PKI DISCLOSURE STATEMENT (PDS)

PROFESSIONAL ID-CARD, ELECTRONIC HEADQUARTERS AND ELECTRONIC SEAL

PKI DISCLOSURE STATEMENT (PDS)

TABLE OF CONTENTS

Page

1. PROVIDER'S CONTACT DATA

Name	Dirección General de la Policía (Ministerio del Interior)		
E-mail	carnetprofesional@policia.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 Professional-ID cards (public officials with and without pseudonym)).

CERTIFICATE	KEY USAGE	EXTENDED KEY USAGE
Signature Certificate (2.16.724.1.2.1.102.30, 2.16.724.1.2.1.102.50)	contentCommitment[1]	
Signature Certificate with Pseudonym (2.16.724.1.2.1.102.41, 2.16.724.1.2.1.102.51)	contentCommitment[2]	

Furthermore, Professional ID card includes the following types of certificates:

CERTIFICATE	KEY USAGE	EXTENDED KEY USAGE
Authentication Certificate (2.16.724.1.2.1.102.31, 2.16.724.1.2.1.102.52)	Digital Signature	Client Authentication Smart card log-on Any purpose Secure E- mail
Authentication Certificate with Pseudonym (2.16.724.1.2.1.102.60)	Digital Signature	Client Authentication Secure E- mail
Encipherment Certificate (2.16.724.1.2.1.102.32, 2.16.724.1.2.1.102.53)	Key Encipherment, Data Encipherment	Secure E-mail Any purpose Files Encryption

Issuance service of qualified electronic certificates for electronic seal.

CERTIFICATE	KEY USAGE	EXTENDED KEY USAGE
Seal certificate (Levels:	Digital Signature,	Email Protection:

[1] Non-repudiation

HIGH and MEDIUM) (2.16.724.1.2.1.102.36/37, 2.16.724.1.2.1.102.57/58)	Key Encipherment Content Commitment	Client Authentication:
Electronic Seal Certificate for entities external to DGP (2.16.724.1.2.1.102.61/62)	Digital Signature, Key Encipherment Content Commitment	Email Protection: Client Authentication:

Issuance service of qualified electronic certificates for website authentication (electronic headquarters)

CERTIFICATE	KEY USAGE	EXTENDED KEY USAGE
Headquarters Certificate (Levels HIGH and MEDIUM) (2.16.724.1.2.1.102.34/35, 2.16.724.1.2.1.102.55/56)	Digital Signature, Key Encipherment	Authentication TSL Web Server

2.2 PROCEDURES FOR VALIDATING CERTIFICATES

Validation Authority(ies)(VA) have as function to check the status of the certificates issued, by the CA (Certification Authorities) of the DGP (National Police Directorate General) following the protocol *Online Certificate Status Protocol* (OCSP). It determines the current status of a digital certificate upon an accepting Third Party 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 digital 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).

In the infrastructure of Public Key of National Police Directorate General it has been deployed a Validation Authority for the internal use of its own services. This Validation Authority fulfills the objectives of universality and redundancy.

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 this sense, revoked certificates that expire will be removed from the CRL, however, information on the status of the certificate will continue to be provided through the OCSP check, regardless of whether it is expired.
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.

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.

On the other hand the CA that issues the CRLs lists (Certificate Revocation Lists) will issue an indirect complete CRL that will include the identification of all non-expired revoked certificates issued by the Public Key Infrastructure of the DGP.

The validity period of this CRL will be established in 48 hours and will be updated after each revocation or every 23 hours (in this way it becomes guaranteed the availability of a new CRL before the arrival of the date set up in the "nextUpdate" field).

The ARL will be stored in a binary file named ARL.crl (http://www.policia.es/crls/ARL.crl and http://pki.policia.es/cnp/crls/ARL.crl).

The complete CRL will be stored in a binary file named CRL.crl (http://www.policia.es/crls/CRL.crl and http://pki.policia.es/cnp/crls/CRL.crl).

Likewise, the certificates of end entity include as distribution point of the CRL the URL http://www.policia.es/crls/CRL.crl or http://pki.policia.es/cnp/crls/CRL.crl.

2.3 USE CONDITIONS

2.3.1 Appropriate use of the certificates

The certificates issued by the National Police Directorate General will be used to fulfill its-own relevant legitimate functions and for the performance of the Directorate General serving staff duties. They will be issued as qualified certificates pursuant the regulations of Articles 28, 38, 45 and Annexes I, III, IV 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 transactions in the internal market as well as those complementary Articles of the Act 59/2003 of December 19th on electronic signature and there will be fulfilled the obligations set up by the above mentioned Acts and those of the specific enforced regulations in the framework of the State General Administration.

1. **Headquarters Certificates,** issued by the Police Directorate General to be used for the identification of electronic headquarters and for establishing electronic communications with them. On the other hand, the electronic Headquarters Certificates (level MEDIUM and HIGH) take into account the requirements of the policy QCP-W following the European guidelines identified in EN 319 411-2.

   Likewise, the National Police Directorate General is adhered to both the Guides of basic requirements for the issuance and management of trust certificates and Guide for the issuance and management of extended validation certificates, requirements established by the entity CA/Browser forum. In case of inconsistency between CPS and the guidelines, the latter will have priority.

2. **Seal Certificates,** issued by the Police Directorate General to be used for guaranteeing the identification and authentication of the fulfillment of the competences of the Body or Entity that has authority for the automatic administrative action. On the other hand, the Seal Certificate for Automatic Action takes into account the requirements of the policies QCP-l for MEDIUM level and QCP-l-qscd for HIGH level pursuant the European guidelines established in EN 319 411-2.

3. **Professional ID-Card certificates**, (certificates of public officials, with and without pseudonym) issued by the Police Directorate General they will be used for the performance of duties that correspond to the staff serving in the above named National Police Directorate General.

   - **Authentication Certificate:** where appropriate to guarantee public official identity by electronic means when performing telematic 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 professional ID Card 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).

   This certificate can be also used as identification tool for making a registration that allows the issuance of qualified certificates by private entities. In this way that private entities are not obliged to make a great investment in deploying and maintaining a registration infrastructure.

   Besides, this certificate has linked to identity (name, surname and DNI/NIE number) the professional job position of the holders, adding to the certificate the following additional information:

   - Professional category
   - Professional e-mail
   - Professional ID card number
   - Unique identifier of the holder in the Information Systems of the General Directorate of Police

     On the other hand the Authentication certificate of Professional ID card (Public Official with and without pseudonym) "HIGH Level" take 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 public official 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 public officials deals with third parties Article 25 of the (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).

  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 as well as those article of the Act Nº 59/2003, dated 19 December on electronic signature) supplementing that.

On the other hand this signature certificate of Professional ID-Card (Public Official with and without pseudonym) HIGH LEVEL takes into account the requirements of the policy QCP-n-qscd following the European guidelines identified in EN 319 411-2.

Due to the above mentioned issues, this certificate must not be used for generating authentication messages (identity confirmation) and for safe access to computer system (by setting private and confidential channels with service providers).

In this case, this certificate has linked to the identity (name, surname and DNI/NIE number).

- Professional Category.
- Professional ID Card Number.

- **Encipherment Certificate:** Allows safe information exchange, in such a way that, only, the certificate holder is able of gain access to that information.

Encipherment certificates can be used for providing the following security services:

- Encipherment of E-mails.
- Encipherment of files.
- Encipherment of transactions.

The use of Encipherment certificate will be restricted to the professional scope, and its personal use is strictly forbidden; the certificate holder has to be aware that the National Police Directorate General, records encrypted material linked with the Encipherment certificate for its recovery in case of emergency situations.

This certificate has linked to the identity (name, surname and DNI/ NIE number).

- Professional Category.
- Professional e-mail address.
- Professional ID Card Number.

4. **Seal certificates for entities external to the DGP,** issued by the Directorate General of the Police to bodies, organizations or public entities external to the DGP as well as private entities external to the DGP shall be used for the sole and exclusive purpose of dealing with the DGP in the performance of operations against its services and may not be used in any other external service by the entities holding the certificates. On the other hand, the Seal certificate for entities external to the DGP takes into account the requirements of the QCP-l policy as established in the European standard EN 319 411-2.

The joint use of the signature certificate provides the following guarantees:

- Authenticity of origin

The officer could, by means of his/her **Authentication Certificate,** where appropriate accredits his/her identity before anybody, by proving his possession and access to the private key linked to the public key which is included in the certificate crediting his/her identity. Both private key and certificate are stored into the professional card, which contains a processor with encryption capacities. This makes it possible to ensure that the private key of the holder (point in which is based the credibility of his/her identity) does not quit the professional card physical support. Thus, the holder, when he/she has to credit electronically his/her identity, must be in possession of his/her professional card and the Personal Identification Number (PIN) to the private key of the certificate.

- Non-repudiation of origin

It ensures that the document comes from the holder whom is stated that originated it. This feature is obtained by means of the electronic signature generated by using the **Signature Certificate.** The recipient of an electronically-signed message can verify the certificate used for such signature through the use of the validation service provided by the Directorate General of the Police. In this way, it guarantees that the document comes from a specific officer.

Due to the fact that the professional card (public officials, with and without pseudonym) - HIGH levels - make use of a qualified electronic signature creation device and that the signature keys are held since the moment of their creation under their holders control, it is guaranteed the commitment of officers with the signature made ("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 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, a unique summary of the document is signed, with a private key, in such a way that any alteration of the message causes an alteration of its summary to happen.

- Confidentiality

By using the **Encipherment Certificate**, it is guaranteed that only the addressee of a message is able to access the content of it.

The sender of the message, making use of the encipherment certificate of the recipient, is able to encipher the information contained in that message, in such a way that only the recipient in possession of the private key linked to the certificate, or authorized staff acting ex officio, is able to access the content of it. The key archiving and retrieval procedures are described in detail under Section 4.12 Custody and retrieval of keys" of Certification Practice Statement (CPS).

The service responsible for custody and access of encipherment certificates and linked private key is the so-called Key Archive and Retrieval Service described in Certification Practice Statement.

2.3.2 Limitations and restrictions on certificates use

The certificates issued by the Directorate General of the Police should be only used under the applicable laws, taking especially into consideration import and export restrictions on cryptography of their time.

Certificates cannot be used to act either as Registration Authority, to sign public key certificates of any type, or Certification Revocations Lists (CRL).

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

Headquarters and seal certificates will not be used for purposes other than those stated in this Certification Practice Statement.

The professional card certificates (public officials, with and without pseudonym) could be only used, where appropriate, to authentication (proof of identity), electronic signature (non repudiation and commitment to the contents signed) and confidentiality (encipherment).

As stated above, 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 Directorate General of the Police, 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 professional card (certificates of public officials, with and without pseudonym) is a qualified electronic signature creation device and as such, guarantees that the keys of signature and authentication are held under the control of the holder since the moment that electronic signature is created, and it is not possible its exportation and use from any other device.

Concerning the encipherment key, it is generated externally to the card, it is imported into it and additionally guarded by the Key Archive and Retrieval Service, in such a way that key could be retrieved if the holder or authorized person so require it.

The holder should be cautious and adopt the necessary means to secure the custody of his/her professional card (public officials, with and without pseudonym) as well as the mechanisms of private keys activation, preventing its lost, dissemination, amendment or unauthorized use.

3. OBLIGATIONS

3.1 AC OBLIGATIONS

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

Services provided by the AC in the CPS context are those of issuance, renovation, suspension and revocation of qualified certificates and provision, where appropriate, of the qualified electronic signature creation device.

The AC has the following obligations:

1º To carry out its operations under the CPS.

2º To 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 9.12.2 Terms and notification mechanism.

4º To apply online for 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 To 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 officers.

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

11º Keep registered all information and documentation related to all certificates issued by the Directorate General of the Police during fifteen years, at least.

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

13º Do not store in any case the data of creation of signature, private key, of the holders of certificates of the Professional Card, for the certificates of signature and authentication.

14º To collaborate on auditing processes.

15º To 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.

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 Offices of issuing certificates of the Directorate General of the Police as AR must fulfill the following obligations:

1º Carry out their operations according to the CPS.

2º Thoroughly check the identity of individuals.

3º Advise officers concerning the issuing of their certificates. Do not storage or copy data of signature creation.

4º Deal the request for revocation as soon as possible.

5º Notify to the official concerning revocation of certificates if this is performed ex officio by the Directorate General of the Police (Ministry of Interior) or upon request of the competent Authority according to the CPS.

6º Check that all included or incorporated information by reference in the certificate is accurate.

7º In relation to Personal Data Protection, the section 10 of the CPS will be applied.

3.3 OBLIGATIONS OF THE CERTIFICATE HOLDERS

The holders of the certificates which are issued under the CPS are obliged to:

1º Provide the Registration Authorities exact, complete and accurate information on the data which they may require for the performance of the registration process.

2º Know and accept the terms and conditions of the trust service, in particular those included in the CPS which that may be applied, as well as the modifications to such terms and conditions.

3º Report to the Directorate General for the Police, by means of the mechanisms which are deployed for that purpose, any malfunctioning of the certificates or their private keys.

4º Protect their private keys and guard the associated certificates, taking all reasonable precautions to avoid their loss, disclosure, alteration or non-authorised use.

5º Accept the restrictions of use which have been established in CPS for keys and certificates issued by the Directorate General for the Police.

6º Immediately request the revocation of a certificate whenever there is awareness or suspicion that a private key corresponding to the public key contained in the certificate is being compromised, among other reasons, due to: loss, theft, potential compromise, third parties knowing the access key, and detection of inaccuracies in the information. The way in which the request can be made is specified in section 4.9.3.

7º Not disclose the access key which allows for the use of the certificates of the Directorate General for the Police.

8º Immediately report the Directorate General for the Police about any situation which might impact the validity of the Certificate.

9º Make sure that all the information contained in the certificate is correct, immediately reporting it when that is not the case.

10º Not to monitor, manipulate or perform "inverse engineering" actions on the technical implementation (hardware and software) of the certification services, without the previous permission of the Reliable Authority.

11º Fulfill the obligations which are laid down for the subscriber in this document and in article 23.1 of Law 59/2003, of 19 December, on the 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) The third parties accepting and relying on the certificates issued by the Directorate General for the Police shall:

- Limit the reliability of the certificates to the uses which are permitted for them, pursuant to the terms of the certificate extensions and the CPS.
- Verify the validity of the certificates on performing any operation which is based on them, through checking that the certificate is valid and has not expired or been revoked.
- Accept their liability for the correct verification of the electronic signatures.
- Accept their liability for the checking of the validity or for the revocation of the certificates which they trust.
- Know the guarantees and responsibilities arising from their acceptance of the certificates which they trust, and accept their obligations.
- Notify any anomalous fact or situation which relates to the certificate, and which may be regarded as a reason for its revocation, by the use of the means which the DGP makes public on the https://sede.policia.gob.es and www.policia.es web pages.

B) Service providers shall verify the validity of the signatures which are generated by the certificates issued by the Directorate General for the Police, through the Validation Service of this General Directorate.

- Should this verification not be conducted, the Directorate General for the Police (Ministry of Interior) will not accept liability for the use and the reliability which the service providers grant to such certificates.
- Should the Service Provider consult the status of a certificate on line (be it related to the headquarters, the seal, the authentication, the signature or the encipherment), he / she shall store the transaction receipt in order to be entitled to file later claims if the status of the certificate at the time of the consultation does not match the real status.

C) Trust in the signatures:

- The service provider shall take the necessary steps to determine the reliability of the signature, by generating all of the certification chain and verifying the expiry and the status of all the certificates of that chain.
- The service provider must know and inquire about the Certification Policies and Practices issued by the Directorate General for the Police (Ministry of Interior).
- Whenever an operation being performed might be regarded as illegal, or in cases of utilization which is not in agreement with the provisions of the CPS, the signature issued by the certificate must not be trusted.

D) For the purpose of relying on the Certificates issued by the Directorate General for the Police (Ministry of Interior), the service provider must know and accept all the restrictions which apply to such Certificates.

4. LIABILITY

4.1 LIABILITY LIMITATIONS

The Certification Authority of the Directorate General for the Police 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 Directorate General for the Police will be liable for the damage caused to the signatory or to good-faith third parties, 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, as qualified reliable service provider, duly informs to officials 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, 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 or suspension of the validity of the electronic certificate.
- The Directorate General for the Police, 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 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 official's and / or service provider's obligations.
- The Directorate General for the Police will not be liable for the defective use of the certificates or the keys, nor will it be liable for any indirect damage which may arise from the use of the certificates.

- The Directorate General for the Police 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 will accept no liability for the non-fulfillment or the delayed fulfillment of any of the obligations contained in 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 will not be liable for the content of documents which have been electronically signed by officials with the signature certificate that is contained in the Professional Card.
- The Directorate General for the Police 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 CPS and of the Law.

4.3 Liability of the Registration Authority

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

4.4 Liability of the Certificate Holder

The certificate holder 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 he / she makes use of his / her certificate.

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

The Professional Card is a personal and non-transferable document issued by the Directorate General for the Police, 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 Certification Authority of the Directorate General for the Police will accept no liability for los 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 using the certificates beyond the limitations established by such

	certificates and the CPS.
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.policia.es/cps **and** http://pki.policia.es/cnp/publicaciones/cps

For the terms and conditions of the trust service

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

For the PKI disclosure statement (PDS)

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

6. PRIVACY POLICY

Pursuant to the Spanish legislation on data protection, this aspect is contained in chapter 10 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 authorisation of the System's Administrator, the Security Officer or the Administrator of Audits on Public-Key Infrastructure of the Directorate General for the Police. Such destruction can be initiated on the written 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 operations on 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 Public-Key Infrastructure of the Directorate General for the Police.

Name	Working Group for the Public-Key Infrastructure of the Directorate General for the Police		
E-mail address	carnetprofesional@policia.es		
Postal Address	C/Miguel Ángel 5 MADRID (España)		
Telephone number	+34913223400	**Fax**	+34913085774

8. APPLICABLE LEGISLATION

The operations and functioning of the Public-Key Infrastructure in the Directorate General for the Police, as well as the present Statement of Certification Practices and the Certification Policies which apply to each type of certificate, 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.
- 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 11/2007, of 22 June, on the Electronic Access of Citizens to Public Services.
- Royal Decree 1671/2009, of 6 November, partially developing Law 11/2007, of 22 June, on the electronic access of citizens to Public Services.
- Royal Decree 668/2015, of 17 July, modifying Royal Decree 1671/2009, of 6 November, partially developing Law 11/2007, of 22 June, on the electronic access of citizens to public services.
- Law 39/2015, of 1 October, on the Common Administrative Procedure of the Public Administrations (entry into force: 2 October 2016).
- Law 40/2015, of 1 October, on the Legal Regime of the Public Sector (entry into force: 2 October 2016).
- 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.
- Organic Law 15/1999, of 13 December, on the Protection of Personal Data.
- Royal Decree 1720/2007, of 21 December, approving the Regulation for the development of Organic Law 15/1999, of 13 December, on the protection of personal data.
- Royal Legislative Decree 1/1996, of 12 April, approving the recast text of the Intellectual Property Law.
- INT/761/2007 ORDER, of 20 March, approving the new professional-card model for the officials of the Spanish National Police, and other identification documents.

- The Organic Rules and other rules affecting the operations of the Directorate General for the Police.

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 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 audit will be conducted on the Public-Key Infrastructure System of the Directorate General for the Police, on an annual basis, pursuant to EN 319 411-2, under the Audit Plan of the Directorate General for the Police. This guarantees the operational and functioning adequacy, under the stipulations which are contained in the Certificate Practice Statement.

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

Notwithstanding the above, the Directorate General for the Police 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 due to keys being compromised.

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.