



APLIKAZIO ETA KODE SINADURAKO ZIURTAGIRIETARAKO BERARIAZKO DOKUMENTAZIOA

© IZENPE 2011

Dokumentu hau IZENPErena da. Kopiarik egitekotan, osorik kopia daiteke soilik

■ Beato Tomás de Zumárraga
71 - 1ª Planta
01008
Vitoria - Gasteiz

www.izenpe.com
info@izenpe.com
Tel.: 945 017 490



1 Sarrera

Dokumentu honek Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, SA enpresak (aurrerantzean IZENPE) jaulkitzen dituen *Aplikazio* eta *Kode Sinadurako* ziurtagirien berariazko dokumentazioa biltzen du.

Dokumentu honen helburua da IZENPEren *Ziurtapen Praktiken Deklarazioan* mota horretako ziurtagirietarako definitutakoa zehaztea eta osatzea.

Dokumentazio honek espezifikoki arautzen du *Ziurtapen Praktiken Deklarazioa*, dokumentuak *berariazko dokumentazioa* deritzon dokumentu honetara jotzen duenean.

1.1 Ziurtagirien deskribapena

Honako ziurtagiriei dagokienez,

- *Aplikazioa*,
Egiazkotasuna eta integritatea ziurtatzeko informatika-aplikazio batek erabiltzen duen ziurtagiria da.
- *Kode-sinadura*,
Software aplikazio baten egilearen identitatea eta edukiaren integritatea bermatzen duen ziurtagiria da, kodea sinatzeko erabiltzen baita ziurtagiri hori.

1.2 Identifikazioa

Ziurtagiri horiek identifikatu ahal izateko, IZENPEk objektu-identifikatzaile (OID) bat esleitzen die.

ZIURTAGIRIA	OID
Aplikazio-ziurtagiria	1.3.6.1.4.1.14777.1.2.2
Kode-sinaduraren ziurtagiria	1.3.6.1.4.1.14777. 1.3.1



2 Eskakizun operatiboak

2.1 Ziurtagiria eskatzea

Eskatzaileak ziurtagiriaren eskaera-formularioa bete beharko du, eta IZENPEk tramitatu dezan aurkeztu, honako bi bide hauen bidez:

- Telematika bidez: www.izenpe.com webgunean interesdunek eskura dute eskaera-formularioa. Eskaera bete egin beharko da, eta sinadura elektronikoari buruzko abenduaren 19ko 59/2003 Legearen arabera ziurtagiri onartu bidez sinatu beharko da elektronikoki. Ondoren, telematikoki igorri beharko zaio IZENPERi.
- Bulegoan bertan: www.izenpe.com webgunean zerrendaturik azaltzen diren erregistro-bulegoetakoren batera jo eta hantxe bete dezake eskatzaileak ziurtagiri-eskaera.
- Ohiko posta bidez: eskatzaileak IZENPERen bulegoetara ohiko posta bidez igorri ahal izango du ziurtagiriaren eskaera.

Ziurtagiri motaren arabera,

- *Aplikazioa*, aurretik, eskatzaileak gako-parea sortu beharko du zerbitzarian bertan, eta IZENPERi eman beharko dio gako publikoa eskaera-formularioarekin batera.

Eskatzailea izango da,

- *Aplikazio-ziurtagiriari* dagokionez, aplikazioaren arduradun tekniko.
- *Kode-sinadurako ziurtagiriari* dagokionez, antolakundeko arduraduna.

2.2 Egiaztatzea

Eskatzaileak, *ziurtagiria jaulkitzeko eskaeraren* bitartez, bertan jasoarazten diren datuak zuzenak eta egiazkoak direla egiaztatuko du.

2.3 Ziurtagiria jaulkitzea

Ziurtagiri motari dagokionez,

- *Aplikazioa*, eskaera sinatua eta gako publikoa eman ondoren, IZENPEk ziurtagiria jaulkitzeari ekingo dio.



- *Kode-sinadura*, ziurtagiria jaulkitzeko eskaera sinatua eman ondoren, IZENPEk ziurtagiria jaulkitzeari ekingo dio.

2.4 Ziurtagiria ematea

Ziurtagiri motari dagokionez,

- *Aplikazioa*,
Ziurtagiria jaulkitzeko eskaeran adierazten den helbide elektronikoan entregatuko dio ziurtagiria IZENPEk eskatzaileari.
Eskatzaileak entrega- eta onarpen-orria sinatu beharko du.
- *Kode-sinadura*
IZENPEk PINa eta PIN hori desblokeatzeko kodea (PUK) emango dio ziurtagiriaren eskatzaileari.
Eskatzaileak entrega- eta onarpen-orria sinatu beharko du.

2.5 Ziurtagiriak ezeztatzea

Honako hauek eska dezakete ziurtagiri bat ezeztatzea:

- Eskatzaileak.
- IZENPEk.
- Eskatzaileak baimendutako hirugarren batek.

Nolanahi ere, hirugarren horri bere izenean jarduteko baimena ematen diola aditzera ematen duen eskatzaileak sinatutako dokumentua aurkeztu beharko du.

Izapideak

Ezeztatzea eskatzen duenak *ziurtagiria ezeztatzeko eskaeraren* formularioa bete beharko du, eta IZENPEN bideratu beharko du ziurtagiriaren eskaerarako aurreikusten diren bide beretatik.

Erregistro Entitateak eskatzailearen identifikazioa jasoaraziko du ezeztatze-eskaeraren bitartez.

Ezeztatzeko arrazoiak

Ziurtapen Praktiken Deklarazioan kontsulta daiteke: www.izenpe.com



2.6 Ziurtagiriak berritzea

Ziurtagiria berritzeko (ezeztatu egin delako edo iraungi egin delako), harpidedunak ziurtagiri berria eskatu beharko du. Horretarako, ziurtagiriak jaulkitzeko finkatutako prozedurari jarraitu beharko dio.



3 Aldaketaren kudeaketa

Dokumentu honetan egiten diren aldaketak IZENPEren Segurtasun Batzordeak onetsiko ditu.

Aldaketa horiek ziurtagiri bakoitzaren berariazko dokumentazioa eguneratzeko dokumentuan jasoko dira, eta IZENPEk bermatuko du dokumentu hori eguneratuta egongo dela.

Berariazko dokumentazioaren bertsio eguneratuak honako helbidean kontsultatu ahal izango dira: www.izenpe.com.



4 Ziurtagirien profilak eta ezeztatutako ziurtagirien zerrendaren profilak

4.1 Aplikazio-ziurtagiriaren profila

Erabilerak: sinadura, SSL

Campo / extensión	Opcional / Crítica	Contenido
version		Versión 3
serialNumber		Número secuencial único
signature		sha-1WithRSAEncryption
issuer		Igual al campo subject del certificado de la CA emisora
validity		3 años
subject		
ST		Provincia
L		Localidad
EA		Correo electrónico
CN		Nombre de la aplicación
OU		Departamento
O		Nombre de la entidad
C		ES
subjectPublicKeyInfo extensions		RSA 1024 bits mínimo
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName	Opcional	Igual a la extensión subjectAltName de la petición, si está presente
extendedKeyUsage		clientAuth, emailProtection
netscapeCertType		SSL_Client, SMIME_Client
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.1.2.2 (1.3.6.1.4.1.14777.101.2.2 en Desarrollo)
cpsURI		http://www.izenpe.com/rpascaplicacion
userNotice		Bermeen mugak ezagutzeko www.izenpe.com Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantias en www.izenpe.com Consulte el contrato antes de confiar en el certificado
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlinterna2
authorityInfoAccess		ocsp http://ocsp.izenpe.com:8094
keyUsage	Crítica	digitalSignature, nonRepudiation



4.2 Kode-sinadurako ziurtagiriaren profila

Campo / extensión	Opcional / Crítica	Contenido
version		Versión 3
serialNumber		Número secuencial único
signature		sha-1WithRSAEncryption
issuer		Igual al campo subject del certificado de la CA emisora
validity		3 años
subject		
ST	Opcional	Provincia
L	Opcional	Localidad
EA		Correo electrónico
CN		Nombre entidad/aplicación
OU	Opcional	Departamento
O		Nombre de la entidad
C		ES
subjectPublicKeyInfo		RSA 1024 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName	Opcional	Igual a la extensión subjectAltName de la petición, si está presente
extendedKeyUsage		codeSigning
netscapeCertType		ObjectSigning
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.1.3.1 (1.3.6.1.4.1.14777.101.3.1 en Desarrollo)
cpsURI		http://www.izenpe.com/rpascafirmacod
userNotice		Bermeen mugak ezagutzeko www.izenpe.com Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantías en www.izenpe.com Consulte el contrato antes de confiar en el certificado
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlinterna2
authorityInfoAccess		ocsp http://ocsp.izenpe.com:8094
keyUsage	Crítica	digitalSignature, nonRepudiation