DNIe Practice Statement and Certification Policy.

Law 59/2003, of December 19, of Electronic Signature, has given to Documento Nacional de Identidad (National Identity Card) new effects and utilities, for instance electronic identity and other personal data of the owner, such as signer identity and the integrity of the documents signed with electronic signature devices, whose incorporation to it is established.

This new identification way based on present DNI, whose issue is regulated by **Real Decreto 1553/2005**, of December 23, will allow citizens to establish their confident relations with others through new technology, the same way they have been doing with the current Card during more than 50 years.

To meet this, Dirección General de la Policía, who is the responsible entity to issue and manage DNI as the RD defines, will establish a Public Key Infrastructure who will give new DNI needed electronic certificates to meet properly previous objectives.

The present document collects the Practice Statement and Certification Policy (DPC) that establishes the operating of Public Key Infrastructure of the Public Identity Certificates and Documento Nacional de Identidad electronic signature (from this point forward DNIe). This DPC also collects a Certification Policy that Dirección General de la Policía (Interior Ministry) uses to certificates management.

This DPC applies to all the participants related to the DNIe hierarchy, including Certification Authorities (AC), Registry Authorities, Citizens, Other Accepting Parts, amongst others.

This Practice Statement and Certification Policy has been developed according to orders given by PKIX task force of IETF (Internet Engineering Task Force), in its model document RFC 3647 (approved in November 2003) "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". In order to give the document a standard character and make easier reading and analysis it, all sections defined at RFC 3647 are included.

"No defined" sentence will figure if nothing has been expected. In addition, established in RFC 3647 chapters, an additional chapter dedicated to personal data protection has been included to fulfill Spanish normative. It has been considered European standards to develop its content, the main ones are:

- ETSI TS 101 456: Policy Requirements for certification authorities issuing qualified certificates.
- ETSI TS 101 862: Qualified Certificate Profile.
- ETSI TS 102 042: Policy Requirements for certification authorities issuing public key certificates.

In the same way, the following has been considered as basic normative applied:

- 1999/93/CE Directive of the European Parliament and Council, of December 1999, which establishes an electronic signature community framework.
- Ley 59/2003, of December 19, Firma Electrónica.
- Ley Orgánica 15/1999, of December 13, of Protección de Datos de Carácter Personal.

• Real Decreto 994/1999, of June 11, which approves Reglamento de Medidas de Seguridad de los Ficheros Automatizados que Contengan Datos de Carácter Personal.
• Real Decreto-Legislativo 1/1996, of April 12, which approves the Texto Refundido de la Ley de Propiedad Intelectual.
• REAL DECRETO 1553/2005, of December 23, which establishes the DNI issue and its electronic signature certificates.

This DPC collects service policy, and also the offered guarantee level statement by the description of the technical and manage measures established to guarantee PKI secure level.

DCP includes all activities aligned to manage electronic certificates in their life cycle and it is used as a guide to the relationship between DNIe and the users. In consequence, all parts involved have the obligation to know the DPC and to adjust their activity to which is established in it.

Public Identity Certificates will be issued as **Recognized Electronic Certificates** achieving requirements defined at appendix I of 1999/93/CE Directive of the European Parliament and Council, of December 1999, which defines an electronic signature community framework, and also at Law 59/2003, of December 19, Electronic Signature.

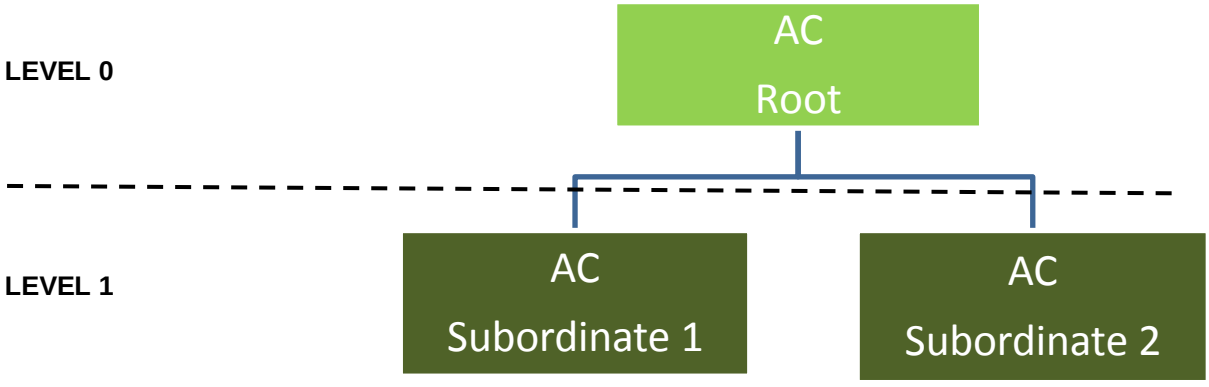
The certification services provider, Dirección General de la Policía (Interior Ministry), will meet requirements defined at appendix II of Directive mentioned above and developed in Law 59/2003, of December 19, of Electronic Signature. Moreover, the certificates meet standards related to recognized certificates, particularly:

• ETSI TS 101 862: Qualified Certificate Profile.
• RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

According to mentioned normative, the advanced electronic signature based on a recognized certificate and generated by a secure signature creator device it is considered as recognized electronic signature. Recognized electronic signature will have the same value respect electronic data, that manual signature has respect paper documents

This DPC assumes that reader knows PKI, certificate and electronic signature meanings, in other case it is recommended to train himself to previous concepts before continue reading this document.

General architecture, at hierarchical level, of the PKI of the DNIe is the following:



☐ In the first level it is located AC root, it represents the confidence point of the whole system. As stated in art. 15 of the Electronic Signature Law, it will allow individuals, legal entities, public or privates to recognize the efficiency of DNIe to validate the identity.

☐ In the second level there are AC Subordinates to the AC Root, it will issue identity and signature new DNI certificates.

Appropriate use of certificates.

Public Identity Certificates, issued by DGP (Interior Ministry) have the following purposes:

• **Authentication Certificate**: It is used to guarantee citizen identity while doing a telematic transaction. Authentication Certificate (Digital Signature) ensures that electronic communication is done with the person who said it. The owner, through his certificate, could identify his identity to anybody because he possesses the identity certificate and the private key associated.

The use of this certificate is not enabled on operations that require non-repudiation of origin, so third accepting parties and telematic service suppliers will not have compromise guarantee of the DNI owner with the signed content.

The main use is to generate authentication messages (identity confirmation) and secure access to computer systems (by establishing private and confidential channels with telematic service suppliers). This certificate also could be used as identification way to a registry execution that allows recognized certificates issue recognized by private entities, without being obliged to carry heavy investment in the deployment and maintenance of a registry infrastructure.

• **Signature Certificate:** The purpose of this certificate is to allow citizen to sign documents or paperwork. This certificate (qualified certificate according to ETSI, RFC3739 and 99/93/EC European Directive and recognized by Electronic Signature Law) allows replacing manual signature for electronic one in citizen relations with other parties (LFE 59/2003 art 3.4 and 15.2).

Signature certificates are recognized according to article 11.1, with the content established in article 11.2 and they are issued achieving articles 12, 13 and 17 to 20 of Ley 59/2003 of 19 December, Firma Electrónica. They achieve European Institute of Telecommunication Normative technical regulations, identified with the TS 101 456 reference.

They are recognized certificates that operate as secure electronic signature creator devices, according to article 24.3 of the 59/2003 Law, December 19. For this, they guarantee the identity of the citizen that owns identification and signature private key and they allow "recognized electronic signature" issue; in other words, advanced electronic signature based in a recognized certificate and generated used a secure device, for this, according to article 3 of the 59/2003 Law of December 19, it is put in the same level, to legal effects, that written signature and there is no need to fulfill any other additional requirement.

According mentioned, this certificate must not be used to generate validation messages (identity verifying) and secure access to computing systems (by establishing private and confidential channels with service providers)

Common use of both certificates provides the following guarantees:

- **Origin Authentification**

Through Authentification Certificate, the citizen will identify himself demonstrating the possession and the access to the private key associated to the public one which is included in the certificate that identifies his identity. Both private key and certificate are stored in Documento Nacional de Identidad, which has a cryptographic capacities processor

This can guarantee that citizen private key (the validation of his identity is based on this point) never leaves DNI physical medium. This way, at the moment the citizen validates electronically himself must have his DNI and his personal access key (PIN) to the certificate private key.

- **No origin refuse**

It ensures that the document comes from citizen who says it comes from. This feature is obtained by electronic signature through Signature Certificate.
The recipient of an electronic signed message could validate the used certificate to that signature using any of the DNIe Validation Service Providers. This ensures that the document provides from a certain citizen.

Because DNIe is a secure signature issue device and signature keys keep under citizen control since their creation, it is guaranteed the agreement between it and the signature done ("no refuse" guarantee)

- **Integrity**

By using **Signature Certificate**, it is possible to check that the document has not been modified by any external agent to the communication.

To guarantee the integrity, the cryptography offers solutions based on special feature functions, called summary functions, which are always used when an electronic signature is done. The use of this system allows checking that a signed message has not been modified since sending to reception. To do that, a unique summary of the document is signed with the private key, so any modification of the message changes the summary.

For your interest: it is available to download the **Practice Statement and Certification Policy** (DPC) in Spanish from the link: http://www.policia.es/dpc