will be made available beyond the validity period of the certificate for the period of time established by the regulations in force.

In the case of commitment of the private key of a Certification Authority or the cessation of activity of the TSP, information on the revocation status shall be provided through the consultation methods/services enabled for this purpose in accordance with the CPS.

Online Validation Service implementing the protocol OCSP:

- WEB: http://ocspclave.policia.es/ocspclave/OcspResponder

The validation service is available on a non-stop basis 24 hours a day, 365 days a year.

2.3 USE CONDITIONS

2.3.1 Appropriate use of the certificates

The qualified centralized signature certificate issued to Spanish and foreign citizens by the Subordinate AC DGP CLAVE will have the following purpose:

- **Qualified Centralized Signature Certificate:** The purpose of this certificate is to allow the citizen to sign formalities or documents. This certificate is a qualified certificate under (EU) Regulation 910/2014.

  Regulation (EU) 910/2014 lies down that qualified certificates for electronic signature will need to fulfill the requirements provided for in Annex I (changes in eIDAs2 Regulation). Besides, the Commission, by means of enforcement measures, may establish reference numbers for the rules which are related to qualified certificates for electronic signature; thus, the fulfillment of the requirements laid down in this Annex will be presumed when a qualified certificate for electronic signature is in compliance with such rules.

The signature certificates are qualified certificates pursuant to the provisions of article 28 and of Annex I of European Parliament and Council's (EU) Regulation 910/2014, of 23 July 2014, on the electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (changes in eIDAs2 Regulation), and to the complementing articles in Law 6/2020, of 11 November, Regulating Certain Aspects of Trusted Electronic Services.

Besides, this certificate takes into account the requirements of the QCP-n-qscd policy, as is laid down in the EN 319 411-2 European rule.

The use of the qualified centralized signature certificate brings the following guarantees:

- Non-repudiation of origin

  It ensures that the document originated from the citizen from whom it allegedly originated. This feature is obtained by means of the electronic signature made by the use of the qualified centralized signature certificate**.** The recipient of an electronically signed message can verify the certificate used for such signature through the use of any of the Qualified Providers of Validation Services for Qualified Centralized Signature Certificates. In this way, it guarantees that the document comes from a specific citizen.

  Given the fact that in the system for qualified centralized certificate signature it is guaranteed that the signature key remain, with a high degree of reliability, under the control of the holder citizen, his / her commitment with the signature made is guaranteed ("non-repudiation" guarantee).

- Integrity

  By the use of the Qualified Centralized Signature Certificate, it is possible to check that the document has not been modified by any agent which is external to the communication. In order to guarantee integrity, cryptography offers solutions which are based on special-characteristics functions, named summary functions that are used whenever an electronic signature is made. The use of this system makes possible to check that a signed message has not been altered between the sending and the reception. To this aim, with the private key, a single summary of the document is signed, such that any alteration of the message causes an alteration of its summary to happen.

2.3.2 Limitations and restrictions on certificates use

Certificates should be only used under the applicable laws, mainly taking into consideration import and export restrictions concerning the existing cryptography of their time.

The certificates issued by the FNMT-RCM (CERES) can be only used with electronic signing (nonrepudiation and commitment to the signed) purposes concerning in the case of the issuance of qualified centralized signature citizen certificates by the Subordinate AC DGP CLAVE.

Certificate profiles do not envisage the use of those certificates and their associated keys to encrypt any type of information.

Certificates cannot be used to act either as Register Authority or as Certification Authority, signing public key certificates of any type or Certificate Revocation Lists (CRL).

The use of the keys of the Certification Authorities is restricted to certificates signings, and CRLs and OCSP generation.

The qualified centralized signature certificate shall not be used to sign authentication messages (confirmation of identity) or secure access to computer systems (by establishing private and confidential channels with service providers).

The qualified trust services offered by the qualified centralized signature certificates have not been designed or authorized for use in high-risk activities or those requiring fail-safe operation, such as those relating to the operation of hospitals, nuclear facilities, air traffic control, railways, or any other activity where failure could result in death, personal injury, or serious damage to the environment.

On the other hand, it is guaranteed that the signature keys remain, with a high level of confidence, under the control of the citizen who holds the qualified centralized signature certificate. The holder must take the necessary care and measures to ensure the safekeeping of the access keys to the certificate, preventing their loss, disclosure, modification, or unauthorized use.

The testing certificates cannot be used outside of the testing scope.

3. OBLIGATIONS

3.1 AC OBLIGATIONS

The subordinate Certification Authority of qualified centralized signature certificates will act linking a certain public key to its holder by issuing a qualified centralized signature certificate, in accordance with Certification Practice Statement (CPS).

Services provided by the AC in the CPS context are those of issuing, renovating and revocation of personal qualified signature certificates and provision of the qualified electronic signature creation device.

The AC has the following obligations:

1º To carry out its operations under the CPS.

2º Publish the CPS on the web site referred to in the section 2.1 Repository.

3º To report changes of the CPS in accordance with section 10.12.2 Period notification mechanism.

4º To apply online a certificate and minimize the necessary time to issue that certificate.

5º To issue certificates in accordance with the known information at the moment of its issuing and error-free of data input.

6º To revoke certificates under Section 4.4 Certificates Suspension and Revocation and publish the revoked Certificates in the directory service and web site referred section 2.1 Repository, with the frequency laid down in dot 4.9.7 Issuance frequency of CRLs of the CPS.

7º In the event that the AC decides to proceed ex officio to revoke a certificate, this should be notified to the certificate users in accordance with the CPS.

8º Online update and publish the certificates data bases in force and revoked certificates.

9º Make available the certificates of the relevant Certification Authority/ies of the Directorate General of the Police (Ministry of Interior) to citizens.

10º To protect the private key of the Certification Authority/ies of the Directorate General of the Police (Ministry of Interior)

11º Keep registered all the information and documentation related to the qualified centralized signature certificates during at least fifteen years from the expiration of the certificate or the end of the service rendered.

12º Use reliable systems and products protected against any modification and that ensure technical and cryptographic safety of certification processes to which they support.

13º Neither store nor copy, by itself or through a third party, signature creation data of the person to whom services have been provided, except in case of management on behalf of the signatory. In this case, proper proceedings and technical and organizational mechanisms will be applied in order to ensure that

the signatory is thoroughly in charge of the control of the exclusive use of signature creation data.

Only the qualified trust services providers that issue qualified centralized signature certificate will be able to manage the electronic signature creation data on behalf of the signatory. To this effect, the signature creation data will be backed up as long as the safety level of the duplicated data is the same than the safety level of the original data and as long as the amount of duplicated data does not exceed the minimum required to ensure the service continuity. Signature creation data will not be duplicated for any other purpose.

14º Collaborate on auditing processes.

15º Operate according to the applicable rules.

16º The qualified trust service provider will count on an updated termination plan in order to ensure the continuity of the service, according to the provisions verified by the monitoring body according to Article 17, section 4, letter i) as it is specified in letter i) section 2 of the Article 24 of the 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 as it is specified in section 5.8.1 (changes in eIDAs2 Regulation).

17º In case the qualified trust service provider manages signature creation data on behalf of the signatory, the services provider must keep them and protect them against any modification, destruction or non-authorized access, as well as ensure their continuous availability for the signatory.

As well as all those included in the Article 24 of the Regulation (EU) Nº. 910/2014 of the European Parliament and of the Council of 23 July 2014 (changes in eIDAs2 Regulation) and the Law 6/2020, of 11 November, Regulating Certain Aspects of Trusted Electronic Services.

3.2 AR OBLIGATIONS

The Offices for Issuing Qualified Centralized Signature Certificates, in their role as RAs, must comply with the following obligations:

1º Carry out their operations according to the CPS.

2º Thoroughly check the identity of individuals.

3º Neither store nor copy the data for the creation of the signature of the certificates or without protection, being only available to the holders of the

qualified centralized signature certificates in accordance with the terms set forth in current legislation.

4º Manage the withdrawal requests as soon as possible.

5º Notify the citizen concerning the withdrawal of certificates if it is performed ex officio by the Directorate General of the Police (Ministry of Interior) or through request from the competent Authority according to the CPS.

6º Check that all the information included or incorporated through reference in the certificate is exact.

7º In accordance with current data protection regulations.

8º Provide citizens with the appropriate mechanisms at the issuing offices so that they can verify the accuracy of the data.

9º The obligations of the registration entities established in the current Resolution of the State Agency for Digital Administration, which establishes the conditions for acting as a face-to-face registration office of the CLAVE system, as well as in subsequent provisions that modify, develop or replace it.

3.3 OBLIGATIONS OF THE CITIZENS HOLDING THE CERTIFICATES

The holders of the issued certificates under the CPS must:

1. Provide the Register Authorities exact, complete and true information concerning the requested data for the register proceeding.
2. Know and accept the terms and conditions of the qualified trust service, in particular those included in the CPS that may be applied, as well as the amendments.
3. Keep and use correctly the keys that allow access to your private key.
4. Communicate to the Competent Authority, through the available mechanisms, any certificate malfunction.
5. Protect private keys, as well as access password and keep linked Certificates, taking any reasonable precaution to avoid loss, diffusion, modification or non-authorized use.
6. Accept use restrictions (section 1.4.2 of the CPS) imposed to passwords and certificated issued by the Directorate General of the Police (Ministry of Interior).
7. Immediately apply for the withdrawal of a certificate in case there is knowledge or suspicion of an awkward situation concerning the private key for the public key contained in the certificate, among other reasons due to: loss, theft,

potential awkward situation, knowledge of personal access password by third parties and detection of inaccurate information. The way to apply is specified at the section 4.9.3 of the CPS.

8. Do not reveal the keys that allow access to the private key.
9. Report immediately to the Competent Authority any situation that may affect the Certificate validity.
10. Ensure that all the information contained both in the Certificate is correct. Immediately notify if not.
11. Not to monitor, manipulate or carry out "reverse engineering" acts over the technical implementation (hardware and software) of the qualified trust services, without prior written permission by the Certification Authority.
12. Fulfill the obligations established for citizens holding the certificates in this document and in the Law 6/2020, of 11 November, Regulating Certain Aspects of Trusted Electronic Services as well as the Regulation (EU) Nº. 910/2014 of the European Parliament and of the Council of 23 July 2014 (changes in eIDAs2 Regulation).

3.4 OBLIGATIONS OF THE RELYING THIRD PARTIES

A. It is the obligation of third parties who accept and trust centralized signature certificates:

- Limit the reliability of the certificates to the uses allowed for them, according to the certificates' extensions and the CPS.
- Verify the validity of the certificates when performing any operation based on them checking that the certificate is valid and that it is not expired or has been cancelled.
- Assume responsibility concerning the correct verification of electronic signatures.
- Assume responsibility concerning validity check, cancellation of the trusted certificates.
- Know guarantees and liabilities linked to the acceptance of the trusted certificates and assume obligations.
- Notify any abnormal fact or situation related to the certificate and that may be considered as a reason to cancel it, with the means made available by the Directorate General of the Police (Ministry of Interior).

B. Services providers must verify the validity of signatures generated by the citizens through the Qualified Validation Services Providers network:

- In case the check is not performed, the Directorate General of the Police (Ministry of Interior) is not liable concerning the use and trust that service providers give to the certificates.
- If a Services Provider checks on line the state of qualified centralized signature Certificate, the transaction proof must be stored to keep the right to perform subsequent claims in case the state of the certificate at the very moment of checking does not match with its real situation.

C. Signature trust:

- The services provider must adopt the necessary measures to determine the signature reliability, building the whole certification chain and verifying the expiration date and the state of all the certificates in such chain.
- The services provider must know and be informed about the Certification Policies and Practices issued by the Directorate General of the Police (Ministry of Interior).
- If an operation that may be considered illicit is carried out, or in case of use not under the provisions of the CPS, the signature issued by the certificate must not be trusted.

D. In order to trust in the Certificates issued by the Directorate General of the Police (Ministry of Interior), the services provider must know and accept every restriction to which the above-mentioned Certificate is submitted.

4. LIABILITY

4.1 LIABILITY LIMITATIONS

The competent authorities with jurisdiction on the qualified centralized signature certificate will be liable in cases of non-fulfillment of the obligations under Law 6/2020, of 11 November, Regulating Certain Aspects of Trusted Electronic Services, in European Parliament's and Council's (EU) 910/2014 Regulation, of 23 July 2014 (changes in eIDAs2 Regulation) at CPS.

In this connection, the qualified trust service provider will accept full third-party liability for the actions of those persons to whom they have delegated the execution of any of the functions which are required for the delivery of the qualified trust services.

4.2 CERTIFICATION-AUTHORITY LIABILITY

- The Competent authority will be liable for the damage caused to any citizen in conducting their activities, when they fail to fulfill their obligations under Law 6/2020, of 11 November, Regulating Certain Aspects of Trusted Electronic Services and the European Parliament and Council's (UE) 910/2014 Regulation, of 23 July 2014.
- The liability of the qualified trust service provider, which is set forth in the legislation, shall apply pursuant to the general rules on contractual or extra-contractual unlawfulness, as appropriate, although it will be for the qualified trust service provider to prove that he acted with the due professional diligence, and will be liable for the damage caused deliberately or by negligence to any natural or legal person, due to non-fulfillment of his / her obligations under Regulation 910/2014.
- Intent or negligence by the qualified trust service provider will be presumed except where the qualified trust service provider demonstrates that the damage referred to in article 13 of 910/2014 Regulation happened without intent or negligence on his / her part (changes in eIDAs2 Regulation).
- When the qualified trust service provider, duly informs citizens in advance, on the limitations for the use of the services which it delivers, and such limitations can be

acknowledged by a third party, the qualified trust service provider will not be liable for the damage caused by failing to fulfill the established limitations in the use of the services.

- Specifically, the Directorate General for the Police (Ministry of Interior), as qualified trust service provider, will be liable for the damage caused to the signatory or to bona fide third parties due to not including, or late inclusion, in the consultation service on the validity of the certificates, or on the certificates for expiry of the validity of the electronic certificate.
- The Directorate General for the Police (Ministry of Interior), as qualified trust service provider, will accept full third-party liability for the actions of the persons to whom they have delegated the execution of some of the functions which are needed for the delivery of the qualified trust services.
- The Directorate General for the Police (Ministry of Interior) will accept no liability for the damage arising from or in connection with the failure to comply with, or with the defective execution of, the citizens and / or service provider's obligations.
- The Directorate General for the Police (Ministry of Interior) will not be liable for the defective use of the Certificates or the passwords, nor will it be liable for any indirect damage which may arise from the use of the Certificate.
- The Directorate General for the Police (Ministry of Interior) will not be liable for the damage which may arise from those operations in which the limitations on the use of the Certificate have not been fulfilled.
- The Directorate General for the Police (Ministry of Interior) will accept no liability for the non-fulfillment or the delayed fulfillment of any of the obligations contained in the CPS, if such non-fulfillment or delay is the consequence of a force majeure event, unforeseeable circumstances, or, generally, any circumstance on which direct control cannot be exerted.
- The Directorate General for the Police (Ministry of Interior) will not be liable for the content of documents which have been electronically signed by citizens with the qualified centralized signature certificates.
- The Directorate General for the Police (Ministry of Interior) does not warrant the cryptographic algorithms, nor will it be liable for the damage caused by successful external attacks on the cryptographic algorithms used, if it exercised due diligence pursuant to the state-of-the-art technology, and acted according to the provisions of the CPS and the Law.

4.3 LIABILITY OF THE REGISTRATION AUTHORITY

The Registration Authority will be fully liable for the correct identification of citizens and for their data validation, with the same limitations as are established for the Certification Authority in the previous section.

4.4 CITIZEN LIABILITY

Citizens will be fully liable for, and will assume all risks arising from, the reliability and safety at work, of the IT equipment or of the means through which they make use of their certificate.

Likewise, citizens will be liable for the risks arising from the acceptance of a safe connection, without previous due verification of the certificate's validity exhibited by the service provider. The procedures for collating the security of the connection with such service provider must be facilitated to the citizen by such service provider.

4.5 ASSIGNMENT OF RESPONSIBILITIES

The General Directorate of the Police (Ministry of the Interior), with respect to the Certification Authorities that issue qualified centralized signature certificates, assumes no responsibility in case of loss or damage:

- Arising from the service they provide, in cases of war, natural disasters or any other fortuitous or force majeure event: disturbance of the public order, transport strike, power and / or telephone failure, computer virus, shortcomings in telecommunications or in the asymmetric key pair commitment, caused by an unforeseeable technological risk. Occurred during the period between the request for a certificate and its delivery to the user.
- Occurred during the period between the request for a certificate and its delivery to the user.
- Occurred during the period spanned between the revocation of a certificate and the moment when the next CRL is published.
- Caused by the failure to observe the limitations established by the certificates and by the CPS when using the certificates.
- Caused by undue or fraudulent use of the issued certificates or CRLs.
- Caused by the undue use of the information contained in the certificate.
- The AC will not be liable for the content of the electronically signed documents or any other information which is authenticated by means of an AC-issued certificate.

As well as those contemplated in the applicable regulations.

5. APPLICABLE AGREEMENTS AND CPS

The Certification Practice Statement (CPS), the terms and conditions of the qualified trust service, and the PKI disclosure statement (PDS) are published in the following URLs:

For the Certification Practice Statement (CPS):

- WEB: http://pki.policia.es/clave/publicaciones/dpc

For the terms and conditions of the qualified trust service

- WEB: http://pki.policia.es/clave/publicaciones/terminos

For the PKI disclosure statement (PDS)

- WEB: http://pki.policia.es/clave/publicaciones/pds

6. PRIVACY POLICY

In accordance with current data protection regulations.

Likewise, the destruction of an audit or registry file can only be effected under authorization of the System's Administrator, the Security Officer and the Administrator of Audits of qualified centralized signature certificates. Such destruction can be initiated underwritten recommendation of any of these three authorities or of the administrator of the audited service, if a period of 15 years of retention has expired.

Lastly, under article 24.2 h) of European Parliament and Council's (EU) Regulation Nº. 910/2014, of 23 July 2014, on the electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (changes in eIDAs2 Regulation), the Directorate General for the Police (Ministry of Interior) will register and will keep accessible, for an appropriate period of time, even after the activities of the qualified trust service provider have ceased to be delivered, all the relevant information which is related to the data issued and received by the qualified trust service provider, in order that they can be specifically used as evidence in legal proceedings, and in order to guarantee the continuity of the service. Such registration activity can be conducted by electronic means.

7. CLAIMS AND JURISDICTION

All claims which occur between the users and the qualified trust service provider will need to be communicated by the disputing party to the Policy-Approving Authority (PAA) of the

Directorate General for the Police (Ministry of Interior), with the aim of attempting for the parties themselves to settle the dispute.

Policy-Approving Authority (PAA) for the qualified centralized signature certificates.

DATA	CONTENT
Name	Working Group for the Public-Identity Certificate
E-mail address	certificados@dnielectrónico.es
Postal Address	C/Miguel Ángel 5 MADRID (España)
Telephone number	+34913223400
Fax	+34913085774

For the resolution of any conflicts which might arise with regard to the CPS, the parties, waiving any other privileges which might correspond to them, shall be subject to the Contentious-Administrative Jurisdiction.

8. APPLICABLE LEGISLATION

The operations and functioning of the qualified centralized signature certificates will be governed by the applicable regulations, more especially by the following:

- Regulation (EU) 2024/1183, of the European parliament and of the council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (hereinafter referred to as eIDAs2 Regulation).
- 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.
- Law 6/2020, of 11 November, Regulating Certain Aspects of Trusted Electronic Services.
- Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Law 48/78, of 28 December, regulating the fee for the issuance and renewal of the DNI.

- Royal Legislative Decree 1/1996, of 12 April, approving the Recast Text of the Intellectual-Property Law.
- Law 39/2015, of 1 October, on the Common Administrative procedure of the Public Administrations (entry into force: 2 October 2016).
- Law 9/2014, of 9 May, named as General Law on Telecommunications.
- ROYAL DECREE 1553/2005, of 13 December, which regulates the issuance of the national identity document and its electronic-signature certificates.
- Royal Decree 1586/2009, of 16 October, which amends Royal Decree 1553/2005, of 23 December, regulating the issuance of the National Identity document and its electronic-signature certificates.
- Royal Decree 869/2013, of 8 November, which amends royal Decree 1553/2005, of 23 December, which regulates the issuance of the National Identity document and its electronic-signature certificates.
- Royal Decree 311/2022, of 3 May, which regulates the National Security Scheme.
- Organic Law 3/2018, of 5 December, on the protection of personal data and guarantee of digital rights.
- PRE/1838/2014 Order, of 8 October, which provides for the publication of the Resolution of the Council of Ministers, of 19 September 2014, which approves Cl@ve, the common platform of the State's Public Administrative Sector for the identification, authentication and electronic signature by the use of concerted keys.
- Royal Decree 414/2015, of 29 May, modifying Royal Decree 1553/2005, of 23 December, which regulates the issuance of the National identity document and its electronic-signature certificates.
- Organic law 4/2000, of 11 January, on the rights and liberties of foreigners in Spain and on their social integration, Title 1, Chapter 1, Articles 3 and 4.
- Royal Decree 557/201, of 20 April, approving the Regulation of Organic law 4/2000, Title 13, Chapter I, Articles 205 and 206, Chapter 2, Articles 207-210 and Chapter 4, Articles 213 and 214.
- Royal Decree 240/2007, of 16 February, on the entry, free circulation and residence in Spain of citizens from the Member States of the European Union and from other States which are party to the Agreement on the European Economic Space.

- INT/1202/2011 Order, of 4 May, regulating the personal data files in the Ministry of Interior, specifically ANNEX I – "Secretary of State for Security, Directorate General for the Police, Spanish National Police, Point no. 3: Adexttra".
- Decision from 28 September 2015, made by the Directorate for Information Technologies and Communications, laying down the conditions for acting as an onsite registration office of the Cl@ve system. (It will be replaced by the current Resolution of the State Agency for Digital Administration, which establishes the conditions for acting as a face-to-face registration office of the CLAVE system).
- Law 40/2015, of 1 October, on the judicial regime of the Public Sector (entry into force: 2 October 2016).
- Organic law 4/2015, of 30 March, on the protection of public safety.
- Royal Decree-Law 14/2019, of 31 October, to adopt emergency measures on security grounds on matters of e-government, public hiring and telecommunications.
- Royal Decree 203/2021, of March 30, approving the Regulation of action and operation of the public sector by electronic means.
- Royal Decree 255/2025, of April 1, regulating the National Identity Document.
- Commission Implementing Regulation (EU) 2025/1567 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the management of remote qualified electronic signature creation devices and of remote qualified electronic seal creation devices as qualified trust services.
- Commission Implementing Regulation (EU) 2025/1943 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards for qualified certificates for electronic signatures and qualified certificates for electronic seals.

9. LICENCES, TRADEMARKS AND AUDITS

9.1 LICENCES

At present, the qualified trust service provider, the Directorate General for the Police, with fiscal number S2816015H, is published on the list of qualified trust services which can be accessed on https://sedediatid.mineco.gob.es/Prestadores/TSL/TSL.pdf

9.2 TRADEMARKS

Not stipulated.

9.3 AUDIT

With regard to qualified centralized signature certificates, audits will be carried out annually in accordance with EN 319 401, EN 319 411-2, and ETSI TS 119 431-1, always in compliance with Regulation 910/2014 (eIDAs) and its update Regulation 2024/1183 (eIDAs2). Specifically, the body responsible for managing the remote signature creation device must carry out annual audits to ensure compliance with the rules for remote electronic signatures, Articles 29 and 29bis of the eIDAs2 Regulation. The remote electronic signature creation device must be certified in compliance with Article 30 of the eIDAs2 Regulation.

On the other hand, the Audit Plan may contemplate the development of internal audits of the Registration Authorities in accordance with EN 319 411-1 and Regulation 910/2014 (amendments in the eIDAs2 Regulation).

Notwithstanding the foregoing, the Competent Authority shall carry out internal audits at its own discretion or at any time, due to a suspicion of non-compliance with any security measure or due to a compromise of keys.

Periodic controls shall also be established in relation to the protection of personal data.

Finally, the qualified trust service provider shall be audited at least every 24 months by a conformity assessment body as established in Regulation 910/2014 (amendments to Regulation eIDAs2).