ANNEX

NOTIFICATION FORM FOR ELECTRONIC IDENTITY SCHEME UNDER ARTICLE 9(5) OF REGULATION (EU) No 910/2014

The kingdom of Spain hereby notifies the European Commission of an electronic identification scheme to be published in the list referred to in Article 9(3) of Regulation (EU) No 910/2014 and confirms the following:

— the information communicated in this notification is consistent with the information which has been communicated to the Cooperation Network in accordance with Article 7(g) of Regulation (EU) No 910/2014, and

— the electronic identification scheme can be used to access at least one service provided by a public sector body in **Spain**.

Date

[signed electronically]

MUÑOZ DE MORA, PABLO (FIRMA)

Firmado digitalmente por MUÑOZ DE MORA, PABLO (FIRMA)
Nombre de reconocimiento (DN): c=ES, serialNumber=01911197N, sn=MUÑOZ, givenName=PABLO, cn=MUÑOZ DE MORA, PABLO (FIRMA)
Fecha: 2018.02.14 08:35:53 +01'00'

1. **General information**

Title of scheme (if any)	Level(s) of assurance (low, substantial or high)
Documento Nacional de Identidad electrónico (DNIe)	**High**

Year of implementation of the scheme: 2006
Application of the scheme: natural persons

2. **Authority(ies) responsible for the scheme**

Name(s) of authority(ies)	Postal address(es)	E-mail address(es)	Telephone No
Ministry of Interior - Kingdom of Spain	**C/ Julián González Segador, s/n 28043 MADRID**	divisiondedocumentacion@policia.es	**(34) 915822814**

Web page of the Ministry of Interior: www.interior.gob.es
Web page of the Spanish electronic ID card: www.dnielectronico.es

3. **Information on relevant parties, entities and bodies (where there are multiple parties, entities or bodies, please list them all, in accordance with Article 3(2) and (3)**

3.1. **Entity which manages the registration process of the unique person identification data**

Name of entity which manages the registration process of the unique person identification data

DIRECCIÓN GENERAL DE LA POLICÍA – DIVISIÓN DE DOCUMENTACIÓN

Person identification data (art. 3.3 of Regulation 910/2014): a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established.

In this regard, the certificates of the electronic ID card link the identity of a natural person (name, surname and ID number) to a particular public key.

The personal data of the citizen included in the certificates are:
- Name and surname
- Number of Spanish ID card
- Public key linked to the citizen
- Date of birth, which can be used to check citizen adulthood, mandatory in order to sign certain documents or have access to certain services
- email address (optional)

Additional information about the Registration Authorities can be found in section 1.3.3 of the Certification Practice Statement and Policies (CPS) [6].

3.2. **Party issuing the electronic identification means**

Name of the party issuing the electronic identity means and indication of whether the party is referred to in Article 7(a)(i), (ii) or (iii) of Regulation (EU) No 910/2014

DIRECCIÓN GENERAL DE LA POLICÍA - DIVISIÓN DE DOCUMENTACIÓN

Article 7(a)(i) [X]	Article 7(a)(ii) [ ]	Article 7(a)(iii) [ ]

3.3. **Party operating the authentication procedure**

Name of party operating the authentication procedure

The authentication procedure of the electronic National Identity Document requires the intervention of two parties:

- the General Secretariat of Digital Administration in the Ministry of Finance and Public Function, who will be in charge of the node that guarantees the interoperability that is included in article 5 of the Commission Implementing Regulation (EU) 2015/1501.

- The General Directorate of the Police, which has the validation lists of the National Identity Document to which the node will connect to validate the identity of the Spanish citizen who identifies with the National Identity Document.

3.4. **Supervisory body**

Name of the supervisory body

There is a dual supervision: The electronic identity is controlled and checked by the Service Inspection which depends on the Secretary of State for Security (Ministry of Interior) as superior body for the issuing of certificates and which receives any complaint lodged or suggestion made by the citizen at the Issuing Offices for digital Certificates; with normative character, the Spanish Data Protection Agency performs checks and controls established by the organic Law 15/1999 dated December 13th 1999 regarding Data Protection, as well as the Ombudsman as the highest institution defending the rights of the citizen.

The regulatory body of the electronic signature and the trust services in Spain is the Information Society Services (Secretary of State for the Information Society and the Digital Agenda, Ministry of Energy, Tourism and the Digital Agenda).

4. **Description of the electronic identification scheme**

Document(s) may be enclosed for each of the following descriptions.

NOTE: As can be seen in the Certification Practice Statement and Policies (CPS) [6], the profile of the certificate of citizen of the electronic Spanish ID card (section 8.1) is considered to be in accordance with the requirements of the annex to the Commission Implementing Regulation (EU) 2015/1501.

(a) Briefly describe the scheme including the context within which it operates and its scope

On site identification of the citizen before the accredited civil servant presenting the necessary documents so that the register can be introduced in the public key infrastructure.

After performing such register, the authentication certificate and signature (the latter in case of adulthood) are issued, endorsed by the Directorate General of Police.

The issued certificates allow the use of the digital identity through electronic means.

The certificates of public identity and the electronic signature of the Spanish ID card (DNIe), issued by the Directorate General of Police (Ministry of Interior) have the following purpose:

- 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).

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.

NOTE: EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
(http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.01.01_60/en_31941102v020101p.pdf)

- 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 signatures shall meet the requirements laid down in Annex I. On the other hand, the Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic signature. Compliance with the requirements laid down in Annex I shall be presumed where a qualified certificate for electronic signature meets those standards.

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."

(b) Where applicable, list the additional attributes which may be provided for natural persons under the scheme if requested by a relying party

It is allowed to include the email at the request of the applicant, the mailing address of the certificate holder.

(c) Where applicable, list the additional attributes which may be provided for legal persons under the scheme if requested by a relying party

Not applicable.

4.1. **Applicable supervisory, liability and management regime**

4.1.1. **Applicable supervisory regime**

Describe the supervisory regime of the scheme with respect to the following:

(where applicable, information shall include the roles, responsibilities and powers of the supervising body referred to in point 3.4, and the entity to which it reports. If the supervising body does not report to the authority responsible for the scheme, full details of the entity to which it reports shall be provided)

(a) supervisory regime applicable to the party issuing the electronic identification means

There is a dual supervision: The electronic identity is controlled and checked by the Service Inspection which depends on the Secretary of State for Security (Ministry of Interior) as superior body for the issuing of certificates and which receives any complaint lodged or suggestion made by the citizen at the Issuing Offices for digital Certificates; with normative character, the Spanish Data Protection Agency performs checks and controls established by the organic Law 15/1999 dated December 13th 1999 regarding Data Protection, as well as the Ombudsman as the highest institution defending the rights of the citizen.

The regulatory body of the electronic signature and the trust services in Spain is the Information Society Services (Secretary of State for the Information Society and the Digital Agenda, Ministry of Energy, Tourism and the Digital Agenda).

(b) supervisory regime applicable to the party operating the authentication procedure

The supervision regime applicable to the General Secretariat of Digital Administration as operator of the node that guarantees the interoperability that is included in article 5 of the Commission Implementing Regulation (EU) 2015/1501 derives from the liability regime included in the applicable national legislation.

The regulatory body of the electronic signature and the trust services in Spain is the Information Society Services (Secretary of State for the Information Society and the Digital Agenda, Ministry of Energy, Tourism and the Digital Agenda).

NOTE: Please note that, if relevant, the information will include functions, responsibility and powers of the supervisory body in chapter 3.4 and its dependency. If the supervisory body does not depend on the authority responsible of the system, full details of the responsible body would be provided.

4.1.2. **Applicable liability regime**

Describe briefly the applicable national liability regime for the following scenarios:

(a) liability of the Member State under Article 11(1) of Regulation (EU) No 910/2014

According to Regulation 910/2014, the notifying Member State (the Kingdom of Spain) would be held responsible of the damages caused deliberately or by negligence to any natural or legal person in case of non-fulfillment of the obligations based on letter d) and f) of article 7 in a cross border transaction.

(b) liability of the party issuing the electronic identification means under Article 11(2) of Regulation (EU) No 910/2014

The issuing party of electronic identification jeans will be held responsible for the damages caused deliberately or by negligence to any natural or legal person in case of non-fulfillment of the obligations based on letter e) of article 7 in a cross border transaction.

For that matter, the Directorate General of Police assumes all responsibility against third parties for the any of the tasks delegated in order to provide trust service. (CPS point 10.8) [6] and (PDS point 4) [7] [8]

(c) liability of the party operating the authentication procedure under Article 11(3) of Regulation (EU) No 910/2014

According to Regulation 910/2014, the General Secretariat of Digital Administration of the Ministry of Finance and Public Function, as the party that performs the authentication procedure, will be liable for damages caused deliberately or by negligence to any natural or legal person in case of breach of its obligations based on letter f) of article 7 in a cross border transaction.

The liability regime is that corresponding to the applicable national legislation.

4.1.3. **Applicable management arrangements**

Describe the arrangements for suspending or revoking of either the entire identification scheme or authentication, or their compromised parts

NOTE: In chapter 5.8 CPS [6] reports the actions to be taken in case of cessation of AC or AR. In chapter 4.9 CPS [6] the revocation of certificates is reported.

The revocation is always final. The temporary suspension of the validity of the certificates is not contemplated.

The consequence of the revoking of the certificates will be the notification to third parties that the said certificate has been revoked, whenever the verification of the certificate is requested by one of the validation service providers.

In any case, the provider will inform the signatory of the revocation of the certificate before or simultaneously to its extinction providing reason, date and time the certificate will lose validity.

The Certificates of Public Identity and Electronic Signature can be revoked by:

- Citizen´s waiver of the system, except as regards the identity certificate.
- Robbery, loss, destruction or deterioration of the DNIe certificate supporting media.
- Citizen´s permanent incapacity or death.
- Change in the identity data.
- Serious inaccuracies in the data facilitated by the citizen for obtaining the DNIe and its certificates, as well as circumstances causing those data, which were originally included in the Certificate, not to match the reality.
- Citizen´s private keys being compromised, either because the factors of loss, robbery, theft, modification, dissemination or revealing of the personal access password (PIN) allowing for the activation of such private passwords, or because of any other circumstances, including accidental ones, indicating that a person other than the holder has made use of the private key.

- Compromise of the private key of the Certification Authority of the Directorate General of Police (Ministry of Interior) issuing the citizen certificate, due to any of the above mentioned reasons.
- Cessation of the activities of the trust service provider, unless, on the express consent of the signatory, the management of the electronic certificates issued be transferred to another trust service provider.
- Failure, by the Certification Authority, the officials in charge of the issuing, or the citizen, to comply with the obligations laid down in the CPS [6].
- Any other reason which might fairly lead to the belief that the trust service has been compromised to the extent that the reliability of the Digital Public Identity is under question.
- Statement affirming that the citizen is not enabled to sign.
- By judicial or administrative order in line with current legislation.
- Requested by the holder.
- All the other reasons which are indicated in the applicable regulations.

4.2. **Description of the scheme components**

Describe how the following elements of Commission Implementing Regulation (EU) 2015/1502 ([1]) have been met in order to reach a level of assurance of an electronic identification means under the scheme the Commission is being notified of:

(include any standards adopted)

4.2.1. **Enrolment**

(a) Application and registration

The Spanish DNI is a document which unequivocally identifies its holder; it has been in existence for over 70 years, and it is issued and managed by the Directorate General of Police. Holding the document is compulsory from the age of 14 for all Spanish citizens residing in the national territory for over 6 months. It is widely endorsed by Spanish citizens.

The document is fully regulated by the national legislation, more specifically through Royal Decree 1553/2005, of 23 December (modified by Royal Decree 869/2013 and Royal Decree 414/2015), regulating the issue of the National identity Document and its authentication certificates and electronic signature; under this piece of legislation, any citizen can obtain information on the regulations corresponding to Spanish citizens´ certification registry.

It is issued at any of the 400 offices which are in existence in the whole of the national territory; the physical presence of the requesting citizen is a "sine qua non" requirement, the purpose being the corroboration of the person´s identity before a public official. A single administrative act is needed for the issue.

At the moment when issuing the card takes place, and through prior knowledge of the terms and conditions [9] of the trust service provision, an information leaflet is also facilitated together with a sealed security envelope which contains the activation PIN (password), generated in the presence of the document´s holder, as is laid down in the Electronic Signature Act. At a later stage, this PIN can be modified by the user in the IT equipment for Updating which are located at the issuing offices, with full guarantee of security and confidentiality.

The information leaflet contains a summary of the content, rights and obligations laid down in the Certification Practice Statement and Policies (CPS)[1] [6], PKI Disclosure Statement (PDS) [7] [8] and its purpose, pursuant to 59/2003 Electronic Signature Act, of 19 December – article 18.b, and article 24.2.d) of Regulation (EU) 910/2014, of is the fulfilling of the obligation to provide the requester with the relevant information on the electronic certificates which will be issued in his/her name.

The Certificates of Public Identity and Electronic Signature, corresponding to the National Identity Document (DNIe), which are stored in the electronic DNI´s chip, for Spanish citizens, 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. 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

[1] https://www.dnielectronico.es

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.

In the above mentioned document sources there is a clear and understandable explanation of the Purpose and the General Aspects of the legislation regulating the National Identity Document, as well as the Electronic Signature, the CPS [6], the PDS [7] [8], the characteristics of the Certificates and their conditions of use, the terms and conditions [9], the obligations and liability of the subscriber, and those of the Directorate General of Police as Qualified Trust Service provider [1], the guarantees, the protection of personal data, the applicable legislation and the competent courts. It also facilitates document-consultation sources, and an email address and Citizen Service telephone number which citizens can use if they have doubts or questions.

With regard to the security levels (Assurance level), their fulfillment is guaranteed through:

Level HIGH

- **Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.** Such terms and conditions can be found in the statement of electronic DNI´s CPS [6], PKI Disclosure Statement [7] [8], as well as in the terms and conditions [9], published in https://www.dnielectronico.es. Besides, the delivery of the electronic national identity document and of the associated certificates is done personally to the holder. Before electronic national identity document is delivered, the citizen is instructed on how to obtain the CPS [6], terms and conditions [9] and the rest of the information referred to in article 18.b) of 59/2003 Act, of 19 December and article 24.2.d) of the Regulation (EU) 910/2014.

- **Ensure the applicant is aware of recommended security precautions related to the electronic identification means.** These can be found in the statement of electronic DNI´s CPS [6], published in https://www.dnielectronico.es (for example, in section 10.6.3. Obligations of citizens holding certificates (CPS) [6] or in the FAQ section of the electronic DNI´s web page).

- **Collect the relevant identity data required for identity proofing and verification.** In this respect, the electronic DNI certificates link the identity of a natural person (Name, Surname and National Identity Document´s number) to a specific public key, without including any kind of attributes. In order to guarantee the authenticity and non-repudiation, all this information will be electronically signed by the provider entrusted with issuing the certificates.

The personal data of the citizen, which are included in the certificates, are:

- Name and surname
- National Identity Document´s number
- Public key associated to that citizen
- Date of birth, which can be used to check citizen adulthood, mandatory in order to sign certain documents or have access to certain services.
- Email address (optional)

The necessary proof which the requester must facilitate for requesting the electronic means of identification is detailed in section 4.1.2. "Registration of the applications certificates" (CPS) [6].

(b) Identity proofing and verification (natural person)

The citizen's identification and authentication for the applications for Public Identity Certificates and electronic signature will follow a process which is integrated in the registry for the issue of the National Identity Document, pursuant to the procedures described in Royal Decree 1553/2005, regulating the issue.

Therefore, when it is a first registration, the citizen must appear at a DNI issuing office with the documents established by Royal Decree 1553/2005, and by the modifications introduced in Royal Decrees 1586/2009 and 869/2013, as well as by section 4.2 of CPS [6], being accompanied by the person who has parental authority or legal custody (or the person who has been empowered by the latter) in cases when the citizen is under 14 years of age, or he / she is a person with supplemented legal capacity.

In the special case of disabled persons who cannot travel to an Issuing Office, they can obtain their DNI and their Public Identity Certificates through a relative who will need to present an accrediting medical certificate at the Office, certifying the impossibility; a mobile team made up of experts from the corresponding documentation office will be sent to the citizen's home and will issue the certificate.

Once the validity period of the physical supporting media of the National Identity Document has expired a period established for each different case in article 6 of Royal Decree 1553/2005, it will be regarded as outdated and all the attributions and legal effects which are provided for in the legal system will become ineffective, the holder remaining obliged to renew the document. Such renewal will be materialized through the physical presence of the Document´s holder at the DNI issuing offices. It will also be compulsory to renew the National Identity Document if changes occur in the data included in it, in which case it will also be necessary to facilitate the documents accrediting such variation.

The loss, theft, destruction or deterioration of the National Identity Document will carry the holder´s obligation to report to the competent authorities and to immediately obtain a duplicate, which will be issued following the established procedure and requirements.

In all the above cases, the loss of validity of the National Identity Document will carry the loss of validity of the certificates which are integrated in it. Both the renewal of the National Identity Document and the issuing of duplicates will, in turn, involve the revocation of the valid certificates and the issuing of new electronic ones.

At any time, without the validity of the supporting means (card) being terminated, it will be possible to request the issue of new certificates, also keeping the same card which corresponds to the National Identity Document. For requesting a new certificate, the holder´s physical presence at an issuing office will also be necessary. The citizen, making use of the IT equipment for DNI Updating, located in such offices, and after an authentication done by means of the card and the biometric templates (fingerprints), which are captured during the card issuing process, may trigger an unsupervised process of his / her certificates´ renewal. If it were not possible to obtain the fingerprints of any of the fingers, the citizen must request the renewal at an issuing post, under the care of an official.

No procedures of electronic application for certificate renewal are implemented, the physical presence of the holder at an Issuing Office being necessary in all cases.

The identity documents are pre-customized, this is they can only be customized at the Documentation Office in which the issue has been foreseen, without the possibility of using any other Office or any other similar Equipment.

With regard to the security levels, their fulfillment is guaranteed in the following manner:

All Spanish citizens shall be entitled to the issue of a National Identity Document; it will be mandatory for persons above the age of fourteen who reside in Spain, and for those persons of the same age who reside abroad but move to Spain for a period of over six months.

Likewise, the electronic national identity document, as is provided for in Royal Decree 1553/2005 and in its amendment introduced by Royal Decree 869/2013, will make electronic identification possible for persons with full capacity to perform legal actions, which hold such document. It will also make possible for them to sign documents electronically, as is provided for in Law 59/2003, of 19 December, on the electronic signature.

Therefore, the electronic DNI is a proof of identity which is acknowledged by the Kingdom of Spain as the official electronic accreditation document corresponding to the personal identity of its holder and to the electronic signing of documents.

NOTE. The security level (Assurance level) applied is HIGH, although the requirements corresponding to SUBSTANCIAL and LOW levels must be fulfilled.

LOW level

- **The person can be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity.** In this respect, the necessary types of proof which must be facilitated by the requester in the application for an electronic means of identification are listed in section 4.1.2, “Registration of applications certificates” (CPS) [6].

- **The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid.** In this respect, in section 4.1.2. CPS [6] the type of proof requested is provided for. Its validation is based on the facilitation of official documents, such as birth certificates issued by civil registries, city council´s census registration notes, etc. Besides, the validity of the document is established at the moment of its presentation; therefore, it is checked and confirmed that it has not been revoked and that it has not become outdated.

- **It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same. In this respect, the data facilitated may be validated against the official registries of the Public Administrations.**

SUBSTANTIAL level

- **NOTE: The above described requirements for the LOW level are met, and the alternative option in section 1 of Commission Implementing Regulation (EU) 2015/1502 is chosen.**

- **The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity. In this respect, the requester is asked to appear at the office, where it is checked whether the he / she facilitates the proof of identity established in section 4.1.2 of the CPS [6].**

  And the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person. In this respect, the data incorporated in the electronic DNI are checked against official registries of the Public Administrations.

  And steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence. In this respect, the appearance of the requester is asked for, as is the facilitation of updated or effective proof of identity (for example, recent photographs of the requester´s face, in full color, or biometric proof of identity).

HIGH Level

- **NOTE: The above described requirements for the SUBSTANTIAL level are met, and the alternative in section 1, letter a) of Commission Implementing Regulation (EU) 2015/1502 is chosen.**

- **In addition to the substantial level, one of the alternatives indicated in letters a) to c) must be met: a) Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source. In this respect, the capturing of the fingerprints is done at the moment of issuing the electronic DNI, and those fingerprints are securely stored in the card´s chip. The verification of the fingerprints´ coincidence is done through the "Match on Card" algorithm, that is, the verification of the biometric data against the reference data is done within the card itself. Therefore, the biometric sensitive data are kept stored internally in the card, and their use is controlled by means of access control procedures.**

- **And the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source. Just as the requester is identified as owning the reclaimed identity, by means of the comparison of one or more of the person´s physical characteristics with an authentic source, he / she is required to appear and facilitate the updated or valid proof of identity (for example, recent photographs of the requester´s face, in full color, or biometric proof of identity such as his / her fingerprints).**

(c) Identity proofing and verification (legal person)

Not Applicable.

(d) Binding between the electronic identification means of natural and legal persons

Not Applicable.

4.2.2. **Electronic identification means management**

(a) Electronic identification means characteristics and design (including, where appropriate, information on security certification)

The electronic DNI 3.0 has the following technical characteristics:
- 400 KB of Flash memory (code + customization).
- 8 KB of RAM memory.
- Dual interface (with and without contacts).
- RSA Crypto library.

- Based on a CC EAL5 certified chip increased with ALC_ DVS.2 and AVA_VAN.5 fulfilling the protection profile: Security IC Platform Protection Profile, Version 1.0, 2007, BSI-CC-PP-0035-2007.

- Authentication electronic certificate.
- Electronic signature certificate.

Support the following cryptographic algorithms:
- **RSA:**
  - **Key length of up to 2048 bits in CRT format (see informative note of the CPS [6]).**
  - **RSA key generation according to PKCS#1 standard.**

- SHA-256 hash algorithm for certificate validation and authentication commands.
- DES and AES triple symmetrical encryption.

And it complies with the following international standards:
- ISO 7816 – Parts 1/ 2/ 3/ 4. Transmission protocol T=0.
- ISO 14443 – Parts 1/ 2/ 3/ 4. Transmission protocol T=CL.
- Internal file structure according to PKCS#15 standard.
- Authentication of information exchanged between both parts; incorporation of cryptographic MAC checksum according to ANSI X9.19 and DES.
- Session key establishment protocol based on the proposed scheme in ISO/IEC 9798 Part 3.
- Session key calculation according to ANSI X9.63.
- Establishment of safe channels based on EN 419212-1:2014
- Common Criteria EAL4+ increased with AVA_VAN.5 with strict fulfillment of the following protection profiles:

- **Protection profiles for secure signature creation device – Part 2: Device with key generation v2.0.1.**
- **Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application v1.0.1.**

The electronic DNI provides the following security features:
- Generation of signature creation data and related signature validation data.
- Export of signature validation data for their subsequent certification.
- Reception and store of certificate information.
- Management of life cycle.
- If it is in operational stage, creation of digital signatures, following these steps:

- **Selection of unique signature creation data in case of multiple instances.**
- **Reception of data to be signed.**
- **Authentication of signer.**
- **Application of the adequate cryptographic function in digital signature generation process.**

The electronic DNI uses two authentication factors for the authentication process, the possession of the card and the knowledge of the secret code or PIN that is delivered to the holder in a security sealed envelope when the document is issued or with the fingerprint, which is a biometric element inherent to the holder of the electronic DNI. Fingerprints are taken while issuing the electronic DNI and are stored in a safe way in the card chip. The verification of the fingerprints match is carried out through the "Match on Card" algorithm.

The electronic DNI is designed in a way that, with the authentication mechanisms above mentioned, the signer must authenticate through the PIN before signing the data. This document also provides the functionality to communicate with the electronic signature creation application through a safe channel (with or without contacts) in order to guarantee the integrity of the data to be signed.

Additionally, if the electronic DNI is going to be used through the non-contact interface (NFC), it is also necessary for the holder to show the CAN (Card Access Number) code, printed at the bottom right corner on the front of the card. It avoids wireless accesses without control.

The functionality of identity authentication is similar to the case of the electronic signature. This electronic DNI protects itself against duplication and manipulation, as well as against attackers with a high potential for attack.

Safe channels

As it has been mentioned, the electronic DNI uses safe channels for its communications. In order to establish a safe channel, first, there is an exchange of public keys of the card and terminal through certificates verified by both parties. Then, a mutual authentication protocol is carried out, with an exchange of seeds to derive a common seed which produces the encryption and authentication session keys.

Once the common seed establishment protocol has finished all the messages must be transmitted in a safe way.

If the established safe channel is severed by the reception of an APDU command that does not respect the safe message format or due to an error concerning the authentication or MAC information, the channel is disabled and the card security status is reset (session keys are erased and presented secrets are invalidated).

The safe channel can be established through both contact and non-contact interfaces.

This proceeding enables both parties (card and external application) to trust in each other through the mutual presentation of certificates and their verification. In the process it is also included the safe exchange of some session keys that are used to secure (encrypt) all the subsequent exchanged messages. It is based on the international standard [EN419212] and its main characteristics are the following:

- Key exchange authentication

This proceeding is connected with section 8.6 of the document [part of family EN419212] with the use of RSA keys of up to 2048 bits, and SHA-256 for the validation of certificates and authentication commands.

The aim of this authentication method is to protect the card privacy, not disclosing the identity before the channels is encrypted and before the previous authentication of the terminal. In order to achieve these goals, a previous step of keys exchange is used through a Diffie-Hellman mechanism.

This alternative is based on the card capacity to verify certificates signed by a root certification authority, possibly through other intermediate certification authorities, and on the check, through challenge-response protocols, to verify if the other party has the private key linked to the certificate.

When the establishment of a safe channel is successful, a new safety status is obtained in the dialogue with the card. Depending on the certificate used by the terminal it may be:

- Administrative safe channel. Associated to the “PRO” access condition and, therefore, it will enable the Administrator to have access to the resources required by this condition.
- User safe channel. It does not provide the fulfillment of any resource access condition, but it will enable the access to the functionalities of electronic signature and authentication.
- PIN safe channel. Used for the presentation of secret codes. Necessary as a previous step to the signature operation.

Messages securing

The electronic DNI can, after the establishment of a safe channel, secure the transmitted messages. Previous authentication of both terminal and card, through electronic certificates, is necessary in order to accomplish the establishment.

Once the channel is established, messages exchanged between document and terminal are encrypted and authenticated. This way, a peer-to-peer communication is guaranteed between the two channel original points. Safe channel may be required by the application or may be an access restriction imposed to some card resource.

As it has been mentioned above, the electronic DNI counts on protection through two safe channels: one to send data and another one to send the secret code. The establishment of the safe channel is carried out through mutual authentication using authentication certificates both for the terminal and for the card.

Component certificate

The electronic DNI also counts on an excellent protection against data duplication. Protection mechanisms are both physical and logical. From the physical point of view, chip hardware is protected thanks to the fulfillment of the safety requirements in the protection profile "Security IC Platform Protection Profile, Version 1.0, 2007, BSI-CC-PP-0035-2007". This fulfillment is attested through the certificate Common Criteria EAL5 increased with ALC_DVS.2 y AVA_VAN.5.

Concerning the logical protection mechanisms, the information stored in the chip counts on several access restrictions depending on the type of information. This involves, as it has been mentioned above, the use of different kinds of safe channels (administrator, user and pin). One of the used parameters in order to establish a safe channel is the component certificate. This certificate contains the chip serial number. The serial number identifies each chip with unambiguous result and it is registered directly in the hardware during the fabrication process, so it is impossible to clone as it is attested by the above mentioned EAL5 certificate.

On the other hand, files created in the process of customization and their contained information is protected by secret codes, biometrics or keys that limit or avoid the access.

The electronic DNI is designed for the holder to be protected in a reliable way against non-authorized use, due to the different authentication methods through which an external entity proves its identity, or the knowledge of some secret piece of data stored in the card.

The correct use of each of these methods enables to obtain safety conditions that are required for the access to the different resources.

- PIN user authentication

The electronic DNI counts on user verification (CHV – Card Holder Verification) for the access to certain files. This verification is carried out through the PIN safe channel, checking the code supplied by the external entity through the command designed for this goal. The piece of data is compared with the reference information stored in the PIN file. The PIN code must be at least 12 bytes long in order to avoid attacks.

The PIN code has its own attempt counter. It is decreased every time a wrong presentation is made, locking if the counter reaches zero. In order to unlock the PIN code it is necessary to present the unlocking code in a correct way. The unblocking operation is carried out through the user authentication with biometrics and the presentation of the "APP" key.

- PIN unlocking

- **Condition 1: Biometrics**

The electronic DNI uses the biometrics verification technology "Match on Card", that is, the verification of biometric data with the reference data is carried out inside the card itself. So, sensitive biometrics data always remain stored inside the card and their use is controlled through access control. This "Match on Card" characteristic establishes an important difference with "Match off Card" algorithms, with a card only used as a data support for external verification.

The user authentication through biometric techniques enables, with the "APP key", to unlock the CHV code and establish a new value. Biometrics is also necessary for the request or renewal of the signature and authentication certificates. Biometric authentication is carried out under an administrator safe channel.

Concerning the biometrics user authentication, the card DNIe-DSCF stores two fingerprints.

After failed attempts to present the fingerprint, the whole fingerprint presentation mechanism is locked.

- **Condition 2: APP key**

The goal of this authentication method is for the external entity to prove that it knows the name and value of a secret code. This code, called "APP key" is usually in a key holder card, but never clearly out of a safe device.

Each APP key has its own attempt counter. After a valid presentation, the corresponding reattempt counter is automatically set in its initial value (3 attempts). The attempt counter decreases every time a wrong presentation is carried out, locking if it reaches zero. If this code is locked, it is not possible to unlock it.

This APP key, together with the biometrics user authentication, enables to unlock the user CHV code. This operation is carried out in a safe way through the use of an administrator safe channel.

Concerning the security levels (Assurance level), they are fulfilled:

NOTE: The applied level is HIGH, even though the SUBSTANTIAL level requisites must be fulfilled.

SUBSTANTIAL level

- **The electronic identification means utilises at least two authentication factors from different categories. In this sense, the electronic DNI uses two authentication factors for the authentication process, the possession of the card and the knowledge of the secret code or PIN that is delivered to the holder in a security sealed envelope when the document is issued or with the fingerprint, which is a biometric element inherent to the holder of the electronic DNI.**

- **The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs. In this sense, the activation of the data related to the identification means is carried out through the secret code or PIN or through the fingerprint of the holder of the identification means.**

HIGH level

- **The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential. In this sense, the certification of the card with the identification means shows that the device is tamper-resistant. Several penetration tests have been made to establish that the card is protected against duplication and manipulation. In the same way, these tests confirm that it resists attacks with a high potential for attack.**

- **The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others. In this sense, the use of the electronic identification means involves the possession of the QSCD card (qualified electronic signature creation device) together with the secret code or PIN and/or personal fingerprint of the holder of the electronic identification means. On the other hand, it enables to activate the private key and, as it has mentioned above, the number of failed attempts is limited.**

  NOTE: The certificates of Identity and Electronic Signature are stored in a Qualified Electronic Signature Creation Device in accordance with Regulation (EU) 910/2014. (DNIe-DSCF / QSCD). See DNIe v2.0 [4] [5] and DNIe v3.0 [2] [3] in eIDAs Observatory (https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds).

(b) Issuance, delivery and activation

The issuance process is carried out in a sole administrative action with the compulsory personal presence of the holder, who is given a safety sealed envelope with the PIN inside, providing the possibility to use the certificates.

The activation of the certificates involves a proceeding to unblock the access conditions to a key and enables its use. For the electronic DNI the activation piece of data is the personal access key (PIN) and/or the fingerprints patterns (biometrics).

Concerning the security levels (Assurance level), their fulfillment is guaranteed: HIGH level

- **The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs. In this sense, the activation of the electronic identification means is carried out through the access personal key (PIN) and/or the**

fingerprints patterns (biometrics). On the other hand, when issuance takes place, a random PIN is generated and delivered to the user in a blind envelope.

(c) Suspension, revocation and reactivation

NOTE: In chapter 4.9 CPS [6] the revocation of certificates is reported.

The revocation of the electronic signature certificates takes place in the very moment of the communication or complaint of the citizen to the competent Authorities, providing the information to the Certification Authority and establishing the revocation.

The certificates issued by any DNI Subordinate Certification Authority start to be valid when they are issued.

The period of validity is submitted to a possible anticipated termination in case of certificate revocation.

The temporary suspension of the certificates validity is not considered.

Revocation is always definitive. Taken into account that certificates suspension is not considered, it is not possible to reactivate them.

The Certificates of Public Identity and Electronic Signature can be revoked by:

- Citizen´s waiver of the system, except as regards the identity certificate.
- Robbery, loss, destruction or deterioration of the DNIe certificate supporting media.
- Citizen´s permanent incapacity or death.
- Change in the identity data.
- Serious inaccuracies in the data facilitated by the citizen for obtaining the DNIe and its certificates, as well as circumstances causing those data, which were originally included in the Certificate, not to match the reality.
- Citizen´s private keys being compromised, either because the factors of loss, robbery, theft, modification, dissemination or revealing of the personal access password (PIN) allowing for the activation of such private passwords, or because of any other circumstances, including accidental ones, indicating that a person other than the holder has made use of the private key.
- Compromise of the private key of the Certification Authority of the Directorate General of Police (Ministry of Interior) issuing the citizen certificate, due to any of the above mentioned reasons.
- Cessation of the activities of the trust service provider, unless, on the express consent of the signatory, the management of the electronic certificates issued be transferred to another trust service provider.
- Failure, by the Certification Authority, the officials in charge of the issuing, or the citizen, to comply with the obligations laid down in the CPS [6].
- Any other reason which might fairly lead to the belief that the trust service has been compromised to the extent that the reliability of the Digital Public Identity is under question.
- Statement affirming that the citizen is not enabled to sign.
- By judicial or administrative order in line with current legislation.
- Requested by the holder.
- All the other reasons which are indicated in the applicable regulations.

Concerning the security levels (Assurance level), their fulfillment is guaranteed: HIGH level

- **It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner.** In this sense, revocation causes are exposed in section 4.9 CPS [6], suspension is not allowed. On the other hand, the citizen can request the revocation and it must take place with the physical attendance of the citizen in any issuance office.

- **The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation.** In this sense, revocation is personally carried out by the user with any DNI issuing work team. The citizen must sign the request through a qualified electronic certificate or handwritten signature. On the other hand, revocation takes place immediately after the management of each request verified as valid. The temporary suspension of the certificates validity is not considered.

- **Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met**. In this sense, concerning the electronic DNI both suspension and reactivation of electronic identification means are not considered.

(d) Renewal and replacement

Concerning the DNI, every renewal, no matter the cause, will involve a change of keys.

In general, the physical support, card, of this document will be valid, from the issuance date or from the renewal date for a period of:

- Two years if the applicant is older than five.
- Five years if the applicant is five years old and not thirty years old when the issuance or renewal takes place.
- Ten years, if the holder is already thirty years old but not seventy years old yet.
- Permanent if the holder is seventy years old or, being thirty years old, is proved to be severely disabled.
- One year for certain exceptional cases contained in the Royal Decree about DNI issuance (for instance, if the citizen cannot provide part of the requested documents at the moment of the issuance).

On the other hand, qualified electronic certificates in the DNI will be valid for a maxim period of 60 months (see informative note of the CPS [6]) as long as this period is no longer than the validity of the physical support. In this case, the certificate expiration date is the same than the support expiration date.

In this context, there may be the following cases of a certificate renewal with change of keys:
- Renewal of certificates due to renewal of support that has reached its expiration date or in those mentioned cases concerning change of data. The renewal will take place with physical attendance of the document holder in the DNI issuance offices, providing, if data have changed, justifying documents that prove such change.
- Renewal of certificates due to issuance of support copy. It is the case of renewal due to theft, loss, destruction, damage or because the DNI chip does not operate properly.
- Renewal due to expiration of the certificates without a change of support. This request can be made through the DNI Updating IT Devices in the DNI issuance offices as long as the physical support (DNI card) has not reached the period in which its renewal can be requested.
- Renewal due to the holder will without a change of support.

This request can be made through the DNI Updating IT Devices in the DNI issuance offices as long as the physical support (DNI card) has not reached the period in which its renewal can be requested.

Concerning the security levels (Assurance level), their fulfillment is guaranteed:

NOTE: The applied level is HIGH, even though the SUBSTANTIAL and LOW level requisites must be fulfilled.

LOW and SUBSTANTIAL level

- **Taking into account the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or is based on a valid electronic identification means of the same, or higher, assurance level. In this sense, the renewal will take place with physical attendance of the document holder in the DNI issuance offices, providing, if data have changed, justifying documents that prove such change. On the other hand, renewal of keys is voluntary, depending on the citizen will and free.**

HIGH level

- **Where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source. In this sense, the renewal of the electronic identification means is allowed (without changing the QSCD card - qualified electronic signature creation device) after the citizen authentication through fingerprints, using the DNI Update Points.**

  NOTE: The certificates of Identity and Electronic Signature are stored in a Qualified Electronic Signature Creation Device in accordance with Regulation (EU) 910/2014. (DNIe-DSCF / QSCD). See DNIe v2.0 [4] [5] and DNIe v3.0 [2] [3] in eIDAs Observatory (https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds).

4.2.3. **Authentication**

Describe the authentication mechanism including terms of access to authentication by relying parties other than public sector bodies

For the implementation of online authentication so that any service provider established in the territory of another Member State can confirm the identification data of the person received in electronic format provided for in Regulation (EU) No 910/2014 Spain will adopt an architecture based on a proxy service.

This implies that it will be the proxy service of the Spanish eIDAS node that manages the request for SAML authentication from another Member State, returning the result of it through a SAML assertion.

For this purpose, the proxy service will transform the SAML request received from the connector of the eIDAS node or from the middleware of the Member State requesting the authentication, in an authentication request to the electronic DNI, behaving therefore as an application that identifies and authenticates a citizen to establish a secure channel of communication with him. The established channel is authenticated at both ends by the use of certificates that guarantee the identity of the parties.

The authentication of the citizen by the proxy service of the eIDAS node initially requires the opening of an SSL tunnel between the citizen's browser and the Spanish eIDAS node's proxy service to establish a trust relationship and subsequently the validation between the eIDAS proxy service Spanish and the validation lists of the National Electronic Identity Document held by the General Directorate of the Police.

In particular, the steps that occur are the following:

1. **The opening of an SSL tunnel begins, for which the eIDAS node's proxy service creates an authenticated message signed with its website authentication certificate and sends it to the citizen's browser.**
2. **The citizen verifies the validity of the offered certificate.**
3. **The session key is generated and encrypted with the public key of the eIDAS proxy service.**
4. **The key exchange message is constructed.**
5. **The citizen introduces or approximates the electronic ID to the reader and, with the electronic authentication certificate, validates the key exchange message.**
6. **The private channel is established.**
7. **The eIDAS node proxy service verifies the session establishment message.**
8. **The proxy service of the eIDAS node checks in the Validation Authority of the electronic DNI, through the OCSP standard the validity status of the Citizen Authentication Certificate.**
9. **A secure channel is established, SSL tunnel is closed.**
10. **The eIDAS node proxy service obtains the citizen identification data present in its Certificate of Authentication.**

As it is reflected in the previous scheme, the authentication process between both parties for the establishment of a secure channel requires the use of:

- **Certificate of website authentication of the eIDAS node's proxy service: This certificate associated with the website linked to the eIDAS node's Spanish proxy service guarantees that the citizen is connecting to that service and not to another. The certificate used by this service will be a qualified certificate of website authentication in accordance with Regulation (EU) No 910/2014, guaranteed by a Certification Authority different from the General Directorate of the Police.**
- **Certificate of authentication of the citizen contained in the National Electronic Identity Document. The citizen to authenticate against the proxy service of the eIDAS node has a certificate with authentication capability, which allows the service to determine the identity of the citizen. The veracity of this certificate will be determined by the General Directorate of the Police.**

The parties involved for the establishment of the private channel are therefore:

- **Electronic DNI: Secure electronic signature and authentication device in possession of the citizen issued by the DNI Institution, which will contain:**
  o Set of private keys of the citizen.
  o Set of citizen certificates.
  o Security elements to guarantee the integrity of the document against possible alterations.
- **Citizen: Individual physical holder of the electronic DNI.**
- **Proxy service of the eIDAS node in Spain.**
- **Validation Authority: Information service on the validity status of citizen certificates.**

The protocol described in the previous scheme corresponds to the establishment of an SSL (Secure Socket Layer) session in the server-client authentication mode, which requires both the service provider (eIDAS node proxy service) to authenticate itself to the client (citizen), as the client authenticates in front of the server. The choice of this mechanism is determined by the fact that practically 100% of the servers and clients used have this capacity.

The goal is to electronically ensure the citizen identity when performing a telematics transaction. The authentication certificate (digital signature) ensures that the electronic communication is established with the appropriate person. The holder can prove the identity through the certificate in any case, because the holder has both the identity certificate and the private key linked to it.

It is mainly used to generate authentication messages (identity confirmation) and safe access to IT systems, through the establishment of private and confidential channels.

Concerning the security levels (Assurance level), their fulfillment is guaranteed:

NOTE: The applied level is HIGH, even though the SUBSTANTIAL and LOW level requisites must be fulfilled.

LOW level

- **The release of personal identification data is preceded by a reliable verification of the electronic identification means and its validity.** See SUBSTANTIAL level.

- **Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline.** In this sense, the authentication method with keys exchange (in detail in HIGH level) attempts to protect the card privacy, not disclosing its identity before the channel is encrypted and the terminal has previously been authenticated. In order to achieve these goals a previous keys exchange step is carried out through a Diffie-Hellman mechanism. This way, all the exchanged data as part of the authentication mechanism are protected with the aim to offer protection against loss and against any risk, including out of line analysis. This alternative is based on the card capacity to verify certificates signed by a root certification authority, possibly through intermediate certification authorities, and the checking through challenge-response protocols that the other party has the private key linked to the certificate.

- **The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.** See HIGH level.

SUBSTANTIAL level

- Low level plus the following:

- **The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication.** In this sense, the electronic DNI uses safe channels for its communications. For the safe channel establishment, a card and terminal public keys exchange is carried out first through certificates to be verified by both parties. This implies that the terminal counts on a valid electronic certificate verified by the electronic DNI before performing the mutual authentication protocol, with seeds exchange for the derivation of a common seed that originates the encryption and authentication session keys. This way, the release of personal identification data is preceded by a reliable verification of the electronic identification means and its validity through a dynamic authentication. On the other hand, the authentication method with keys exchange (in detail in HIGH level) is based on the card capacity to verify certificates signed by a root certification authority, possibly through intermediate certification authorities, and the checking through challenge-response protocols that the other party has the private key linked to the certificate.
- **The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.** See HIGH level.

HIGH level

- Substantial level plus the following:

- **The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing,**

eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms. In this sense, thanks to the use of these two mechanisms (safe channels and messages securing) safety controls are established to verify the electronic identification means, so it is not really likely that activities such as attempts to guess, listen, reproduce or manipulate the communication by an attacker with a basic improved potential for attack can modify the authentication mechanisms. These mechanisms are explained in detail:

Safe channels establishment

The electronic DNI uses safe channels for its communications. For the safe channel establishment, a card and terminal public keys exchange is carried out first through certificates to be verified by both parties. This implies that the terminal counts on a valid electronic certificate verified by the electronic DNI before performing the mutual authentication protocol, with seeds exchange for the derivation of a common seed that originates the encryption and authentication session keys. This way, the release of personal identification data is preceded by a reliable verification of the electronic identification means and its validity through a dynamic authentication.
Once the common seed establishment protocol is finished all the messages must be transmitted secured.

If the established safe channel is severed by the reception of a APDU command that does not respect the safe message format or due to an error concerning the authentication or MAC information, the channel is disabled and the card security status is reset (session keys are erased and presented secrets are invalidated).
The safe channel can be established through both contact and non-contact interfaces.

This proceeding enables both parties (card and external application) to trust in each other through the mutual presentation of certificates and their verification. In the process it is also included the safe exchange of some session keys that are used to secure (encrypt) all the subsequent exchanged messages. It is based on the international standard [EN419212] and its main characteristics are the following:

- Key exchange authentication

This proceeding is connected with section 8.6 of the document [part of family EN419212] with the use of RSA keys of up to 2048 bits, and SHA-256 for the validation of certificates and authentication commands.

The aim of this authentication method is to protect the card privacy, not disclosing the identity before the channels is encrypted and before the previous authentication of the terminal. In order to achieve these goals, a previous step of keys exchange is used through a Diffie-Hellman mechanism. This way all the exchanged data as part of the authentication mechanism are protected with the aim to offer protection against loss and against any risk, including out of line analysis.

This alternative is based on the card capacity to verify certificates signed by a root certification authority, possibly through intermediate certification authorities, and the checking through challenge-response protocols that the other party has the private key linked to the certificate.

Messages securing

The electronic DNI can, after the establishment of a safe channel, secure the transmitted messages. Previous authentication of both terminal and card, through electronic certificates, is necessary in order to accomplish the establishment.

Once the channel is established, messages exchanged between document and terminal are encrypted and authenticated. This way, a peer-to-peer communication is guaranteed between the two channel original points. Safe channel may be required by the application or may be an access restriction imposed to some card resource.

As it has been mentioned above, the electronic DNI counts on protection through two safe channels: one to send data and another one to send the secret code. The establishment of the safe channel is carried out through mutual authentication using authentication certificates both for the terminal and for the card.

It can be said that thanks to the use of these two mechanisms: safe channels and messages securing, safety controls to verify the electronic identification means are established, so it is not really likely that activities such as attempts to guess, listen, reproduce or manipulate the communication by an attacker with a high potential for attack can modify the authentication mechanisms.

4.2.4. **Management and organisation**

Describe the management and organisation of the following aspects:

The Directorate General of Police is a qualified trust service provider (QTSP) [1] issuing qualified certificates. Established and supervised in Spain, it is published in the List of trust service providers (TSL) https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf [10] and is in accordance with Regulation (EU) 910/2014 considering the standards ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 guarantees compliance.

NOTE:

ETSI EN 319 401: General Policy Requirements for Trust Service Providers
(http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/en_319401v020101p.pdf)

ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
(http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.01.01_60/en_31941101v010101p.pdf)

ETSI EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
(http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.01.01_60/en_31941102v020101p.pdf)

(a) General provisions on management and organization

Concerning the security levels (Assurance level), their fulfillment is guaranteed:

HIGH level

- **Providers delivering any operational service covered by this Regulation are a public authority or a legal entity recognised as such by national law of a Member State, with an established organisation and fully operational in all parts relevant for the provision of the services. In this sense, according to the article 3 of the Royal Decree 1553/2005, of the 23rd of December, concerning the DNI and its electronic signature certificates, the Ministry of Interior is the competent body for the exercise of the management, direction, organization, development and administration functions in relation to all the aspects of DNI issuance and manufacturing, according to legislation about citizen security and electronic signature.**

  In the same line, the exercise of the above mentioned competences, including the issuance of the qualified electronic signature certificates, will be carried out by the Directorate General of Police, which is also responsible for the custody and responsibility for files, automated or not, related to the DNI. This way, the Directorate General of Police is submitted to the duties imposed to the responsible for the files, under the Organic Act 15/1999 of the 13th of September, about Personal Data Protection.

  Concerning the applicable legislation from the internal point of view, we find the Royal Decree 1553/2005 of the 23rd of December, about the issuance of DNI and its electronic signature certificates last amend by the Royal Decree 414/2014 of the 29th of May.

- **Providers comply with any legal requirements incumbent on them in connection with operation and delivery of the service, including the types of information that may be sought, how identity proofing is conducted, what information may be retained and for how long. In this sense, in the section 4.2.1 about Enrolment there is a description of the type of information that can be requested as well as the way to perform the identity proofing. The information to store and how long is described in sections 5.4 and 5.5 of CPS [6]. All this in compliance with the national legal requirements of the application as well as regulatory developments.**

- **Providers are able to demonstrate their ability to assume the risk of liability for damages, as well as their having sufficient financial resources for continued operations and providing of the services. In this sense, the Qualified Trust Service Provider [1] complies with the Law 59/2003 of the 19th December about electronic signature and Regulation (EU) 910/2014.**

- **Providers are responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the providers themselves had performed the duties. In this sense, the Qualified Trust Service Provider [1] is responsible according to the**

article 11 of the Regulation (EU) No. 910/2014 of the European Parliament and of the Council of the 23rd of July, 2014, on electronic identification and trust services for electronic transactions in the internal market, and repealing Directive 1999/93/CE.

- **Electronic identification schemes not constituted by national law shall have in place an effective termination plan. Such a plan shall include orderly discontinuations of service or continuation by another provider, the way in which relevant authorities and end users are informed, as well as details on how records are to be protected, retained and destroyed in compliance with the scheme policy.** In this sense, it is not applicable.

(b) Published notices and user information

Concerning the security levels (Assurance level), their fulfillment is guaranteed: HIGH level

- **The existence of a published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage. The service definition shall include a privacy policy.** In this sense, there are information channels related to the electronic identity, the information brochures delivered to the citizen before of the issuance, the CPS [6], PDS [7] [8], terms and conditions [9], at citizen disposal on the electronic DNI web page (https://www.dnielectronico.es/). There is also a FAQ on this web page that offers the resolution of frequent interesting questions for the citizen. On the other hand, both the electronic DNI and the linked certificates are personally delivered to the citizen. At the moment of delivery of the electronic DNI, and through prior knowledge of the terms and conditions [9], the citizen is told how to obtain the CPS [6], as well as the rest of information contained in the article 18.b) of the Law 59/2003 of the 19th of December and article 24.2.d) of the Regulation (UE) 910/2014.

- **Appropriate policy and procedures are to be put in place in order to ensure that users of the service are informed in a timely and reliable fashion of any changes to the service definition and to any applicable terms, conditions, and privacy policy for the specified service.** In this sense, the CPS [6] is published at the very moment of creation and is published again when any amendment is passed. In case of significant CPS [6] modifications as well as in PDS [7] [8] or terms and conditions [9], they will be published in the internet web page (https://www.dnielectronico.es/).

- **Appropriate policies and procedures are to be put in place that provide for full and correct responses to requests for information.** In this sense, both CPS [6], PDS [7] [8], terms and conditions [9], as in the above mentioned web page of the electronic DNI (https://www.dnielectronico.es/) there are operative communication channels for consultation.

(c) Information security management

Concerning the security levels (Assurance level), their fulfillment is guaranteed:

NOTE: The applied level is HIGH, even though the SUBSTANTIAL and LOW level requisites must be fulfilled.

LOW level

- **There is an effective information security management system for the management and control of information security risks.** In this sense, the National Security Framework (ENS) regulated by Royal Decree 3/2010 of the 8th of January amended by the Royal Decree 951/2015 of the 23rd of October, has the goal to establish the security policy concerning the use of electronic means and consists of basic principles and minimum requirements that enable an adequate protection of the information through the security management that is legally applied to the Spanish Administration.

  The Directorate General of Police is a qualified trust service provider (QTSP) [1] issuing qualified certificates. Established and supervised in Spain, it is published in the List of trust service providers (TSL) https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf [10] and is in accordance with Regulation (EU) 910/2014 considering the standards ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 guarantees compliance.

SUBSTANTIAL and HIGH level

- Low level plus the following:

- **The information security management system adheres to proven standards or principles for the management and control of information security risks.** In this sense, the above mentioned ENS

ensures it.

The Directorate General of Police is a qualified trust service provider (QTSP) [1] issuing qualified certificates. Established and supervised in Spain, it is published in the List of trust service providers (TSL) https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf [10] and is in accordance with Regulation (EU) 910/2014 considering the standards ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 guarantees compliance.

(d) Record keeping

Concerning the security levels (Assurance level), their fulfillment is guaranteed: HIGH level

- **Record and maintain relevant information using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention.** In this case, information is registered and kept according to the above mentioned ENS and together with the good practices recommended by ISO 27002 and the Organic Act concerning Personal Data Protection. In the same way, paper records are also kept according to the National Archival Law and other applicable regulation.

  The Directorate General of Police is a qualified trust service provider (QTSP) [1] issuing qualified certificates. Established and supervised in Spain, it is published in the List of trust service providers (TSL) https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf [10] and is in accordance with Regulation (EU) 910/2014 considering the standards ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 guarantees compliance.

- **Retain, as far as it is permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed.** In this case, information generated by auditing records is kept online until it is filed. Once filed, audit records will be kept at least during 15 years. All the information and documents related to qualified certificates will be kept during at least 15 years. For the audit records it is applicable the CPS [6], always taking into account any peculiarity specified in it concerning the Certificate and the data involved. Records are kept and protected during the necessary period for audit and breaches investigation within the limit established only by the legislation.

  The Directorate General of Police is a qualified trust service provider (QTSP) [1] issuing qualified certificates. Established and supervised in Spain, it is published in the List of trust service providers (TSL) https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf [10] and is in accordance with Regulation (EU) 910/2014 considering the standards ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 guarantees compliance.

(e) Facilities and staff

NOTE: The Directorate General of Police is a qualified trust service provider (QTSP) [1] issuing qualified certificates. Established and supervised in Spain, it is published in the List of trust service providers (TSL) https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf [10] and is in accordance with Regulation (EU) 910/2014 considering the standards ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 guarantees compliance.

Concerning the security levels (Assurance level), their fulfillment is guaranteed: HIGH level

- **The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil.** The Royal Decree 951/2015 that amends the above mentioned ENS demands qualified staff and certified material concerning information security.

- **The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures.** In this sense, the public financing of the electronic DNI issuance project as well as the development of its functionalities ensures the necessary staff for the operation and assignment of resources for the service in order to be provided in a proper way according to the established policies and procedures.

- **Facilities used for providing the service are continuously monitored for, and protect against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service.** In this sense, facilities where the service is provided are under continuous control with a complete control system for physical access at the entrance and exit with several control levels and 24 hour surveillance, 7 days a week, also CCTV, etc. On the other hand, the CPS [6] in force informs about service protection against natural events as

well as about the measures taken concerning used facilities to provide the service.

- **Facilities used for providing the service ensure that access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors.** Used facilities to provide the service ensure that the access to those areas with management of personal, cryptographic or confidential information is limited to the staff or the authorized subcontractors with the following security measures: police control, controlled access through cards, reinforced doors and CCTV.

Besides, all the information and documents related to the facilities and staff is regulated by the above mentioned CPS in force [6].

(f) Technical controls

NOTE: The Directorate General of Police is a qualified trust service provider (QTSP) [1] issuing qualified certificates. Established and supervised in Spain, it is published in the List of trust service providers (TSL) https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf [10] and is in accordance with Regulation (EU) 910/2014 considering the standards ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 guarantees compliance.

Concerning the security levels (Assurance level), their fulfillment is guaranteed:

NOTE: The applied level is HIGH, even though the SUBSTANTIAL and LOW level requisites must be fulfilled.

LOW level

- **The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.** There are technical controls described in the above mentioned ENS to manage the risks (risk assessment and management) that may affect the security of services and to protect confidentiality, integrity and availability.

- **Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.** The electronic communication channels used to exchange personal or confidential information are protected against tapping, manipulation and reproduction through the establishment of VPN and cryptographic cards concerning the DNI. For the rest of the information, connections among staff are carried out through Macrolan. Anyway, each worker has a professional card with a cryptographic chip that enables the encryption of information in case it is requested.

- **Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, is restricted to the roles and applications strictly requiring access. It shall be ensured that such material is never persistently stored in plain text.** The storage is carried out in a Restricted Access Area and its generation is accomplished according to a cryptographic keys generation ceremony and according to recognized standards.

- **Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches.** The above mentioned ENS obliges to design and keep certain procedures to ensure a constant security over time. This regulation imposes some periodic assessments according to the requirements of such decree. On the other hand, all the information and documents related to technical controls to ensure that security is kept over time are regulated by the above mentioned CPS in force [6].

- **All media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.** The above mentioned ENS ensures that all the means containing personal, cryptographic or confidential information are stored, transported and erased in a safe way.

HIGH and SUBSTANTIAL levels

- Low level plus the following:

- **Sensitive cryptographic material, if used for issuing electronic identification means and authentication is protected from tampering.** Confidential cryptographic material, if used to issue electronic and authentication identification means, is protected against its manipulation. On the other hand, cryptographic security modules used to issue the electronic DNI comply with the requirements established in an electronic signature product protection profile of a standardized certification authority, according to ITSEC, Common Criteria or FIPS 140-2 Level 3

or higher security level.

Also, the certificates of Identity and Electronic Signature are stored in a Qualified Electronic Signature Creation Device in accordance with Regulation (EU) 910/2014. (DNIe-DSCF / QSCD). See DNIe v2.0 [4] [5] and DNIe v3.0 [2] [3] in eIDAs Observatory (https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds).

Besides, the information and documents related to technical controls are regulated by the above mentioned CPS in force [6].

(g) Compliance and audit

Concerning the security levels (Assurance level), their fulfillment is guaranteed: HIGH level

- **The existence of periodical independent external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy. In this sense, independent periodic external audits are foreseen according to the Royal Decree 3/2010 that regulates the above mentioned ENS. On the other hand, the Directorate General of Police is a qualified trust service provider (QTSP) [1] that must be audited at least every 24 months by a conformity assessment body (CAB) according to the article 20.1 of the Regulation 910/2014 (eIDAs), point 9 DPC [6] and point 9 PDS [7] [8].**

  In this regard, on June 22, 2017, the CAB (AENOR) issued certificate to the Police General Directorate as Qualified Trusted Service Provider (PSC-2017/0012) [1] in accordance with Regulation (EU) 910/2014, considering the standards ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2.

  AENOR (http://www.aenor.es) **is a CAB (conformity assessment body) accredited against the requirements of the eIDAS Regulation. See CAB (AENOR) in eIDAs Observatory** (https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation).

- **Where a scheme is directly managed by a government body, it is audited in accordance with the national law. In this sense, the National Police Force is a State body that manages directly the system and it will be audited according to the national competent legislation.**

  Besides, based on the temporary measure of the article 51 of the Regulation (EU) No 910/2014 of the European Parliament and of the Council of the 23rd of July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/CE.

  "A certification-service-provider issuing qualified certificates under Directive 1999/93/EC shall submit a conformity assessment report to the supervisory body as soon as possible but not later than 1 July 2017. Until the submission of such a conformity assessment report and the completion of its assessment by the supervisory body, that certification- service-provider shall be considered as qualified trust service provider under this Regulation."

  On the other hand, in article 20.1 of the Regulation 910/2014 we can read the following:

  "Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it."

  Also in compliance with point 9 of CPS [6] and point 9 of PDS [7] [8].

  Being the Directorate General of Police a qualified trust service provider [1] that issues qualified certificates it is foreseen, in the estimated period, the elaboration of the corresponding assessment report according to the Regulation 910/2014.

  In this regard, on June 22, 2017, the CAB (AENOR) issued certificate to the Police General Directorate as Qualified Trusted Service Provider (PSC-2017/0012) [1] in accordance with Regulation (EU) 910/2014, considering the standards ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2.

AENOR (http://www.aenor.es) **is a CAB (conformity assessment body) accredited against the requirements of the eIDAS Regulation. See CAB (AENOR) in eIDAs Observatory** (https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation).

4.3. **Interoperability requirements**

Describe how the interoperability and minimum technical and operational security requirements under Commission Implementing Regulation (EU) 2015/1501 ([21]) are met. List and attach any document that may give further information on compliance, such as the opinion of the Cooperation Network, external audits, etc.

Article 12 of Regulation 910/2014 (Cooperation and Interoperability) provides that the national systems for electronic identification, notified pursuant to article 9. Section 1, will interoperate, and that will make necessary to establish an interoperability framework.

The interoperability framework will consist, among other factors, of a single reference to a minimum set of data for persons´ identification, which will unequivocally present a natural or legal person, and which will be available in the electronic identification systems.

In this respect, the Commission Implementing Regulation (EU) 2015/1501 provides for the technical and operational requirements in the interoperability framework, aimed at guarantee the interoperability of the electronic identification systems which the Member States may notify the Commission.

These requirements include, in particular, the minimum set of persons´ identification data which in an exclusive and unequivocal manner refer to a natural or legal person, as is laid down in article 11 and in the annex to the Commission Implementing Regulation (EU) 2015/1501, whenever it is used in a trans-border context. For the case of the electronic identity document (DNI), it is the minimum set of data for a natural person, which is listed in the Annex to the Commission Implementing Regulation (EU) 2015/1501.

As can be confirmed in the CPS [6], the profile of the Citizen's Certificate of the electronic DNI (section 8.1) is considered pursuant to the requirements listed in the Annex to Commission Implementing Regulation (EU) 2015/1501, since the current trans-border identification rules do not make compulsory to incorporate new attributes or a specific type of semantics beyond what is already included in the profile for Citizen's certificate, of the electronic DNI.

In any case, the creation of new certificate profiles is being assessed, pursuant to the technical specifications for purposes of trans-border identification (such as, for example, European regulations EN 319 412-1, EN 319 412-2, EN 319 412-5, or others).

Regarding the rest of the technical requirements established in the Commission Implementing Regulation (EU) 2015/1501, the Kingdom of Spain will deploy its national node of the electronic identification interoperability architecture (eIDAS node) applying the reference implementation foreseen in Art. 12.4 of the Commission Implementing Regulation (EU) 2015/1501. The application of this reference implementation ensures compliance with the technical specifications provided in Art. 12.1 of the Commission Implementing Regulation (EU) 2015/1501 and that detail those technical requirements.

In particular, the application of said reference implementation ensures that:

- **In accordance with article 5 of the Commission Implementing Regulation 2015/1501:**
  1. **The Spanish node will be able to connect with the nodes of other Member States.**
  2. **The Spanish node will be able to distinguish between public sector agencies and other user parties by technical means.**
  3. **The online authentication mechanism made available by the Kingdom of Spain shall not impose disproportionate technical requirements and costs on the other Member States in order to interoperate with the application adopted by the first Member State.**

- **In accordance with article 6**
  1. **The Spanish node will ensure the protection of the privacy and confidentiality of the data exchanged, as well as the maintenance of integrity between the nodes, by applying the**

[2] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ L 235, 9.9.2015, p. 1).

technical solutions and protection practices included in the reference implementation, and they include, among others, the encryption of messages between nodes.

2. The Spanish node will not store any personal data, except for the data necessary to ensure that in the event of an incident, the sequence of message exchange can be reconstructed to establish the place and nature of the incident. These data will consist of the following elements: identification of the node; identification of messages; date and time of the messages, identification of the user part requesting the authentication, identification of the Member State that carries out the authentication.

- In accordance with article 7
  1. The Spanish node will guarantee the integrity and authenticity of the data in its communications with the rest of the nodes to ensure that all requests and answers are authentic and have not been altered, through the technical solutions and protection practices included in the implementation of reference, and that include, among others, the electronic signature of messages between nodes.

- In accordance with article 8
  1. The Spanish node will use for the syntax the message formats defined in the technical specifications of the eIDAS interoperability framework. This syntax will allow:
     a) the correct treatment of the minimum set of identification data of the person representing exclusively an individual or legal entity;
     b) the correct treatment of the security level of the electronic identification means;
     c) the distinction between public sector agencies and other user parties;
     d) the flexibility to meet the needs for additional attributes related to identification.

- In accordance with article 9
  1. The General Secretariat of Digital Administration, as operator of the Spanish node, will communicate the metadata of the management of said node in accordance with the standardized manner defined in the technical specifications of the eIDAS interoperability framework, so that it can be processed by mechanical means and in a safe and reliable way.
  2. The parameters of the Spanish node relevant to security will be recovered automatically.

- In accordance with article 10
  1. The General Secretariat of Digital Administration, as operator of the Spanish node, will comply with the requirements of the ISO / IEC 27001 standard by complying with national legislation on information security, in this case Royal Decree 3/2010 of January 8, which regulates the National Security Scheme in the field of Electronic Administration.
  2. The General Secretariat of Digital Administration will implement critical security updates without undue delay.

In relation to the interoperability requirement established in Article 11 of Commission Implementing Regulation 2015/1501 regarding the identification data of the person:

- The electronic DNI serves only for the identification of natural persons, so it does not contain identification data of legal entity.
- The minimum set of identification data that the electronic DNI will use to exclusively represent a natural person corresponds to the mandatory attributes described in the Annex to the Commission Implementing Regulation 2015/1501:
  1. a) last name or current surnames;
  2. b) name or current names;
  3. c) birth date;
  4. d) a unique identifier made by the issuing Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as constant as possible over time. In the case of the electronic DNI, this identifier will be made from the National Identity Document Number assigned to the citizen, to which the prefixes corresponding to the issuing Member State and the receiving Member State of the cross-border identification will be added.

- Identification data will be transmitted according to the Latin alphabet.

4.4. **Supporting documents**

List here all supporting documentation submitted and state to which of the elements above they relate. Include any domestic legislation which relates to the electronic identification provision relevant to this notification. Submit an English version or English translation whenever available.

JUSTIFICATION DOCUMENTS

- [1] AENOR Certificate to the Police General Directorate as Qualified Trusted Service Provider (PSC-2017/0012) in accordance with Regulation (EU) 910/2014, considering the standards ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2.
- [2] NCC (National Cryptologic Centre) Certification of the DNIe-DSCF product (secure signature creation device) version: 3.0.
- [3] BOE (Official State Gazette) publication; DNIe-DSCF certification; version 3.0 (BOE Certification DNIe 2017-02-CCRA).
- [4] NCC (National Cryptologic Centre) Certification of the DNIe-DSCF product (secure signature creation device) version: 2.0.
- [5] BOE (Official State Gazette) publication; DNIe-DSCF certification; version 2.0 (BOE Certification DNIe 2013-07-CCRA).
- [6] Certification Practice Statement and Policies (CPS).
- [7] PKI Disclosure Statement (PDS version ESP).
- [8] PKI Disclosure Statement (PDS version ENG).
- [9] Terms and Conditions.
- [10] Trust service list (TSL), https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf

APPLICABLE LEGISLATION

- Organic law 4/2015, of 30 March, on Citizenship Security Protection.
- 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).
- Organic law 15/1999, of 13 December, on Personal Data Protection; as the implementing regulations approved by Royal Decree 1720/2007 of 21 December.
- Law 84/78, of 28 December, regulating the fee for the DNI´s issue and renewal.
- Royal Legislative Decree 1/1996, of 12 April, approving the rewritten text corresponding to the Intellectual-Property Law.
- Law 11/2007, of 22 June, on electronic access of citizens to Public Services (repealed act, effective as of 2 October 2016, by 2.b single derogatory provision, in Law 39/2015, from 1 October).
- Law 39/2015, of 1 October, on the common administrative procedures of public authorities (effective as of 2 October 2016).
- Law 9/2014, of 9 May, General Telecommunications, which, in its sixth and final Provision, covers the modification of law 59/2003, of 19 December, on the electronic signature.
- Royal Decree 1553/2005, of 23 December, regulating the issuing of the National Identity Document and its electronic signature certificates.
- Royal Decree 1586/2009, of 16 October, modifying Royal Decree 1553/2005, of 23 December, regulating the issuing of the National Identity Document and its electronic signature certificates.
-Royal Decree 869/2013, of 8 November, modifying Royal Decree 1553/2005, of 23 December, regulating the issue of the national identity document and its electronic signature certificates.
- Royal Decree 3/2010, of 8 January, regulating the National Security Framework in the field of Electronic Administration.
- Royal Decree 951/2015, of 23 October, which modifies Royal Decree 3/2010, of 8 January, regulating the National Security Framework in the field of Electronic Administration.
- Royal Decree 414/2015, of 29 May, which modifies Royal Decree 1553/2005, of 23 December, regulating the issue 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 557/2011, of 20 April, approving the Regulation of Organic law 4/2000, Title 13, Chapter 1, 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 movement and residence in Spain of citizens of the Member States of the European Union and of other states which are party to the Agreement on the European Economic Space.
- Order INT/1202/2011, of 4 May, regulating the personal data files of the Ministry of Interior, more specifically ANNEX 1, Secretary of State for Security, Directorate General of Police, scope National Police Force, Point 3: Adexttra.
- Law 40/2015, of 1 October, on legal regime of the public Sector (entry into force: 2 October 2016).
- Royal Decree 1708/2011, of 18 November, establishing the Spanish Archives System and regulating the Archive System of the General State Administration and of its Public Bodies and its rules for access.