Bugzilla ID: 526181
Bugzilla Summary: Add Spanish government DNIe root certificate

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	**Data**
CA Name	Dirección General de la Policía (Ministerio del Interior)
Website URL	http://www.policia.es http://www.dnielectronico.es/ http://www.dnie.es
Organizational type	National Government CA
Primary market / customer base	DNIe, is the electronic Spanish National Identity Card. It is the electronic version of the Spanish National Identity Document (DNI) issued by the Dirección General de la Policía (the National Police Force in Spain). The DNI is required for every citizen over 14 years of age. Most of the Spanish citizens use the DNIe to identify themselves and interact against both, government and privates online services.
CA Contact Information	**CA Email Alias:** certificados@dnielectronico.es An email alias is being requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization. **CA Phone Number:** 34913223400 A main phone number from which Mozilla can reach the organization responsible for root certificates for the CA. **Title / Department:** Technical Office of the eDNI If Mozilla needed to call your main phone number, what Title/Department should the Mozilla representative ask for

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data**
Certificate Name	AC RAIZ DNIE
Cert summary / comments	
The root CA certificate URL	https://bugzilla.mozilla.org/attachment.cgi?id=410022
SHA-1 fingerprint.	22:29:F0:56:D3:4D:1C:B6:3E:98:6F:26:B2:D0:8A:B9:4F:F0:8E:4D (different than provided in bug)
Valid from	2006.02.16
Valid to	2036.02.08
Cert Version	3
Modulus length / key length	4096

Test Website(s)	If SSL… For testing purposes, please provide a URL to a website whose SSL cert chains up to this root. If not SSL, please provide a test cert chaining up to this root.
CRL URL	http://crls.dnielectronico.es/crls/ARL.crl CP section 4.9.7: DNIe **The PKI does not publish CRLs in open access repositories. These are only available as a medium for exchange of certificates status with Service Providers Validation.** DNIe publish a new CRL in your repository at the time that occurs any revocation, and, ultimately, at intervals not exceeding 24 hours (although not changes occurring in the CRL) to those generated by subordinate CAs and 3 months for ARL generated by the CA Root.
OCSP Responder URL	http://ocsp.dnie.es http://ocsp.dnielectronico.es
CA Hierarchy	The PKI includes three subordinates CA. The validation activity has been segregated in order to improve privacy. The number of subordinates CA will be increased if necessary.
Sub-CAs operated by 3rd parties	Are all of the subordinate CAs operated internally by the Dirección General de la Policía?
cross-signing	None
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	SSL/TLS & code/document signing If this hierarchy does not issue SSL certificates, then the Websites (SSL/TLS) trust bit should not be enabled. I did not find information in the CP showing that the certs would be used for S/MIME. In addition, the statement that the CRLs are not publicly available would also indicate that the Email (S/MIME) trust bit should not be enabled. It looks like the certificates issued within the DNIe hierarchy are used only for identification purposes. Therefore, I think that only the Code/Document Signing trust bit should be enabled. Do you agree? Google Translate of CP section 1.4.1: The Public Identity Certificates issued by the Directorate General of Police (Interior Ministry) will aim at: • Certificate of Authentication: Securing electronic identity citizen to make a transaction telematics. The Certificate of Authentication (Digital Signature) ensures that electronic communication is done with the person who says it is. The holder may, through its certificate to prove their identity to anyone because he is in possession of the certificate of identity and the private key associated with it. The use of this certificate is not enabled in operations requiring no repudiation of origin, so the third acceptors and providers of telematic services will not guarantee the commitment of the holder of the ID with the signed content. Its main use is to generate messages authentication (confirmation of identity) and secure access to systems computer (through establishment of private and confidential channels with telematics service providers). This certificate can also be used as identification for the execution of an order to issue registration certificates recognized by private entities without being bound to these to invest heavily in deploying and maintaining a logging infrastructure.

	Signature Certificate: The purpose of this certificate is to enable the citizen sign paperwork or documents. This certificate (certified as qualified ETSI, the European Directive RFC3739 and 99/93/EC. and recognized by law Electronic Signature) can replace handwritten signatures by electronic citizen relations with third parties (LFE No. 59/2003 s. 3.4 and 15.2). Signature certificates are recognized certificates in accordance with what is provided in Article 11.1, with the content prescribed by Article 11.2, and issued in compliance with the obligations of Articles 12, 13, and 17 to 20 of Law 59/2003 of 19 December, electronic signature, and which comply with that technical regulations mandated by the European Institute of Standards Telecommunications, identified with the reference TS 101 456. Recognized certificates are functioning as creation devices electronic signature in accordance with Article 24.3 of Law 59/2003 of 19 December. Therefore, guaranteeing the identity of the citizen holder private key and signature identification, and allow the generation of the "Electronic signature" that is, the advanced electronic signature is based on a qualified certificate and which has been generated using a trusted device, therefore, in accordance with the provisions of Article 3 of Law 59/2003 of 19 December, the firm is equated written for effect legal, without fulfilling any additional requirement. As described above, this certificate shall not be used to generate authentication messages (confirmation of identity) and access insurance systems (by establishing private channels and confidential service providers computer). The joint use of both certificates provides the following guarantees: • Authenticity of origin The Citizens may, through its Certificate of Authentication, prove your identity to anyone, showing the ownership and access to key associated private to public is included in the certificate showing your identity. Both private key and certificate are stored in the National Identity Card, which has a processor with cryptographic capabilities. This will ensure that the private key citizen (the point at which underpin the credibility of your identity) leaves no at any time the hardware of the National Identity Document. Of Thus the citizen at the time of its electronic credit identity must be in possession of your ID and personal password (PIN) to the certificate private key. • Non-repudiation of origin Ensures that the document comes from the citizen who claims to be from. This property is obtained by electronic signature by means of Certified Signature. The recipient of a signed electronically can verify the signature certificate used to using any of the Service Providers DNIe validation. This ensures that the document comes from a particular citizen. Since the DNIe is a secure signature creation and that the keys to remain firm from the moment of its creation under the control of holder citizen is guaranteed the same commitment made by signing (guarantee of "non repudiation"). • Integrity With the use of the signing certificate, it shows that the document has not been modified by any external agent communication. To ensure the integrity, cryptography offers solutions based on functions of special features, called abstract tasks, which provided it is done using an electronic signature. Use of this system shows that a signed message has not been altered between the sending and welcome. This is signed with the private key unique summary document so that any alteration of the message reverts to a impairment of its summary.

SSL Validation Type DV, OV, and/or EV	**If SSL certs** are issued in this hierarchy, do you perform identity/organization verification for all SSL certificates? Is it ever the case for SSL certs that the ownership of the domain name is verified, but the identity/organization of the subscriber is not verified?
EV policy OID(s)	Not EV
CP/CPS	Certificate Policy (Spanish): http://www.dnie.es/PDFs/politicas_de_certificacion.pdf List of e-services accepting DNIe certificates: http://www.dnie.es/servicios_disponibles/index.html
AUDIT	Please see sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/ We need a publishable statement or letter from an auditor (who meets the policy requirements) that states that they have reviewed the practices as outlined in the CP/CPS for these roots, and that the CA does indeed follow these practices and meets the requirements of one of: • ETSI TS 101 456 • ETSI TS 102 042 • WebTrust Principles and Criteria for Certification Authorities
Organization Identity Verification	3.2.2 Authentication of the identity of a legal NONE – certs are issued to individuals, not organizations. Will need to translate these sections: 3.2.3 Authentication of the identity of an individual 4.1.2 Registration of license applications
Domain Name Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate *or* has been authorized by the domain registrant to act on the registrant's behalf; **If SSL certs are issued in this hierarchy, and the Websites trust bit is to be enabled…** Please provide translations into English of the sections of the CP/CPS documents that describe the procedures for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber. Please also list the corresponding document(s) and section or page numbers containing the original text.
Email Address Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate *or* has been authorized by the email account holder to act on the account holder's behalf;

	If email (S/MIME) certs are issued in this hierarchy, and the Email trust bit is to be enabled… Please provide translations into English of the sections of the CP/CPS documents that describe the procedures for verifying that the email account associated with the email address in the cert is owned/controlled by the subscriber. Please also list the corresponding document(s) and section or page numbers containing the original text.
Identity of Code Signing Subscriber	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for certificates to be used for digitally signing code objects, the CA takes reasonable measures to verify that the entity submitting the certificate signing request is the same entity referenced in the certificate *or* has been authorized by the entity referenced in the certificate to act on that entity's behalf; Will need to translate these sections: 3.2.3 Authentication of the identity of an individual 4.1.2 Registration of license applications
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. . For the ones that are applicable, please provide further information and translations into English of the CP/CPS where relevant. • Long-lived DV certificates (SSL) o • Wildcard DV SSL certificates (SSL) o • Delegation of Domain / Email validation to third parties (SSL/Email) o • Issuing end entity certificates directly from roots o • Allowing external entities to operate unconstrained subordinate CAs o • Distributing generated private keys in PKCS#12 files o • Certificates referencing hostnames or private IP addresses o • OCSP Responses signed by a certificate under a different root o • CRL with critical CIDP Extension o • Generic names for CAs

	o