

# Política de Certificació

Projecte e-firmaGV



**Certificats per a  
Correu i Aplicacions Segures**

**Data:** 20 de gener de 2003

**Versió:** 1.0

**Arxiu:** PKIGVA-CP-02V1.0-v.doc

**OID:** 1.3.6.1.4.1.8149.3.2.1.2.1.0

**Preparat per:** Proyecto e-firmaGV

## Taula de Contingut

<b>1. INTRODUCCIÓ.....</b>	<b>7</b>
1.1. VISTA GENERAL.....	7
1.2. IDENTIFICACIÓ .....	7
1.3. COMUNITAT I ÀMBIT D'APLICACIÓ.....	8
1.3.1. Autoritats de Certificació .....	8
1.3.2. Autoritats de Registre .....	8
1.3.3. Entitats Finals .....	8
1.3.4. Àmbit d'aplicació .....	9
1.4. DADES DE CONTACTE.....	9
1.4.1. Persona de Contacte.....	10
1.4.2. Determinació de l'adequació de la CPS a la Política.....	10
<b>2. CLÀUSULES GENERALS .....</b>	<b>11</b>
2.1. OBLIGACIONS.....	11
2.1.1. Obligacions de la CA.....	11
2.1.2. Obligacions de la RA.....	11
2.1.3. Obligacions dels Subscriptors .....	11
2.1.4. Obligacions de les parts confiants.....	11
2.1.5. Obligacions del repositori .....	11
2.2. RESPONSABILITAT .....	11
2.2.1. Responsabilitat de la CA .....	11
2.2.2. Responsabilitat de la RA.....	12
2.3. RESPONSABILITAT FINANCERA .....	12
2.3.1. Indemnització a les parts confiants .....	12
2.3.2. Relacions fiduciàries .....	12
2.3.3. Processos administratius.....	12
2.4. INTERPRETACIÓ I EXECUCIÓ.....	12
2.4.1. Lleis governamentals.....	12
2.4.2. Extinció, subsistència, fusió i notificació.....	12
2.4.3. Procediments de resolució de disputes .....	12
2.5. TARIFES.....	13
2.5.1. Tarifes d'emissió de certificat o renovació.....	13
2.5.2. Tarifes d'accés als certificats .....	13
2.5.3. Tarifes d'accés a la informació d'estat o revocació.....	13
2.5.4. Tarifes d'altres servicis com a informació de polítiques .....	13
2.5.5. Política de reintegraments.....	13
2.6. PUBLICACIÓ I REPOSITORIS .....	13
2.6.1. Publicació d'informació de la CA .....	13

2.6.2.	<i>Freqüència de publicació</i> .....	13
2.6.3.	<i>Controls d'accés</i> .....	14
2.6.4.	<i>Repositoris</i> .....	14
2.7.	CONTROL DE CONFORMITAT .....	14
2.7.1.	<i>Freqüència dels controls de conformitat per a cada entitat</i> .....	14
2.7.2.	<i>Identificació/qualificació de l'auditor</i> .....	14
2.7.3.	<i>Relació entre l'auditor i l'entitat auditada</i> .....	14
2.7.4.	<i>Tòpics coberts pel control de conformitat</i> .....	14
2.7.5.	<i>Accions que s'han de prendre com a resultat d'una deficiència</i> .....	14
2.7.6.	<i>Comunicació de resultats</i> .....	14
2.8.	POLÍTICA DE CONFIDENCIALITAT .....	15
2.8.1.	<i>Tipus d'informació que s'ha de mantindre confidencial</i> .....	15
2.8.2.	<i>Tipus d'informació no considerada confidencial</i> .....	15
2.8.3.	<i>Divulgació d'informació de revocació/suspensió de certificats</i> .....	15
2.8.4.	<i>Enviament a l'autoritat judicial i/o policial</i> .....	15
2.8.5.	<i>Publicació com a part d'un descobriment civil</i> .....	15
2.8.6.	<i>Divulgació a petició del propietari</i> .....	15
2.8.7.	<i>Altres circumstàncies de publicació d'informació</i> .....	15
2.9.	DRETS DE PROPIETAT INTEL·LECTUAL .....	15
<b>3.</b>	<b>IDENTIFICACIÓ I AUTENTIFICACIÓ</b> .....	<b>16</b>
3.1.	REGISTRE INICIAL .....	16
3.1.1.	<i>Tipus de noms</i> .....	16
3.1.2.	<i>Necessitat dels noms de ser significatius</i> .....	16
3.1.3.	<i>Regles per a interpretar diversos formats de noms</i> .....	16
3.1.4.	<i>Unicitat dels noms</i> .....	16
3.1.5.	<i>Procediments de resolució de disputes de noms</i> .....	16
3.1.6.	<i>Reconeixement, autenticació i funció de les marques registrades</i> .....	16
3.1.7.	<i>Mètodes de prova de possessió de la clau privada</i> .....	16
3.1.8.	<i>Autenticació de la identitat d'una organització</i> .....	16
3.1.9.	<i>Autenticació de la identitat d'un individu</i> .....	17
3.2.	RENOVACIÓ RUTINÀRIA DE LA CLAU .....	17
3.3.	RENOVACIÓ DE CLAU DESPRÉS D'UNA REVOCACIÓ – CLAU NO COMPROMESA .....	17
3.4.	SOL·LICITUD DE REVOCACIÓ .....	17
<b>4.</b>	<b>REQUERIMENTS OPERACIONALS</b> .....	<b>18</b>
4.1.	SOL·LICITUD DE CERTIFICATS .....	18
4.2.	EMISSIÓ DE CERTIFICATS .....	18
4.3.	ACCEPTACIÓ DE CERTIFICATS .....	19
4.4.	SUSPENSIÓ I REVOCACIÓ DE CERTIFICATS .....	19
4.4.1.	<i>Circumstàncies per a la revocació</i> .....	19

4.4.2.	<i>Qui pot sol·licitar la revocació</i> .....	19
4.4.3.	<i>Procediment de sol·licitud de revocació</i> .....	19
4.4.4.	<i>Període de gràcia de la sol·licitud de revocació</i> .....	21
4.4.5.	<i>Circumstàncies per a la suspensió</i> .....	21
4.4.6.	<i>Qui pot sol·licitar la suspensió</i> .....	21
4.4.7.	<i>Procediment per a la sol·licitud de suspensió</i> .....	21
4.4.8.	<i>Límits del període de suspensió</i> .....	21
4.4.9.	<i>Freqüència d'emissió de CRLs (si és aplicable)</i> .....	21
4.4.10.	<i>Requisits de comprovació de CRLs</i> .....	21
4.4.11.	<i>Disponibilitat de comprovació on-line de revocació/estat</i> .....	21
4.4.12.	<i>Requisits de comprovació on-line de revocació</i> .....	21
4.4.13.	<i>Altres formes de divulgació de revocació disponibles</i> .....	22
4.4.14.	<i>Requisits de comprovació per a altres formes de divulgació de revocació</i> .....	22
4.4.15.	<i>Requisits especials de renovació de claus compromeses</i> .....	22
4.5.	<b>PROCEDIMENTS DE CONTROL DE SEGURETAT</b> .....	22
4.5.1.	<i>Tipus d'esdeveniment registrats</i> .....	22
4.5.2.	<i>Freqüència de processat de logs</i> .....	22
4.5.3.	<i>Període de retenció per als logs d'auditoria</i> .....	22
4.5.4.	<i>Protecció dels logs d'auditoria</i> .....	22
4.5.5.	<i>Procediments de backup dels logs d'auditoria</i> .....	22
4.5.6.	<i>Sistema de recollida d'informació d'auditoria (intern vs extern)</i> .....	23
4.5.7.	<i>Notificació al subjecte causa de l'esdeveniment</i> .....	23
4.5.8.	<i>Anàlisi de vulnerabilitats</i> .....	23
4.6.	<b>ARXIU DE REGISTRES</b> .....	23
4.6.1.	<i>Tipus d'esdeveniments registrats</i> .....	23
4.6.2.	<i>Període de retenció per a l'arxiu</i> .....	23
4.6.3.	<i>Protecció de l'arxiu</i> .....	23
4.6.4.	<i>Procediments de backup de l'arxiu</i> .....	23
4.6.5.	<i>Requeriments per al segellat de temps dels registres</i> .....	23
4.6.6.	<i>Sistema de recollida d'informació d'auditoria (intern vs extern)</i> .....	24
4.6.7.	<i>Procediments per a obtenir i verificar informació arxivada</i> .....	24
4.7.	<b>CANVI DE CLAU</b> .....	24
4.8.	<b>RECUPERACIÓ EN CAS DE COMPROMÍS D'UNA CLAU O UN DESASTRE</b> .....	24
4.8.1.	<i>Alteració dels recursos maquinari, programari i/o dades</i> .....	24
4.8.2.	<i>La clau pública d'una entitat es revoca</i> .....	24
4.8.3.	<i>La clau d'una entitat es compromet</i> .....	24
4.8.4.	<i>Instal·lació de seguretat després d'un desastre natural o altre tipus de desastre</i> .....	24
4.9.	<b>CESSAMENT D'UNA CA</b> .....	24
<b>5.</b>	<b>CONTROLS DE SEGURETAT FÍSICA, PROCEDIMENTAL I DE PERSONAL</b> .....	<b>25</b>
5.1.	<b>CONTROLS DE SEGURETAT FÍSICA</b> .....	<b>25</b>

5.1.1.	Ubicació i construcció.....	25
5.1.2.	Accés físic.....	25
5.1.3.	Alimentació elèctrica i aire condicionat.....	25
5.1.4.	Exposició a l'aigua.....	25
5.1.5.	Protecció i prevenció d'incendis.....	25
5.1.6.	Sistema d'emmagatzematge.....	25
5.1.7.	Eliminació de residus.....	25
5.1.8.	Backup remot.....	26
5.2.	CONTROLS PROCEDIMENTALS.....	26
5.2.1.	Papers de confiança.....	26
5.2.2.	Nombre de persones requerides per tasca.....	26
5.2.3.	Identificació i autenticació per cada paper.....	26
5.3.	CONTROLS DE SEGURETAT DE PERSONAL.....	26
5.3.1.	Requeriments d'antecedents, qualificació, experiència i acreditació.....	26
5.3.2.	Procediments de comprovació d'antecedents.....	26
5.3.3.	Requeriments de formació.....	26
5.3.4.	Requeriments i freqüència de l'actualització de la formació.....	26
5.3.5.	Freqüència i seqüència de rotació de tasques.....	27
5.3.6.	Sancions per accions no autoritzades.....	27
5.3.7.	Requeriments de contractació de personal.....	27
5.3.8.	Documentació proporcionada al personal.....	27
<b>6.</b>	<b>CONTROLS DE SEGURETAT TÈCNICA.....</b>	<b>28</b>
6.1.	GENERACIÓ I INSTAL·LACIÓ DEL PARELL DE CLAUS.....	28
6.1.1.	Generació del parell de claus.....	28
6.1.2.	Entrega de la clau privada a l'entitat.....	28
6.1.3.	Entrega de la clau pública a l'emissor del certificat.....	28
6.1.4.	Entrega de la clau pública de la CA als usuaris.....	28
6.1.5.	Grandària de les claus.....	28
6.1.6.	Paràmetres de generació de la clau pública.....	28
6.1.7.	Comprovació de la qualitat dels paràmetres.....	28
6.1.8.	Maquinari/programari de generació de claus.....	29
6.1.9.	Finalitats de l'ús de la clau.....	29
6.2.	PROTECCIÓ DE LA CLAU PRIVADA.....	29
6.2.1.	Estàndards per als mòduls criptogràfics.....	29
6.2.2.	Control multipersona (n de entre m) de la clau privada.....	29
6.2.3.	Custòdia de la clau privada.....	29
6.2.4.	Còpia de seguretat de la clau privada.....	30
6.2.5.	Arxiu de la clau privada.....	30
6.2.6.	Introducció de la clau privada en el mòdul criptogràfic.....	30
6.2.7.	Mètode d'activació de la clau privada.....	30

6.2.8.	<i>Mètode de desactivació de la clau privada</i> .....	30
6.2.9.	<i>Mètode de destrucció de la clau privada</i> .....	30
6.3.	ALTRES ASPECTES DE LA GESTIÓ DEL PARELL DE CLAUS .....	30
6.3.1.	<i>Arxiu de la clau pública</i> .....	30
6.3.2.	<i>Període d'ús per a les claus públiques i privades</i> .....	31
6.4.	DADES D'ACTIVACIÓ.....	31
6.4.1.	<i>Generació i activació de les dades d'activació</i> .....	31
6.4.2.	<i>Protecció de les dades d'activació</i> .....	31
6.4.3.	<i>Altres aspectes de les dades d'activació</i> .....	31
6.5.	CONTROLS DE SEGURETAT INFORMÀTICA.....	31
6.5.1.	<i>Requeriments tècnics de seguretat informàtica específics</i> .....	31
6.5.2.	<i>Valoració de la seguretat informàtica</i> .....	32
6.6.	CONTROLS DE SEGURETAT DEL CICLE DE VIDA .....	32
6.6.1.	<i>Controls de desenrotllament del sistema</i> .....	32
6.6.2.	<i>Controls de gestió de la seguretat</i> .....	32
6.6.3.	<i>Avaluació de la seguretat del cicle de vida</i> .....	32
6.7.	CONTROLS DE SEGURETAT DE LA XÀRCIA .....	32
6.8.	CONTROLS D'ENGINYERIA DELS MÒDULS CRIPTOGRÀFICS.....	32
<b>7.</b>	<b>PERFILS DE CERTIFICAT I CRL.....</b>	<b>33</b>
7.1.	PERFIL DE CERTIFICAT .....	33
7.1.1.	<i>Número de versió</i> .....	33
7.1.2.	<i>Extensions del certificat</i> .....	33
7.1.3.	<i>Identificadors d'objecte (OID) dels algorismes</i> .....	34
7.1.4.	<i>Formats de noms</i> .....	34
7.1.5.	<i>Restriccions dels noms</i> .....	34
7.1.6.	<i>Identificador d'objecte (OID) de la Política de certificació</i> .....	34
7.1.7.	<i>Ús de l'extensió "Policy Constraints"</i> .....	35
7.1.8.	<i>Sintaxi i semàntica dels qualificadors de política</i> .....	35
7.1.9.	<i>Tractament semàntic per a l'extensió crítica "Certificate Policy"</i> .....	35
7.2.	PERFIL DE CRL .....	35
7.2.1.	<i>Número de versió</i> .....	35
7.2.2.	<i>CRL i extensions</i> .....	35
<b>8.</b>	<b>ESPECIFICACIÓ DE L'ADMINISTRACIÓ .....</b>	<b>36</b>
8.1.	PROCEDIMENTS D'ESPECIFICACIÓ DE CANVIS.....	36
8.2.	PROCEDIMENTS DE PUBLICACIÓ I NOTIFICACIÓ .....	36
8.3.	PROCEDIMENTS D'APROVACIÓ DE LA CPS .....	36
<b>ANNEX I</b>	<b>.....</b>	<b>37</b>

## 1. INTRODUCCIÓ

Esta Política de Certificació s'adequa amb l'especificació del RFC 2527 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" proposat per S. Chokhani i W. Ford, de l'Internet Engineering Task Force (IETF), per a este tipus de documents. S'inclouen totes les seccions de l'especificació a fi de dotar de consistència el document. Quan no existisca cap disposició o limitació respecte d'una secció apareixerà la frase "No estipulat" continguda en la dita secció.

Esta Política de Certificació assumix que el lector coneix els conceptes bàsics de PKI, certificat i firma digital, en cas contrari es recomana al lector que es forme en el coneixement dels anteriors conceptes abans de continuar amb la lectura d'este document.

### 1.1. Vista General

Esta Política de certificació conté les regles a les quals se subjecta l'ús dels certificats definits en esta política. Es descriuen els papers, responsabilitats i relacions entre l'usuari final i la PKI i les regles de sol·licitud, adquisició gestió i ús dels certificats.

La Política de Certificació referida en este document s'utilitzarà per a firma digital i xifrat de missatges de correu electrònic S/MIME i per a firma de documents, formularis i autenticació d'usuari en aquelles aplicacions i servicis amb capacitats de PKI pertanyents a l'àmbit de la Generalitat Valenciana, a entitats i organismes vinculats a ella, o a alguna Administració Pública o Corporativa amb la qual haja establert conveni de certificació, que siguen autoritzades per l'Autoritat d'Aprovació de Polítiques de PKIGVA.

L'entitat involucrada en l'ús dels certificats emesos davall l'empar de la present política és la pròpia Generalitat Valenciana així com les entitats i organismes vinculats a ella, i les Administracions Públiques o Corporatives amb les quals haja establert conveni de certificació.

### 1.2. Identificació

Nom de la política	Certificats per a Correu i Aplicacions Segures
Qualificador de la política	L'ús d'este certificat està restringit a correu segur i aplicacions pertanyents a la Generalitat Valenciana, a entitats i organismes vinculats a ella, o a alguna Administració Pública amb la qual haja establert conveni de certificació.
Versió de la política	1.0
Estat de la política	Vigent
Referència de la política / OID (Object Identifier)	1.3.6.1.4.1.8149.3.2.1.2.1.0

<b>e-firmagv</b>	<b>Política de certificació: Certificats per a Correu i Aplicacions Segures</b>
Data d'emissió	27 de gener de 2003
Data d'expiració	No aplicable.
CPS relacionada	Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana. Versió 1.0.  OID: 1.3.6.1.4.1.8149.2.1.0  Disponible en <a href="http://www.pki.gva.es/cps">http://www.pki.gva.es/cps</a>
Localització	Esta Política de certificació es pot trobar en: <a href="http://www.pki.gva.es/cps/pol2101.htm">http://www.pki.gva.es/cps/pol2101.htm</a>

## 1.3. Comunitat i Àmbit d'aplicació

### 1.3.1. Autoritats de Certificació

La CA que pot emetre certificats d'acord amb esta política és la "CAGVA" pertanyent a la PKI de la Generalitat Valenciana.

### 1.3.2. Autoritats de Registre

Les Autoritats de Registre que gestionen les sol·licituds de certificats definits en esta política estaran definides en el document "Àmbits de Certificació i Punts de Registre", que es pot consultar en <http://www.pki.gva.es/cp02/acpr.htm>.

### 1.3.3. Entitats Finals

#### 1.3.3.1. Subscriptors

El grup d'usuaris que poden sol·licitar certificats definits per esta política està format per les persones que encaixen en algun dels àmbits de certificat, determinats per la Direcció General de Telecomunicacions i Modernització, a través del document "Àmbits de Certificació i Punts de Registre", ubicat en <http://www.pki.gva.es/cp02/acpr.htm>.

El suport de claus i certificats serà smart card, disquet o CDROM cosa que dependrà del perfil dels sol·licitants i de les aplicacions a les quals es destine el seu ús més freqüent.

Es limita el dret de sol·licitud de certificats definit en esta Política de Certificat a persones físiques. No s'acceptaran sol·licituds de certificat realitzades en nom de persones jurídiques, entitats o organitzacions.

#### 1.3.3.2. Parts confiants

Es limita el dret a confiar en els certificats emesos conforme a esta política a:

- Els usuaris de clients de correu electrònic S/MIME en l'àmbit de la verificació de la identitat de l'emissor de missatges de correu electrònic i del xifrat d'estos.
- Les aplicacions i servicis pertanyents a la Generalitat Valenciana, a alguna de les entitats o organitzacions vinculades a la Generalitat o a Administracions Públiques o Corporatives amb les quals s'haja firmat conveni de certificació, que siguen autoritzades per l'Autoritat d'Aprovació de Polítiques de PKIGVA en l'àmbit de firma i verificació de la firma de documents i formularis, xifrat de documents i autenticació d'usuaris.
- Les aplicacions i servicis que, sense pertànyer a la Generalitat Valenciana, entitats o organismes vinculats a ella, ni a Administracions Públiques ni Corporatives amb les quals s'haja establert conveni de certificació, s'empren en relacions entre ciutadans, empreses o altres Administracions Públiques amb la Generalitat Valenciana, entitats o organismes vinculats a ella o Administracions Públiques amb què s'haja establert conveni de certificació.

#### 1.3.4. Àmbit d'aplicació

##### 1.3.4.1. Usos Permesos

Els certificats emesos per la PKI de la Generalitat Valenciana davall esta Política de Certificació, poden utilitzar-se per a la firma digital i xifrat de missatges de correu electrònic S/MIME. Així mateix, poden utilitzar-se com a mecanisme d'identificació davant de servicis i per a la firma electrònica de documents.

##### 1.3.4.2. Usos Restringits

Els certificats emesos per la PKI de la Generalitat Valenciana davall esta Política de Certificació poden ser utilitzats, de forma restringida pels usuaris d'aplicacions i servicis pertanyents a l'àmbit de la Generalitat Valenciana o al d'altres Administracions Públiques o Corporatives amb les quals s'haja establert conveni de certificació, per a la firma o xifrat de documents i formularis, la comprovació de firma i l'autenticació d'usuari.

##### 1.3.4.3. Usos Prohibits

Està prohibit l'ús dels certificats emesos per la PKI de la Generalitat Valenciana davall esta Política de certificació per a qualsevol ús no especificat pels punts "1.3.4.1 Usos Permesos" i "1.3.4.2 Usos Restringits" del present document.

## 1.4. Dades de contacte

Esta Política de Certificació és propietat de la "Direcció General de Telecomunicacions i Modernització".

Nom ..... *Direcció General de Telecomunicacions i Modernització*  
Adreça d'email ..... [dgtm@gva.es](mailto:dgtm@gva.es)  
Adreça ..... *C/ Colom, 66 – 46004 València (Spain)*  
Número de telèfon ..... *+34-96-196 1061*  
Número de fax ..... *+34-96-196 1001*

Esta Política de Certificació està administrada per l'Autoritat d'Aprovació de Polítiques (AAP) de la PKI de la Generalitat Valenciana.

Nom ..... *AAP PKI de la Generalitat Valenciana*  
Adreça d'email ..... [Aap@pki.gva.es](mailto:Aap@pki.gva.es)  
Adreça ..... *C/ Colom, 66 – 46004 València (Spain)*  
Número de telèfon ..... *+34-902-482-481*  
Número de fax ..... *+34- 96 196-1001*

#### 1.4.1. Persona de Contacte

Per a més informació relacionada amb la present Política de Certificació, per favor contacte amb:

Nom ..... *Projecte e-firmaGV*  
Adreça d'email ..... [firma@gva.es](mailto:firma@gva.es)  
Adreça ..... *C/ Colom, 66 – 46004 València (Spain)*  
Número de telèfon ..... *+34-902 482 481*  
Número de fax ..... *+34- 96 196-1001*

#### 1.4.2. Determinació de l'adequació de la CPS a la Política

L'Autoritat d'Aprovació de Polítiques (AAP) de la PKI de la Generalitat Valenciana és l'entitat que determina l'adequació d'esta política a la CPS de la seua PKI.

## 2. Clàusules Generals

### 2.1. Obligacions

#### 2.1.1. Obligacions de la CA

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

Adicionalment, les CAs especificades en el punt 1.3.1 "Autoritats de Certificació" estan obligades a:

- Adaptar les seues operacions per a complir allò que s'ha estipulat per esta Política de Certificació.
- Emetre certificats de conformitat amb esta Política de Certificació.

#### 2.1.2. Obligacions de la RA

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 2.1.3. Obligacions dels Subscriptors

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 2.1.4. Obligacions de les parts confiants

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 2.1.5. Obligacions del repositori

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.2. Responsabilitat

#### 2.2.1. Responsabilitat de la CA

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

## 2.2.2. Responsabilitat de la RA

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

## 2.3. Responsabilitat Financera

### 2.3.1. Indemnització a les parts confiants

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.3.2. Relacions fiduciàries

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.3.3. Processos administratius

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

## 2.4. Interpretació i Execució

### 2.4.1. Lleis governamentals

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.4.2. Extinció, subsistència, fusió i notificació

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.4.3. Procediments de resolució de disputes

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

## 2.5. Tarifes

### 2.5.1. Tarifes d'emissió de certificat o renovació

No s'aplica cap tarifa sobre l'emissió o renovació de certificats davall l'empara de la present Política de certificació.

### 2.5.2. Tarifes d'accés als certificats

L'accés als certificats emesos davall esta política, donada la seua naturalesa pública, és lliure i gratuït i per tant no hi ha cap tarifa d'aplicació sobre este.

### 2.5.3. Tarifes d'accés a la informació d'estat o revocació

L'accés a la informació d'estat o revocació dels certificat és lliure i gratuïta i per tant no s'aplicarà cap tarifa.

### 2.5.4. Tarifes d'altres servicis com a informació de polítiques

No s'aplicarà cap tarifa pel servici d'informació sobre esta política ni per cap altre servici adicional del qual es tinga coneixement en el moment de la redacció del present document.

### 2.5.5. Política de reintegraments

Si no existix cap tarifa d'aplicació per a esta Política de certificació no és necessària cap política de reintegraments.

## 2.6. Publicació i Repositoris

### 2.6.1. Publicació d'informació de la CA

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

La present Política de Certificació és pública i es troba disponible, en format PDF, en la ubicació especificada en l'apartat localització del punt "1.2 Identificació" del present document.

### 2.6.2. Freqüència de publicació

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.6.3. Controls d'accés

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.6.4. Repositoris

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

## 2.7. Control de conformitat

### 2.7.1. Freqüència dels controls de conformitat per a cada entitat

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.7.2. Identificació/qualificació de l'auditor

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.7.3. Relació entre l'auditor i l'entitat auditada

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.7.4. Tòpics coberts pel control de conformitat

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.7.5. Accions que s'han de prendre com a resultat d'una deficiència

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.7.6. Comunicació de resultats

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

## 2.8. Política de Confidencialitat

### 2.8.1. Tipus d'informació que s'ha de mantindre confidencial

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.8.2. Tipus d'informació no considerada confidencial

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.8.3. Divulgació d'informació de revocació/suspensió de certificats

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.8.4. Enviament a l'autoritat judicial i/o policial

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.8.5. Publicació com a part d'un descobriment civil

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.8.6. Divulgació a petició del propietari

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 2.8.7. Altres circumstàncies de publicació d'informació

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

## 2.9. Drets de propietat intel·lectual

Tots els drets de propietat intel·lectual de la present Política de Certificació pertanyen i romandran en propietat de la Generalitat Valenciana.

## 3. IDENTIFICACIÓ I AUTENTIFICACIÓ

### 3.1. Registre inicial

#### 3.1.1. Tipus de noms

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 3.1.2. Necessitat dels noms de ser significatius

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 3.1.3. Regles per a interpretar diversos formats de noms

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 3.1.4. Unicitat dels noms

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 3.1.5. Procediments de resolució de disputes de noms

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 3.1.6. Reconeixement, autenticació i funció de les marques registrades

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 3.1.7. Mètodes de prova de possessió de la clau privada

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 3.1.8. Autenticació de la identitat d'una organització

El dret de sol·licitud de certificats definit en la present Política de Certificació es troba limitat a persones físiques. No s'acceptaran sol·licituds de certificat realitzades en nom de persones jurídiques, entitats o organitzacions. Per tant, no es considera necessària la identificació de cap organització.

### 3.1.9. Autenticació de la identitat d'un individu

L'autenticació de la identitat del sol·licitant d'un certificat es realitzarà per mitjà de la presentació del Document Nacional d'Identitat (DNI) del sol·licitant davant de l'Operador de Registre en el moment d'arreglar el certificat.

És necessari destacar que en este tipus de certificats s'inclou l'adreça de correu electrònic del subscriptor com a element necessari per a suportar el protocol S/MIME, però que PKIGVA no garantix que esta adreça de correu estiga vinculada amb el subscriptor del certificat, per la qual cosa la confiança o no que esta adreça siga la del titular del certificat correspon únicament a la part confiant. PKIGVA únicament garantix que l'adreça de correu que consta en el certificat va ser l'aportada pel subscriptor en el moment de la formalització de la seua sol·licitud i/o que consta com vinculada al titular en les bases de dades de personal de la Generalitat Valenciana.

## 3.2. Renovació rutinària de la clau

L'autenticació per a la renovació del certificat es pot realitzar utilitzant les tècniques per a l'autenticació i identificació inicial o bé utilitzant sol·licituds firmades digitalment o altres sistemes en els quals quede perfectament identificat el sol·licitant de la renovació, per mitjà del certificat original que es pretén renovar, sempre que este no haja vençut ni s'haja procedit a la seua revocació.

## 3.3. Renovació de clau després d'una revocació – Clau no compromesa

La política d'identificació i autenticació per a la renovació d'un certificat després d'una revocació sense compromís de la clau serà la mateixa que per al registre inicial.

## 3.4. Sol·licitud de revocació

La política d'identificació per a les sol·licituds de revocació és la mateixa que per al registre inicial. La política d'autenticació acceptarà sol·licituds de revocació firmades digitalment pel subscriptor del certificat.

PKIGVA o qualsevol de les entitats que la componen poden sol·licitar d'ofici la revocació d'un certificat si tingueren el coneixement o sospita del compromís de la clau privada del subscriptor, o qualsevol altre fet que recomanara mamprendre la dita acció.

## 4. REQUERIMENTS OPERACIONALS

### 4.1. Sol·licitud de certificats

El sol·licitant d'un certificat acollit a la present Política de Certificació haurà d'omplir una sol·licitud de certificat a través d'un formulari web ubicat en <http://www.pki.gva.es>, apartat "Gestió de Certificats", subapartat "Gestió de Certificats per a Correu i Aplicacions Segures".

Una vegada omplert el formulari de sol·licitud, este s'envia, automàticament, a l'Autoritat de Registre de PKIGVA.

És atribució de l'Autoritat de Registre de PKIGVA el fet de determinar l'adequació d'un tipus de certificat a les característiques del sol·licitant, segons les disposicions de la Política de Certificació aplicable, i d'esta manera accedir o denegar la gestió de la sol·licitud de certificat d'este.

En el cas de denegació de la sol·licitud de certificat per part de l'Operador de l'Autoritat de Registre, el sol·licitant rebrà un correu electrònic en l'adreça que va fer constar en la seua sol·licitud, i li informará dels motius del rebuig d'esta.

Les sol·licituds de certificat una vegada acceptades són enviades a l'Autoritat de Certificat per l'Autoritat de Registre de PKIGVA.

### 4.2. Emissió de certificats

L'emissió del certificat tindrà lloc una vegada que PKIGVA haja dut a terme les verificacions necessàries per a validar la sol·licitud de certificat. El mecanisme pel qual es determina la naturalesa i la forma de realitzar dites comprovacions és esta Política de Certificació.

Després de l'emissió del certificat l'Autoritat de Registre ho notificarà al subscriptor d'este per mitjà de la presentació d'una pàgina html de retorn de sol·licitud o l'enviament d'un correu electrònic firmat a l'adreça que figure en la sol·licitud, en el qual a més se li informará sobre l'adreça de l'oficina –Punt de Registre d'Usuari–, en la qual ha d'arreglar el certificat, per a això haurà de presentar document acreditatiu d'identitat (DNI, passaport o carta de residència) i firmar el Contracte de Certificació.

El Contracte de Certificació és un document que ha de ser firmat manualment pel sol·licitant i per la persona destinada al Registre d'usuaris, i la finalitat del qual és vincular la persona que s'ha de certificar amb l'acció de la sol·licitud, amb el coneixement de les normes d'ús i amb la veracitat de les dades presentades. El formulari del Contracte de Certificació s'arregla en l'Annex I.

### 4.3. Acceptació de certificats

El subscriptor demostra la seua acceptació del certificat amb la firma del Contracte de Certificació i l'arreglada d'este.

### 4.4. Suspensió i revocació de certificats

#### 4.4.1. Circumstàncies per a la revocació

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.4.2. Qui pot sol·licitar la revocació

La revocació d'un certificat es pot iniciar tant pel subscriptor d'este com per part de PKIGVA.

Els subscriptors de certificats poden sol·licitar la seua revocació per qualsevol raó o sense cap raó i han de sol·licitar la revocació davall les condicions especificades en el següent apartat.

#### 4.4.3. Procediment de sol·licitud de revocació

Es determina que:

- S'acceptaran sol·licituds de revocació remotes si estan firmades digitalment amb un certificat de PKIGVA i presencials si es complixen els requisits d'identificació de l'usuari establits per al registre inicial (presentació en algun Punt de Registre d'Usuari i presentació de DNI, passaport o carta de residència).
- En el cas de produir-se una sol·licitud de revocació sense possible verificació de la identitat del sol·licitant (telefònica, correu electrònic sense firma digital, etc.), es procedirà a la suspensió del certificat durant un termini màxim de 15 dies naturals, durant els quals es procedirà a verificar la veracitat de la sol·licitud. En el cas de no poder verificar la falsedat de la sol·licitud en el dit termini, es procedirà a la revocació del certificat. És important assenyalar que el certificat no serà utilitzable des del moment del processament de la sol·licitud.
- Després de la revocació del certificat el subscriptor d'este haurà de destruir la clau privada que es corresponga amb la pública continguda en el certificat.

Una sol·licitud de revocació tant si es realitza en paper o de forma electrònica (ex.: correu electrònic) ha de contindre la informació següent:

Sol·licitud de revocació de certificat

Data : \_\_\_\_\_

**Secció 1 - Detalls del certificat (si es coneixen)**

ID certificat: .....

Número de sèrie del certificat: .....

Tipus de certificat: .....

**Secció 2 - Dades del subscriptor del certificat**

Nom: .....

NIF: .....

**Secció 3 - Motius de la revocació \***

.....  
.....  
.....  
.....  
.....

\* La simple voluntat de revocació del subscriptor del certificat és un motiu vàlid per a la sol·licitud d'esta.

**Secció 4 - Autorització**

Autoritzat per:  Subscriptor del certificat  
 Tercera part autoritzada (especificar)

.....

Firma: .....

#### 4.4.4. Període de gràcia de la sol·licitud de revocació

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.4.5. Circumstàncies per a la suspensió

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.4.6. Qui pot sol·licitar la suspensió

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.4.7. Procediment per a la sol·licitud de suspensió

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.4.8. Límits del període de suspensió

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.4.9. Freqüència d'emissió de CRLs (si és aplicable)

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.4.10. Requisits de comprovació de CRLs

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.4.11. Disponibilitat de comprovació on-line de revocació/estat

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.4.12. Requisits de comprovació on-line de revocació

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.4.13. Altres formes de divulgació de revocació disponibles

A més de la consulta de revocats per mitjà de Llistes de Certificats Revocats (CRL) i per mitjà del servici OCSP, és possible comprovar la validesa dels certificats per mitjà d'un formulari web que, a partir d'una adreça de correu electrònic, torna els certificats vinculats a eixa adreça i l'estat d'estos. Este formulari es troba en el lloc web de l'Autoritat de Certificat (<http://www.pki.gva.es>).

#### 4.4.14. Requisits de comprovació per a altres formes de divulgació de revocació

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.4.15. Requisits especials de renovació de claus compromeses

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 4.5. Procediments de Control de Seguretat

#### 4.5.1. Tipus d'esdeveniment registrats

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.5.2. Freqüència de processat de logs

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.5.3. Període de retenció per als logs d'auditoria

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.5.4. Protecció dels logs d'auditoria

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.5.5. Procediments de backup dels logs d'auditoria

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.5.6. Sistema de recollida d'informació d'auditoria (intern vs extern)

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.5.7. Notificació al subjecte causa de l'esdeveniment

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.5.8. Anàlisi de vulnerabilitats

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 4.6. Arxiu de registres

#### 4.6.1. Tipus d'esdeveniments registrats

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.6.2. Període de retenció per a l'arxiu

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.6.3. Protecció de l'arxiu

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.6.4. Procediments de backup de l'arxiu

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 4.6.5. Requeriments per al segellat de temps dels registres

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### **4.6.6. Sistema de recollida d'informació d'auditoria (intern vs extern)**

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### **4.6.7. Procediments per a obtindre i verificar informació arxivada**

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### **4.7. Canvi de Clau**

No estipulat.

### **4.8. Recuperació en cas de compromís d'una clau o un desastre**

#### **4.8.1. Alteració dels recursos maquinari, programari i/o dades**

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### **4.8.2. La clau pública d'una entitat es revoca**

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### **4.8.3. La clau d'una entitat es compromet**

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### **4.8.4. Instal·lació de seguretat després d'un desastre natural o altre tipus de desastre**

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### **4.9. Cessament d'una CA**

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

## 5. CONTROLS DE SEGURETAT FÍSICA, PROCEDIMENTAL I DE PERSONAL

### 5.1. Controls de Seguretat Física

#### 5.1.1. Ubicació i construcció

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 5.1.2. Accés físic

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 5.1.3. Alimentació elèctrica i aire condicionat

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 5.1.4. Exposició a l'aigua

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 5.1.5. Protecció i prevenció d'incendis

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 5.1.6. Sistema d'emmagatzematge

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 5.1.7. Eliminació de residus

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 5.1.8. Backup remot

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 5.2. Controls procedimentals

#### 5.2.1. Papers de confiança

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 5.2.2. Nombre de persones requerides per tasca

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 5.2.3. Identificació i autenticació per cada paper

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 5.3. Controls de seguretat de personal

#### 5.3.1. Requeriments d'antecedents, qualificació, experiència i acreditació

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 5.3.2. Procediments de comprovació d'antecedents

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 5.3.3. Requeriments de formació

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 5.3.4. Requeriments i freqüència de l'actualització de la formació

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 5.3.5. Freqüència i seqüència de rotació de tasques

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 5.3.6. Sancions per accions no autoritzades

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 5.3.7. Requeriments de contractació de personal

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 5.3.8. Documentació proporcionada al personal

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

## 6. CONTROLS DE SEGURETAT TÈCNICA

### 6.1. Generació i instal·lació del parell de claus

#### 6.1.1. Generació del parell de claus

El parell de claus per als certificats emesos davall l'àmbit de la present Política de Certificació es generen per l'Autoritat de Certificació de la Generalitat Valenciana o en targeta criptogràfica de l'usuari.

#### 6.1.2. Entrega de la clau privada a l'entitat

La clau privada es troba continguda en la smart card que s'entrega al subscriptor amb el seu certificat en el moment que es registre.

En cas de suport disquet o CDRom, la clau privada es troba en el fitxer PKCS#12. Este fitxer conté les claus i el certificat d'usuari en un fitxer xifrat.

#### 6.1.3. Entrega de la clau pública a l'emissor del certificat

La clau pública que serà certificada és generada per l'Autoritat de Registre i entregada a l'Autoritat de Certificació per mitjà de l'enviament d'una sol·licitud de certificat en format PKCS#10, firmada digitalment per l'Operador de l'Autoritat de Registre.

#### 6.1.4. Entrega de la clau pública de la CA als usuaris

La clau pública de l'Autoritat de Certificació que emet el certificat del subscriptor es poden descarregar del lloc web <http://www.pki.gva.es>.

Adicionalment les claus públiques de totes les CA's pertanyents a la jerarquia de confiança de PKIGVA es poden descarregar del lloc web <http://www.pki.gva.es>.

#### 6.1.5. Grandària de les claus

La grandària de les claus és de 1024 bits.

#### 6.1.6. Paràmetres de generació de la clau pública

No aplicable.

#### 6.1.7. Comprovació de la qualitat dels paràmetres

No aplicable.

### 6.1.8. Maquinari/programari de generació de claus

La generació de la clau es realitza en smart cards criptogràfiques en cas de suport smart card.

En el cas que el contingut del certificat i les claus siga disquet o CDROM, es generaran en un sistema pertanyent al nucli protegit de la PKI.

### 6.1.9. Finalitats de l'ús de la clau

La clau definida per la present política s'utilitzarà per a la verificació de la identitat dels usuaris davant d'aplicacions i servicis interns a l'àmbit de la Generalitat Valenciana. A més, esta clau s'emprarà amb el propòsit de proporcionar "Correu Segur". Per als certificats X.509 v3, este propòsit es definirà en el paràmetres de "Key Usage" i "Extended Key Usage" de la manera següent:

Key Usage:

- Digital Signature
- Data Encipherment
- Key Encipherment

Extended Key Usage

- Client Authentication

La definició detallada del perfil de certificat i els usos de les claus es troben en l'apartat 7 "Perfils de certificat i CRL" d'este document.

## 6.2. Protecció de la Clau Privada

### 6.2.1. Estàndards per als mòduls criptogràfics

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 6.2.2. Control multipersona (n de entre m) de la clau privada

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 6.2.3. Custòdia de la clau privada

No es custodien claus privades de firma dels subscriptors dels certificats definits per la present política. Sí es fa custòdia, de les claus vinculades als certificats de xifrat.

#### 6.2.4. Còpia de seguretat de la clau privada

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 6.2.5. Arxiu de la clau privada

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 6.2.6. Introducció de la clau privada en el mòdul criptogràfic

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

#### 6.2.7. Mètode d'activació de la clau privada

La clau privada del subscriptor s'activa per mitjà de la introducció del PIN de la smart card que la conté.

En el cas que el suport siga disquet o CDROM, l'activació de la clau privada es realitzarà a través de la introducció de la paraula de pas d'accés a esta clau, continguda en el fitxer PKCS#12.

#### 6.2.8. Mètode de desactivació de la clau privada

La desactivació de la clau privada del subscriptor s'aconsegueix per mitjà de l'extracció de la smartcard que la conté del lector PC/SC.

En el cas que el suport siga disquet o CDROM, la desactivació es realitzarà tancant l'aplicació que la utilitza o tancant el mòdul criptogràfic associat.

#### 6.2.9. Mètode de destrucció de la clau privada

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 6.3. Altres aspectes de la gestió del parell de claus

#### 6.3.1. Arxiu de la clau pública

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 6.3.2. Període d'ús per a les claus públiques i privades

Els certificats emesos a l'empar de la present política tenen una validesa de tres (3) anys.

El parell de claus utilitzat per a l'emissió dels certificats es crea per a cada emissió, i per tant també tenen una validesa de tres (3) anys.

## 6.4. Dades d'activació

### 6.4.1. Generació i activació de les dades d'activació

Les dades d'activació de la clau privada consisteixen en el PIN de la smart card que la conté i que es proporciona al subscriptor del certificat amb este.

La generació del PIN de la smart card es realitza en el moment en què esta s'inicia, i se li comunica la dada al subscriptor en el moment en què se li fa entrega. És responsabilitat i obligació del subscriptor la modificació d'eixe PIN preconfigurat per un del seu exclusiu coneixement de forma immediata a la recepció de la smart card i abans del seu primer ús.

En el cas que el suport siga disquet o CDRROM, es proporcionarà al subscriptor la paraula de pas d'accés a la clau privada o de protecció del fitxer que conté el PKCS#12. Igualment és responsabilitat i obligació del subscriptor la modificació d'eixa paraula de pas preconfigurada per una del seu exclusiu coneixement de forma immediata a la recepció del fitxer PKCS#12 i abans del seu primer ús.

### 6.4.2. Protecció de les dades d'activació

El subscriptor del certificat és el responsable de la protecció de les dades d'activació de la seua clau privada.

### 6.4.3. Altres aspectes de les dades d'activació

No estipulat.

## 6.5. Controls de Seguretat Informàtica

### 6.5.1. Requeriments tècnics de seguretat informàtica específics

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 6.5.2. Valoració de la seguretat informàtica

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

## 6.6. Controls de Seguretat del Cicle de Vida

### 6.6.1. Controls de desenrotllament del sistema

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 6.6.2. Controls de gestió de la seguretat

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 6.6.3. Avaluació de la seguretat del cicle de vida

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

## 6.7. Controls de Seguretat de la Xàrcia

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

## 6.8. Controls d'enginyeria dels mòduls criptogràfics

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

## 7. PERFILS DE CERTIFICAT I CRL

### 7.1. Perfil de Certificat

Esta política de certificació especifica l'ús de dos certificats distints per a firma digital i xifrat de dades. El perfil d'estos dos certificats és idèntic excepte en l'apartat 7.1.2 Extensions del certificat. En este punt s'especifica quan hi ha diferències entre estos dos certificats.

#### 7.1.1. Número de versió

La present política s'implementa sobre certificats X.509 versió 3 (X.509 v3).

#### 7.1.2. Extensions del certificat

Les extensions utilitzades pels certificats emesos davall l'empar de la present política són:

- Key Usage {joint-iso-itu-t(2) ds(5) certificateExtension(29) keyUsage(15)}

Marcada com a crítica i amb la següent combinació de valors:

- Per al certificat de firma:
  - Digital Signature
- Per al certificat de xifrat
  - Data Encipement
  - Key Encipement

- Extended Key Usage {joint-iso-itu-t(2) ds(5) certificateExtension(29) extKeyUsage(37)}

Marcada com a crítica i amb la següent combinació de valors:

Per als dos certificats

- Email Protection
- Client Autentication

- Certificate Policies. {joint-iso-itu-t(2) ds(5) certificateExtension(29) certificatePolicies(32)}

Marcada com a crítica i amb la següent combinació de valors:

- Policy OID: 1.3.6.1.4.1.8149.3.2.1.2.1.0
- Policy CPS Location: <http://pki.gva.es/cps/pol2101.htm>

- Policy Notice: L'ús d'este certificat està restringit a correu segur i aplicacions pertanyents a la Generalitat Valenciana, a entitats i organismes vinculats a ella, o a alguna Administració Pública amb la qual haja establert conveni de certificat. Este certificat s'ha emés com *Certificat Reconegut* d'acord amb el Reial Decret-Llei 14/1999, de 17 de setembre.
  
- Subject Alternative Name {joint-iso-itu-t(2) ds(5) certificateExtension(29) subjectAltName(17)}  
Marcada com a crítica i amb el valor:
  - Nombre RFC822: Adreça de correu electrònic del subscriptor.
  - Directory name: uid=*NIF*, cn=Nom|Primer cognom|Segon cognom
  
- CRL Distribution Point {joint-iso-itu-t(2) ds(5) certificateExtension(29) cRLDistributionPoints(31)}  
Marcada com a no crítica.

### 7.1.3. Identificadors d'objecte (OID) dels algoritmes

Identificador d'Objecte (OID) dels algoritmes Criptogràfics:

- md5withRSAEncryption (1.2.840.113549.1.1.4)
- SHA1withRSAEncryption (1.2.840.113549.1.1.5)

### 7.1.4. Formats de noms

Els certificats emesos davall la present política contenen el distinguished name X.500 de l'emissor i el subscriptor del certificat en els camps issuer name i subject name respectivament.

- Subject name: cn=*NOM COGNOM1 COGNOM2* – NIF:*nif*, ou=Ciutadans, o=Generalitat Valenciana, c=ES

El camp cn del subject name s'ompli obligatòriament en majúscules, prescindint d'accents i substituint la lletra "Ñ" per la "N" i la lletra "Ç" per la "C".

- Issuer name: cn=CAGVA, ou=PKIGVA, o=Generalitat Valenciana, c=ES

### 7.1.5. Restriccions dels noms

Els noms continguts en els certificats estan restringits a distinguished names X.500, únics i no ambigus.

### 7.1.6. Identificador d'objecte (OID) de la Política de certificació

L'identificador d'objecte definit per PKIGVA per a identificar la present política és el següent:

### 7.1.7. Ús de l'extensió "Policy Constraints"

No es fa ús de l'extensió "Policy Constraints" en els certificats emesos davall la present Política de Certificació.

### 7.1.8. Sintaxi i semàntica dels qualificadors de política

No estipulat.

### 7.1.9. Tractament semàntic per a l'extensió crítica "Certificate Policy"

L'extensió "Certificate Policy" identifica la política que definix les Pràctiques que PKIGVA associa explícitament amb el certificat. Addicionalment l'extensió conté un qualificador de la política i una adreça URL de localització d'esta.

## 7.2. Perfil de CRL

### 7.2.1. Número de versió

El format de les CRLs utilitzades en la present política és l'especificat en la versió 2 (v2).

### 7.2.2. CRL i extensions

La present Política de Certificació suporta i utilitza CRLs d'acord amb l'estàndard ITU - X.509.

## 8. ESPECIFICACIÓ DE L'ADMINISTRACIÓ

### 8.1. Procediments d'especificació de canvis

Segons el que especifica la Declaració de Pràctiques de Certificació (CPS) de la PKI de la Generalitat Valenciana.

### 8.2. Procediments de publicació i notificació

Quan es realitzen modificacions significatives en la present Política de Certificació estes es notificaran per mitjà de correu electrònic, als subscriptors dels certificats afectats.

En el cas de modificacions significatives en la Declaració de Pràctiques de Certificació de PKIGVA la notificació es farà extensiva als subscriptors de tots els certificats emesos.

Addicionalment les modificacions es faran públiques en el lloc web PKIGVA en <http://www.pki.gva.es>

Esta notificació es realitzarà amb anterioritat a l'entrada en vigor de la modificació que l'haja produït.

### 8.3. Procediments d'aprovació de la CPS

L'Autoritat d'Aprovació de Polítiques (AAP) de PKIGVA és l'entitat encarregada de l'aprovació en el moment de la seua creació de la present Política de Certificació (CP), així com de la Declaració de Pràctiques de Certificació (CPS).

L'AAP també s'encarrega d'aprovar i autoritzar les modificacions dels dits documents.

**Annex I****CONTRACTE DE CERTIFICAT - CODI 1.3.6.1.4.1.8149.3.2.1.2.1.0****Secció 1 - Dades de la persona sol·licitant**

Cognoms: .....

Nom: ..... DNI/NIF: .....

Organisme: .....

Organització (si és diferent a Generalitat Valenciana): .....

Adreça de correu electrònic: .....

Adreça postal: ..... Tel.: .....

**Secció 2 - Dades del funcionari adscrit a Registre**

Nom i cognoms: .....

DNI/NIF: .....

**Secció 3 - Data i Firma**

Sol·licite el Certificat associat a la Política de Certificat amb codi 1.3.6.1.4.1.8149.3.2.1.2.0.6, per a *Correu i Aplicacions Segures*, emés per la Generalitat Valenciana. Declare que conec i accepte les normes d'utilització d'este tipus de certificats que es troben exposades en <http://www.pki.gva.es>. Declare, així mateix, que les dades exposades són vertaderes.

..... a ..... de ..... de 2.00...

Firma de la persona sol·licitant

Firma del funcionari de Registre

Firmat:

Firmat:

Exemplar per a la persona sol·licitant - Anvers

**CONTRACTE DE CERTIFICACIÓ - CODI 1.3.6.1.4.1.8149.3.2.1.2.1.0****Condicions d'utilització dels certificats**

1. Els certificats associats a la Política de Certificat per a *Correu i Aplicacions Segures*, emesos per la Generalitat Valenciana són del tipus X509v3 i es regixen per la Declaració de Pràctiques de Certificat de la Generalitat Valenciana, en tant que Prestador de Servicis de Certificat, així com per la Política de Certificat referida. Estos dos documents s'han d'interpretar segons la legislació de la Comunitat Europea, l'Ordenament Jurídic Espanyol i la legislació pròpia de la Generalitat Valenciana.
2. Les persones sol·licitants hauran de ser persones físiques, que pertanyen a algun dels àmbits de certificat descrits en <http://www.pki.gva.es/cp02/acpr.htm> i en possessió d'un NIF.
3. La persona sol·licitant és responsable de la veracitat de les dades aportades en tot moment al llarg del procés de sol·licitud i registre. Serà responsable de comunicar qualsevol variació de les dades aportades per a l'obtenció del certificat.
4. El titular del certificat és responsable de la custòdia de la seua clau privada i de comunicar amb la major brevetat possible qualsevol pèrdua o sostracció d'esta clau.
5. El titular del certificat és responsable de limitar l'ús del certificat al que disposa la Política de Certificat associada, que és un document públic i que es troba disponible en <http://www.pki.gva.es>.
6. La Generalitat Valenciana, com a Prestadora de Servicis de Certificat, no se responsabiliza del contingut dels documents firmats i faran ús dels certificats per ella emesos.
7. La Generalitat Valenciana, com a Prestadora de Servicis de Certificat, és responsable del compliment de les legislacions Europea, Espanyola i Valenciana, pel que a Firma Electrònica es referix. És, així mateix, responsable del compliment del que disposa la Declaració de Pràctiques de Certificat de la Generalitat Valenciana i en la Política de Certificat associada a este tipus de certificats.
8. El període de validesa d'estos certificats és de tres (3) anys. Per a la seua renovació hauran de seguir el mateix procediment que per a la primera sol·licitud o bé els procediments previstos en la Política de Certificat associada.
9. Els certificats emesos perdran la seua eficàcia, a més del venciment del període de validesa, quan es produïska una revocació, quan s'inutilitze el suport del certificat, davant de resolució judicial o administrativa que ordene la pèrdua d'eficàcia, per inexactituds greus en les dades aportades pel sol·licitant i per mort del titular del certificat. Altres condicions per a la pèrdua d'eficàcia s'arreglen en la Declaració de Pràctiques de Certificat i en la Política de Certificat associada a este tipus de certificats.
10. La documentació que s'ha d'aportar per a la identificació dels sol·licitants serà el Document Nacional d'Identitat o Passaport vàlid i vigent.

Exemplar per a la persona sol·licitant - Revers

**CONTRACTE DE CERTIFICAT - CODI 1.3.6.1.4.1.8149.3.2.1.2.1.0****Secció 1 - Dades de la persona sol·licitant**

Cognoms: .....

Nom: ..... DNI/NIF: .....

Organisme: .....

Organització (si és diferent a Generalitat Valenciana): .....

Adreça de correu electrònic: .....

Adreça postal: ..... Tel.: .....

**Secció 2 - Dades del funcionari adscrit a Registre**

Nom i cognoms: .....

DNI/NIF: .....

**Secció 3 - Data i Firma**

Sol·licite el Certificat associat a la Política de Certificat amb codi 1.3.6.1.4.1.8149.3.2.1.2.0.6, per a *Correu i Aplicacions Segures*, emés per la Generalitat Valenciana. Declare que conec y accepte les normes d'utilització d'este tipus de certificats que es troben exposades en <http://www.pki.gva.es>. Declare, així mateix, que les dades exposades són vertaderes.

..... a ..... de ..... de 2.00...

Firma de la persona sol·licitant

Firma del funcionari de Registre

Firmat:

Firmat:

Exemplar per a la Generalitat Valenciana