PKI DISCLOSURE STATEMENT (PDS)

DNIE AND CENTRALIZED SIGNATURE

PKI DISCLOSURE STATEMENT (PDS)

TABLE OF CONTENTS

1. PROVIDER'S CONTACT DATA

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

2. TYPES OF CERTIFICATES, VALIDATION PROCEDURES AND USE CONDITIONS

2.1 TYPES OF CERTIFICATES

Issuance service of qualified electronic certificates for electronic signature (national E-ID cards (DNIe)) and centralized Citizens' signature certificates.

Signature Certificate (2.16.724.1.2.2.2.3)	Content Commitment[1]
Authentication Certificate (2.16.724.1.2.2.2.4)	Digital Signature
Centralized Signature Certificate (2.16.724.1.2.2.2.11)	Content Commitment

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.

This consultation service must be provided under the provisions of the 59/2003 Act on electronic signature Section 18 paragraph d: The same guarantees "the availability of a fast and reliable consultation service on the full validity of the of the certificates" 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:

- **"Ministerio de Hacienda y Función Pública" (Ministry of Finance and Public Function)**, shall use for validation answers (OCSP protocol) of national ID card (DNIe), the certificate for verification of Electronic Signature Service and digital identity of the platform @firma.

[1] Non-repudiation.

- **"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.

It is compulsory to verify revocations for each use of public identity certificates and electronic signature. The common procedure for checking certificate validity will be consultation to the Providers of Validation Services, who via OCSP protocol will inform about the certificate status.

On line Validation Service implementing the protocol OCSP:

WEB: http://ocsp.dnie.es

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

Public Identity Certificates and electronic signature of the National ID card (DNIe), issued by the National Police Directorate General (Ministry of the Interior) will have as aim:

- **Authentication Certificate:** To guarantee citizen's identity by electronic means when performing telematics transactions. The Authentication Certificate (Digital Signature) assures that the electronic communication is performed by the person he/she claims to be. The holder/bearer would be able, of proving his/her identity before anyone provided he/she is in possession of the identity certificate and the private key associated to the same.

  This certificate use is not authorized for operations requesting non-repudiation in origin, therefore the accepting third parties and service providers would not have guaranty of the National ID Card (DNIe) holder commitment with the signed content. Its main use will be for generating authentication messages (identity confirmation) and for safe access to computer systems by establishing private and confidential with services providers).

  Besides, the certificate can also be used as identification mean for making a record allowing the issuing of qualified certificates by private entities, without being necessary that the same have to make a great investment implementing and maintaining register infrastructure.

  On the other hand this certificate takes into account the requirements of the NCP+ Policy following the European guidelines identified in EN 319 411-1.

- **Signature Certificate:** The aim of this certificate is to allow citizens to sign procedures or documents. This qualified certificate according to (EU) Regulation 910/2014) allows the substitution of handwritten signature for the electronic one in citizens deals with third parties (Art. 25 of the (EU) Regulation 910/2014 of the European Parliament and of the Council dated 23rd July 2014 on electronic identification and trust services for electronic transaction in the internal market and repealing Directive 1999/93/EC).

  The Regulation (EU) 910/2014 establishes that qualified certificates for electronic signature, will meet the requirements laid down in Annex I. On the other hand, the Commission, by implementing acts, will be able of establishing reference number of regulations on qualified certificates for electronic signature where the fulfillment of the requirements established by the mentioned Annex will be taken

for granted whenever a qualified certificate for electronic signature meets those regulations.

Signature certificates are qualified certificates following the provisions of Art.28 and Annex I of the Regulation (EU) 910/2014 of The European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transaction in the internal market and repealing Directive 1999/93/EC as well as those article of the Act Nº 59/2003, dated 19 December on electronic signature) supplementing that.

On the other hand this certificate takes into account the requirements of the QCP-n-qscd Policy (QCP-n-qscd, Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD) following the European guidelines identified in EN 319 411-2.

They are qualified certificates used in a qualified electronic signature creation device, pursuant Article 29 and Annex II of (EU) Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transaction in the internal market and repealing Directive 1999/93/EC.

For these reason they guarantee the citizen's identity to whom is holder of the private key of identification and signature, and allow the generation of the "qualified electronic signature", that is , the advanced electronic signature based in a qualified certificate and that has been generated using a qualified electronic signature creation device, therefore, pursuant Article 25 of (EU) Regulation 910/2014 of The European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transaction in the internal market and repealing Directive 1999/93/EC, it will have legal effect to those of a handwritten signature, without further need of other additional requirements.

Due to our above description, this certificate could not be used for generating authentication messages (identity confirmation) or for safe access to computer systems (by establishing private and confidential private channels with the service providers).

As, technically, it is possible to dissociate the certificates contained in the electronic- national ID, the Royal Decree 869/2013, of 8th November, adds an amendment to the decree regulating the Spanish National Identity Document Nº (1553/2005), aiming at giving the chance to all the Spanish citizens of proving their identity by electronic instrument, preserving at the same time the capacity of electronic signature for those persons having legal capacity to this aim.

This Royal Decree rules that "in case of Spanish national under age, or not having full legal capacity, the national identify card will only have the utility of electronic identification and the same will be issued with the corresponding authentication certificate activated."

It is also ruled that "the electronic signature certificate activation will be on voluntary basis and its use will be made by personal and secret key that the holder of o the national identity document can input confidentially into the system."

The joint use of both certificates grants the following guarantees:

- Authenticity of origin:

  The Citizen, by means of his / her **Authentication Certificate**, may accredit his / her identity to any person, by proving the ownership of and access to the private key which is associated to the public one included in the certificate accrediting his / her identity. Both the private key and the certificate are stored in the National

Identity Document, which is equipped with a processor with cryptographic capabilities. This makes possible to guarantee that the citizen's private key (this is the basic aspect for the credibility of his / her identity) never leaves the physical supporting media of the National Identity Document. In this way, when the citizen needs to electronically accredit his / her identity, he / she must be in possession of his / her DNIe and of the personal password (PIN) for access to the certificate's private key.

- Non-repudiation of origin

  It ensures that the document originates from the citizen from whom it allegedly originates. This feature is obtained by means of the electronic signature made by means of the **Signature Certificate.** The recipient of an electronically-signed message can verify the certificate used for that signature by using any of the Providers of DNIe-Validation Services. In this way, it is guaranteed that the document comes from a specific citizen.

  Since the DNIe is a qualified electronic signature creation device, and given the fact that the signature key are held, from the moment they are created, 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 **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 the integrity, cryptography offers solutions which are based on functions of special characteristics, 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.

On another note, the centralized-signature certificate of the National Identity Document issued to Spanish and foreign citizens by the Directorate General for the Police (Ministry of interior) will have the following purpose:

- **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. 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, and to the complementing articles in Law 59/2003, of 19 December, on the electronic signature.

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

The use of the 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 **Signature Certificate.** The recipient of an electronically-signed message can verify the certificate used for such signature through the use of any of the Providers of Validation Services for the centralized-signature certificate. In this way, it guarantees that the document comes from a specific citizen.

  Given the fact that in the system for 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 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 la Directorate General of the Police (Ministry of Interior) can be only used with identification (identity proof) and electronic signing (non repudiation and commitment to the signed) purposes concerning the DNIe (National ID card).

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.

Likewise, the authentication certificate should not be used for signing formalities and documents where it is necessary to record the commitment of the signee to the signed content. Similarly, the signature certificate should not be used to sign authentication messages (proof of identity) and to secure access to computer systems (through establishment of private channels and confidential with the service providers).

The trusted services provided by the DNIe, have not been designed or authorized to be used in high risk activities or those requiring a fail-safe activity, as those related to the functioning of hospital, nuclear, air or train traffic control premises or any other where a failure could lead to death, injuries or serious damages to the environment

The DNIe is a qualified electronic signature creation device and as such, guarantees that the keys are held under the control of the citizen holder of the DNIe since the electronic signature is created and it is not possible its exportation and use from any other device. Holders should take care and make use of the necessary means to guarantee the custody of their card and the mechanisms of private keys activation, preventing its lost, dissemination, amendment or unauthorized use.

On the other hand, it is guaranteed that the signature keys remain, with a high trust level, under the control of the citizen holder of the centralized signature certificate. The holder should be cautious and ensure the necessary means to guarantee the custody of access keys to the certificate, avoiding its loss, dissemination, amendments or unauthorized use.

3. OBLIGATIONS

3.1 AC OBLIGATIONS

The subordinate Certification Authority of DNIe and centralized signature certificates will act linking a certain public key to its holder by issuing a qualified 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 National ID Document and centralized signature certificates during at least fifteen years.

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 trust services providers that issue qualified certificates 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, Directorate General of the Police (Ministry of Interior) 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.

17º In case the services 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 and the next Act that regulates certain aspects of the trust electronic services.

3.2 AR OBLIGATIONS

The National ID Document and centralized signature certificates Issuing Offices as AR must fulfill the following obligations:

1º Carry out their operations according to the CPS.

2º Thoroughly check the identity of individuals.

3º Notify the issuing of the pair of certificates to the citizen, for the National ID Document issuing. Neither store nor copy the data for the creation of the signature of the National ID Document certificates or without protection, being only available to the holders of the centralized signature certificates.

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 relation to Personal Data Protection, the section 11 of the CPS will be applied.

8º Set at the citizens' disposal, at National ID Document issuing offices, proper mechanisms to check data verification

9º The obligations of the registering entities established in the Decision of 28th September, 2015, from the Directorate of IT and Communications, establishing the conditions to act as on-site register office of Cl@ve system.

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 trust service, in particular those included in the CPS that may be applied, as well as the amendments.
3. Keep and use in a proper way the National ID Document as well as Certificates and passwords. The holder is obliged to keep it.
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. Not disclose the personal access password that enables to use the National ID document and centralized signature certificates.
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 and National ID Document 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 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 Article 23.1 of the Act 59/2003 of 19 December, on electronic signature as well as the Regulation (EU) Nº. 910/2014 of the European Parliament and of the Council of 23 July 2014 and the next Act that regulates certain aspects of the trust electronic services.

3.4 OBLIGATIONS OF THE RELYING THIRD PARTIES

A) It is mandatory for the third parties that accept and trust in the certificates issued for National ID documents and centralized signatures:

- 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 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 a National ID Document and 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 National Identity Document (DNIe) and the centralized signature certificate will be liable in cases of non fulfillment of the obligations under Law 59/2003, of 19 December, on the Electronic Signature and the development regulations, in European Parliament's and Council's (EU) 910/2014 Regulation, of 23 July 2014, and the forthcoming Law regulating specific aspects of trust electronic services at CPS.

In this connection, the 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 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 59/2003, of 19 December, of the Electronic signature, European Parliament and Council's (UE) 910/2014 Regulation, of 23 July 2014, and the forthcoming Law which regulates specific aspects of trust electronic services.
- The liability of the 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 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.
- When the Directorate General for the Police (Ministry of Interior), as 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 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 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 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 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 or of the information stored in the processor of the cryptographic card in the electronic National Identity Document.
- 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 DNIe and 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.

The electronic National Identity Document is a personal and non-transferable document issued by the Ministry of Interior, enjoying the protection which the law provides for with regard to public and official documents. The holder will be obliged to safeguard it, and will be responsible for ensuring its preservation.

4.5 ASSIGNMENT OF RESPONSIBILITIES

The Directorate General for the Police (Ministry of Interior) will accept no liability toward the DNIe and centralized signature Certification Authorities for loss or damage:

RESP.1	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.
RESP.2	Occurred during the period between the request for a certificate and its delivery to the user.
RESP.3	Occurred during the period spanned between the revocation of a certificate and the moment when the next CRL is published.
RESP.4	Caused by the failure to observe the limitations established by the certificates and by the CPS when using the certificates.
RESP.5	Caused by undue or fraudulent use of the issued certificates or CRLs.
RESP.6	Caused by the undue use of the information contained in the certificate.
RESP.7	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.

5. APPLICABLE AGREEMENTS AND CPS

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

For the Certification Practice Statement (CPS):

- WEB: http://www.dnie.es/dpc and http://pki.policia.es/dnie/publicaciones/dpc

For the terms and conditions of the trust service

- WEB: http://www.dnie.es/terminos and http://pki.policia.es/dnie/publicaciones/terminos

For the PKI disclosure statement (PDS)

- WEB: https://www.dnie.es/pds and https://pki.policia.es/dnie/publicaciones/pds

6. PRIVACY POLICY

Pursuant to the Spanish legislation on data protection, this aspect is contained in chapter 11 of the Certification Practice Statement, with a view to comply with such legislative provisions.

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 DNIe Audits and of 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, 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 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 Electronic DNIe and the centralized-signature certificates.

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 DNI's operations and functioning, and the operations and functioning of the centralized-signature certificates will be governed by the applicable regulations, more especially by the following:

- 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 59/2003, of 19 December, on the Electronic Signature (Consolidated text, latest modification on 2 October 2015).
- 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).
- Organic Law 15/1999, of 13 December, on the protection of Personal Data, and its implementing Regulation, which was approved by Royal Decree 1720/2007, of 21 December.
- 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, which, in its Final Provision no. 6, informs on the amendment of Law 59/2003, of 19 December, on the electronic signature.
- 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 3/2010, of 8 January, which regulates the National Security Scheme in the area of the Electronic Administration.
- Royal Decree 951/2015, of 23 October, amending royal Decree 3/2010, of 8 January, which regulates the National Security Scheme in the area of the Electronic administration.
- 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.
- Law 40/2015, of 1 October, on the judicial regime of the Public Sector (entry into force: 2 October 2016).

9. LICENSES, TRADEMARKS AND AUDITS

9.1 LICENSES

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

9.2 TRADEMARKS

Not stipulated.

9.3 AUDIT

An internal audit will be conducted on the DNIe (National Identity Card) and centralized-signature certificates, on an annual basis, pursuant to EN 319 411-2, under the Audit Plan of the Competent Authority. This guarantees the operational and functioning adequacy, under the stipulations which are contained in the Certificate Practice Statement.

Besides, the Audit Plan will consider the development of internal audits of the Registration authorities, pursuant to EN 319 411 – 1 and Regulation 910/2014.

Notwithstanding the above, the Competent Authority will conduct internal audits in its own discretion or at any time, based on suspicion of non-compliance of any of the security measures or the key commitment.

Periodic controls will also be established with regard to the protection of personal data.

Lastly, the qualified trust service provider will be audited, at least every 24 months, by a conformity assessment bodies pursuant to Regulation 910/2014.