Política de certificació digital de la UOC

Document aprovat pel Consell de Direcció de la UOC el dia 8 de febrer de 2016

Índex

1. Introducció

Aquest document conté les normes de certificació digital de clau pública aplicables als sistemes d'informació que ofereixen suport a procediments acadèmics i de gestió electrònics de la Universitat Oberta de Catalunya (UOC).

Una política de certificació de clau pública és un document que especifica normes de negoci, tècniques, organitzatives i de seguretat en l'ús de certificats electrònics X.509v3, d'acord amb la política de seguretat criptogràfica.

Aquest document estableix la política de certificació digital de la UOC, d'acord amb els requisits de seguretat i proporcionalitat corresponents als sistemes electrònics de suport a procediments acadèmics i de gestió, definits en les normes que regulen l'ús dels mitjans electrònics en els serveis públics.

La UOC adquirirà i admetrà certificats a terceres entitats prestadores de serveis de certificació, d'acord amb aquesta política, i els emprarà en procediments acadèmics i de gestió electrònics.

Per aquest motiu, cal garantir uns nivells de qualitat en la certificació, per a la qual cosa es considera necessari disposar d'un document que formalitzi els tipus de certificats que s'han de fer servir, en relació amb els diferents col·lectius i aplicacions de la UOC, i els requisits aplicables al cicle de vida d'aquests certificats.

Els continguts d'aquesta política de certificació de clau pública s'han estructurat per a cobrir els controls que preveu la norma internacional ISO/IEC 27002:2006 – Tecnologia de la Informació: Tècniques de seguretat: Codi de pràctiques per a la gestió de la seguretat de la informació, seccions 12.3.1 i 15.1.6, i es basen en les recomanacions de millors pràctiques contingudes a la IETF RFC 3647, a l'ETSI TS 101 456 i a la TS 102 042, entre altres.

2. Continguts generals de la política de certificació digital

2.1. Identificació de la política de certificació digital

Aquesta política de certificació digital s'identifica amb el següent identificador d'objecte: 1.3.6.1.4.1.43653.1.3

2.2. Vigència

Aquesta política de certificació entra en vigor l'endemà del dia de ser aprovada.

2.3. Àmbit d'aplicació

Aquesta política és aplicable a tots els sistemes d'informació de suport a procediments acadèmics i de gestió electrònics, i també a les relacions per mitjans electrònics amb tercers que no formen part de la comunitat universitària, emprats per la UOC.

3. Tipologia de certificats

Aquesta política defineix els tipus de certificats següents:

- Certificats de tercers i d'estudiants:
    - Certificat-tipus de persona física.
    - Certificat-tipus de persona jurídica.
    - Certificat-tipus de representant.
    - Certificat-tipus de personal al servei d'una organització privada.
- Certificats de la UOC:
    - Certificat-tipus de seu electrònica.
    - Certificat-tipus de persona jurídica.
    - Certificat-tipus de personal al servei de la UOC.
- Certificats d'ús tècnic
    - Certificat-tipus d'entitat de segellament de data i hora.
    - Certificat-tipus de servidor segur.

- Certificat-tipus d'aplicació segura.
- Certificat-tipus de signatura de programari.

En termes generals, la UOC ha d'admetre els certificats, sempre que hi hagi les condicions següents:

- Els prestadors hagin comunicat l'inici de la seva activitat al Ministeri d'Indústria, Energia i Turisme.
- Quan es tracti de certificats de signatura electrònica, aquests hagin estat admesos pel Ministeri d'Indústria, Energia i Turisme.
- Els certificats compleixin les condicions addicionals establertes per aquesta política i els seus estàndards de desenvolupament.

Els certificats per a l'ús propi de la UOC s'han d'adquirir, d'acord amb el que determina aquesta política.

La UOC adquireix o admet certificats per als usos següents:

- Autenticació basada en certificats X.509v3, d'acord amb la *política d'autenticació electrònica* corresponent.
- Signatura electrònica, avançada o reconeguda, basada en certificats X.509v3, *d'acord amb la política de signatura electrònica* corresponent.
- Xifratge asimètric o mixt, basat en certificats X.509v3, d'acord amb la *política de xifratge* corresponent.
- Protecció d'evidències electròniques, basada en certificats X.509v3, d'acord amb la *política d'evidència electrònica* corresponent.

3.1. Certificats de tercers i d'estudiant

3.1.1. Certificat-tipus de persona física

Són certificats de persona física els certificats emesos a persones físiques per a actuar a títol individual.

Els certificats de persona física es poden emprar, en general, per a la realització d'actes en nom propi, o en nom de terceres persones físiques o jurídiques, quan la persona física acrediti la representació prèviament.

Així mateix, els certificats de persona física poden incorporar atributs o circumstàncies específiques de les persones físiques, que poden ser utilitzats per les aplicacions de la

Universitat, d'acord amb les condicions addicionals que es determinin en la *política d'autenticació, signatura electrònica, xifratge o evidència electrònica* corresponent.

Els certificats de persona física amb pseudònims es poden admetre per a relacions electròniques amb la Universitat, en els àmbits de la participació dels estudiants i altres fórmules de democràcia electrònica, per a afavorir l'exercici de les llibertats públiques, sempre que es compleixin els requisits que es preveuen per a aquest tipus de certificats a la Llei 59/2003, de 19 de desembre, de signatura electrònica.

El certificat-tipus de persona física s'identifica amb l'identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.1 i pot tenir els nivells de seguretat següents:

- Certificat-tipus de persona física de nivell 1, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.1.1, que correspon a un certificat que ofereix garantia d'identitat.
- Certificat-tipus de persona física de nivell 2, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.1.2, que correspon a un certificat que ofereix garantia d'identitat i d'origen de dades.
- Certificat-tipus de persona física de nivell 3, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.1.3, que correspon a un certificat reconegut que ofereix garantia d'autenticitat documental.
- Certificat-tipus de persona física de nivell 4, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.1.4, que correspon a un certificat que ofereix garantia de reconeixement de signatura.

3.1.2. Certificat-tipus de persona jurídica

Són certificats de persona jurídica els certificats emesos a persones jurídiques, d'acord amb l'article 7 de la Llei 59/2003, per a actuar a títol individual, tot i que incorporin altres atributs o informacions personals que els vinculin a altres entitats, sempre que no es tracti de la representació.

Els certificats de persona jurídica es poden emprar, en general, per a la realització d'actes en nom propi, o en nom de terceres persones físiques o jurídiques, quan la persona física acrediti la representació prèviament.

Tanmateix, els certificats de persona jurídica poden incorporar atributs o circumstàncies específiques de les persones jurídiques, que poden ser utilitzats per les aplicacions de la Universitat, d'acord amb las condicions addicionals que es determinin en la *política d'autenticació, signatura electrònica, xifratge o evidència electrònica* corresponent.

No s'admet l'ús de certificats de persona jurídica amb pseudònim, ni es poden emprar quan la normativa aplicable al procediment exigeixi l'actuació d'un representant legal o voluntari

amb apoderament suficient. En aquest cas, s'han de fer servir certificats de persona física que tingui aquesta condició o la de representant.

El certificat-tipus de persona jurídica s'identifica amb l'identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.10 i pot tenir els nivells de seguretat següents:

- Certificat-tipus de persona jurídica de nivell 1, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.10.1, que correspon a un certificat que ofereix garantia d'identitat.
- Certificat-tipus de persona jurídica de nivell 2, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.10.2, que correspon a un certificat que ofereix garantia d'identitat i d'origen de dades.
- Certificat-tipus de persona jurídica de nivell 3, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.10.3, que correspon a un certificat reconegut que ofereix garantia d'autenticitat documental.
- Certificat-tipus de persona jurídica de nivell 4, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.10.4, que correspon a un certificat que ofereix garantia de reconeixement de signatura.

3.1.3. Certificat-tipus de representant

Són certificats de representant els certificats emesos a persones físiques o jurídiques per a actuar en representació de terceres persones físiques o jurídiques i que incorporen les dades de la representació i de la persona representada.

Els certificats de representant no es poden emprar per a la realització d'actes en nom propi.

Tanmateix, els certificats de representant poden incorporar atributs o circumstàncies específiques dels representants, que poden ser utilitzats per les aplicacions de la Universitat, d'acord amb les condicions addicionals que es determinin en la *política d'autenticació, signatura electrònica, xifratge o evidència electrònica* corresponent.

No s'admet l'ús de certificats de representant amb pseudònim.

El certificat-tipus de representant s'identifica amb l'identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.4 i pot tenir els nivells de seguretat següents:

- Certificat-tipus de representant de nivell 1, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.4.1, que correspon a un certificat que ofereix garantia d'identitat.
- Certificat-tipus de representant de nivell 2, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.4.2, que correspon a un certificat que ofereix garantia d'identitat i d'origen de dades.

– Certificat-tipus de representant de nivell 3, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.4.3, que correspon a un certificat reconegut que ofereix garantia d'autenticitat documental.
– Certificat-tipus de representant de nivell 4, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.4.4, que correspon a un certificat que ofereix garantia de reconeixement de signatura.

3.1.4. Certificat-tipus de personal al servei d'una organització

Són certificats de personal al servei d'una organització els certificats emesos a persones físiques que incorporen atributs o informacions personals que els vinculen a altres entitats, sempre que no es tracti de la representació, per a actuar dins de l'àmbit corporatiu de l'organització.

Així mateix, els certificats de personal al servei d'una organització poden incorporar atributs o circumstàncies específiques de les organitzacions, que poden ser utilitzats per les aplicacions de la Universitat, d'acord amb les condicions addicionals que es determinin en la *política d'autenticació, signatura electrònica, xifrat o evidència electrònica* corresponent.

El certificat-tipus de personal al servei d'una organització s'identifica amb l'identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.12 i pot tenir els nivells de seguretat següents:

- Certificat-tipus de personal al servei d'una organització de nivell 1 1.3.6.1.4.1.43653.1.3.1.7.1, amb identificador d'objecte, que correspon a un certificat que ofereix garantia d'identitat.
- Certificat-tipus de personal al servei d'una organització de nivell 2 1.3.6.1.4.1.43653.1.3.1.7.2, amb identificador d'objecte, que correspon a un certificat que ofereix garantia d'identitat i d'origen de dades.
- Certificat-tipus de personal al servei d'una organització de nivell 3 1.3.6.1.4.1.43653.1.3.1.7.3, amb identificador d'objecte, que correspon a un certificat reconegut que ofereix garantia d'autenticitat documental.
- Certificat-tipus de personal al servei d'una organització de nivell 4 1.3.6.1.4.1.43653.1.3.1.7.4, amb identificador d'objecte, que correspon a un certificat que ofereix garantia de reconeixement de signatura.

3.2. Certificats de la UOC

3.2.1. Certificat-tipus de persona jurídica de la UOC

Són certificats de persona jurídica de la UOC els certificats emesos a la UOC com a persona jurídica, d'acord amb l'article 7 de la Llei 59/2003, per a actuar a títol individual, tot i que incorporin altres atributs o informacions personals que els vinculin a altres entitats, sempre que no es tracti de la representació.

Els certificats de persona jurídica de la UOC es poden emprar, en general, per a la realització d'actes en nom propi, o en nom de terceres persones físiques o jurídiques, quan aquestes acreditin la representació prèviament.

Tanmateix, els certificats de persona jurídica de la UOC poden incorporar atributs o circumstàncies específiques de les persones jurídiques, que poden ser utilitzats per les aplicacions de la UOC, d'acord amb les condicions addicionals que es determinin en la *política d'autenticació, signatura electrònica, xifratge o evidència electrònica* corresponent.

El certificat-tipus de persona jurídica de la UOC s'identifica amb l'identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.10 i pot tenir els nivells de seguretat següents:

- Certificat-tipus de persona jurídica de la UOC de nivell 1, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.10.1, que correspon a un certificat que ofereix garantia d'identitat.
- Certificat-tipus de persona jurídica de la UOC de nivell 2, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.10.2, que correspon a un certificat que ofereix garantia d'identitat i d'origen de dades.
- Certificat-tipus de persona jurídica de la UOC de nivell 3, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.10.3, que correspon a un certificat reconegut que ofereix garantia d'autenticitat documental.
- Certificat-tipus de persona jurídica de la UOC de nivell 4, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.10.4, que correspon a un certificat que ofereix garantia de reconeixement de signatura.

3.2.2. Certificat-tipus de personal al servei de la UOC

Són certificats de personal al servei de la UOC els certificats emesos a persones físiques que incorporen atributs o informacions personals que els vinculen a la UOC, sempre que no es tracti de la representació, per a actuar dins de l'àmbit corporatiu de la Universitat.

Així mateix, els certificats de personal al servei de la UOC poden incorporar atributs o circumstàncies específiques del personal al servei de la UOC, que poden ser utilitzats per les aplicacions de la UOC, d'acord amb les condicions addicionals que es determinin en la *política d'autenticació, signatura electrònica, xifrat o evidència electrònica* corresponent.

El certificat-tipus de personal al servei de la UOC s'identifica amb l'identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.7 i pot tenir els nivells de seguretat següents:

- Certificat-tipus de personal al servei de la UOC de nivell 1 1.3.6.1.4.1.43653.1.3.1.7.1, amb identificador d'objecte, que correspon a un certificat que ofereix garantia d'identitat.
- Certificat-tipus de personal al servei de la UOC de nivell 2 1.3.6.1.4.1.43653.1.3.1.7.2, amb identificador d'objecte, que correspon a un certificat que ofereix garantia d'identitat i d'origen de dades.
- Certificat-tipus de personal al servei de la UOC de nivell 3 1.3.6.1.4.1.43653.1.3.1.7.3, amb identificador d'objecte, que correspon a un certificat reconegut que ofereix garantia d'autenticitat documental.
- Certificat-tipus de personal al servei de la UOC de nivell 4 1.3.6.1.4.1.43653.1.3.1.7.4, amb identificador d'objecte, que correspon a un certificat que ofereix garantia de reconeixement de signatura.

3.3. Certificats d'ús tècnic

3.3.1. Certificat-tipus de segellament de data i hora (marques de temps)

Són certificats d'entitat de segellament de data i hora els certificats emesos a persones físiques o jurídiques per a actuar com a prestadors del servei de segellament de data i hora.

El certificat-tipus d'entitat de segellament de data i hora s'identifica amb l'identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.8 i pot tenir el nivell de seguretat següent:

- Certificat-tipus d'entitat de segellament de data i hora de nivell únic, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.8.1

3.3.2. Certificat-tipus de servidor segur

Són certificats de servidor segur els certificats emesos a persones físiques o jurídiques per a identificar i garantir les comunicacions segures amb els seus servidors, sense la consideració legal de seu electrònica.

El certificat-tipus de servidor segur s'identifica amb l'identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.9 i pot tenir els nivells de seguretat següents:

- Certificat-tipus de servidor segur de nivell mitjà, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.9.1, que correspon a un certificat basat en mitjà equivalent a dispositiu segur.
- Certificat-tipus de servidor de nivell alt, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.9.2, que correspon a un certificat basat en dispositiu segur.

3.3.3. Certificat-tipus d'aplicació segura

Són certificats d'aplicació segura els certificats emesos a persones físiques o jurídiques per a autenticar comunicacions, missatges i documents de manera automàtica, sense la consideració legal de segell electrònic.

El certificat-tipus d'aplicació segura s'identifica amb l'identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.13 i pot tenir els nivells de seguretat següents:

- Certificat-tipus d'aplicació segura de nivell mitjà, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.13.1, que correspon a un certificat reconegut que ofereix garantia d'autenticitat documental.
- Certificat-tipus d'aplicació segura de nivell alt, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.13.2, que correspon a un certificat reconegut i que està basat en dispositiu segur.

3.3.4. Certificat-tipus de signatura de programari

Són certificats de signatura de programari els certificats emesos a persones físiques o jurídiques per a protegir el programari que s'ha de distribuir per xarxes.

El certificat-tipus de signatura de programari s'identifica amb l'identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.11 i pot tenir el nivell de seguretat següent:

- Certificat-tipus de signatura de programari de nivell únic, amb identificador d'objecte 1.3.6.1.4.1.43653.1.3.1.11.1.

4. Comunitat d’usuaris dels certificats

4.1. Prestadors de serveis de certificació

Poden ser prestadors de serveis de certificació totes les entitats que operin a l’Estat espanyol, en els termes de la legislació vigent de signatura electrònica, i hagin comunicat l’inici de la seva activitat al del Ministeri d’Indústria, Energia i Turisme, de manera que apareguin a la llista de confiança de prestadors de serveis de certificació publicada pel Ministeri.

4.2. Entitats de registre

Els prestadors de serveis de certificació defineixen, sota la seva responsabilitat, quines entitats poden actuar com a entitats de registre del servei de certificació corresponent.

La UOC ha de poder actuar com a entitat de registre amb relació als certificats corporatius, quan els adquireixi, i també com a entitat de registre de les entitats a les quals presta assistència.

Quan emeti certificats corporatius, la UOC ha de definir les entitats de registre en la seva Declaració de pràctiques de certificació.

4.3. Usuaris finals

4.3.1. Sol·licitants de certificats

La UOC ha de poder actuar com a sol·licitant de certificats quan adquireix certificats corporatius, i també com a sol·licitant de certificats de les entitats a les quals presta assistència.

4.3.2. Subscriptors de certificats

Cada entitat que rebi certificats té la condició de subscriptora d’aquests, en els termes i amb les obligacions que indiqui la política o declaració de pràctiques de confiança del prestador corresponent.

4.3.3. Verificadors de certificats

La UOC ha d'actuar com a verificador de certificats, mitjançant els procediments tècnics que descriu aquesta política de certificació, sense perjudici de l'existència d'altres verificadors diferents.

5. Requisits d'operació del cicle de vida dels certificats

Aquesta secció descriu les normes que aplica la UOC en relació amb el cicle de vida dels certificats que adquireix.

Les normes referides als serveis d'informació d'estat de certificats també són aplicables als certificats que admeti la UOC. Han d'estar prèviament classificats per l'Agència Catalana de Certificació o comunicats al Ministeri d'Indústria, Energia i Turisme.

5.1. Sol·licitud d'emissió de certificat

5.1.1. Legitimació per a sol·licitar l'emissió

La UOC pot sol·licitar els certificats d'ús propi definits per aquesta política, i també els certificats de les entitats a les quals presta assistència.

Quan la política o declaració de pràctiques de confiança del prestador no garanteixi la reposició en menys de 24 hores d'un certificat, en cas de pèrdua, robatori o incidència que de qualsevol altra manera impliqui la incapacitat per a fer servir el certificat, la UOC podrà sol·licitar més d'un certificat per a cada persona, com a mesura de contingència.

5.1.2. Procediment d'alta; responsabilitats

El procediment d'alta i les responsabilitats són les previstes a les polítiques o declaracions de pràctiques del prestador de serveis de certificació corresponent.

5.2. Acceptació del certificat

La UOC pot rebre i acceptar el lliurament dels certificats corporatius, sempre que les dades d'activació de les claus privades dels certificats siguin lliurades directament als posseïdors dels certificats.

5.3. Ús del parell de claus i del certificat

Els certificats s'han d'emprar d'acord amb les limitacions previstes pels prestadors corresponents de serveis de certificació. La UOC només ha d'adquirir o admetre certificats que siguin compatibles amb les seves normatives de seguretat criptogràfica, de gestió de claus, d'autenticació, de signatura o de xifratge.

La UOC ha d'implantar mesures per a informar els subscriptors i posseïdors de claus de les seves obligacions i limitacions d'ús.

Amb relació a la verificació de certificats i signatures electròniques, la UOC ha d'utilitzar programari de verificació de signatura electrònica amb la capacitat tècnica, operativa i de seguretat suficient per a executar el procés de verificació de signatura correctament, i ha d'aplicar les normes següents:

- La signatura electrònica s'ha de poder verificar d'acord amb els requeriments establerts en la *política d'autenticació, signatura electrònica, xifratge o evidència electrònica* corresponent.
- La UOC ha d'haver utilitzat informació de revocació actualitzada en el moment de la verificació de la signatura.
- El tipus i classe de certificat ha de ser apropiat per a l'ús que se'n pretén fer, dins dels límits d'ús corresponents.
- La UOC ha de prendre en consideració altres limitacions addicionals d'ús del certificat indicades de qualsevol manera en el certificat, incloent-hi les no processades automàticament pel programari de verificació, incorporades per referència al certificat.
- La UOC ha d'establir el significat de la signatura i la intenció del signatari, atès que l'acte de signar pot tenir implicacions diferents segons l'aplicació de la signatura, en especial quan les signatures són regulades per normatives de signatura.
- Finalment, la confiança ha de ser raonable d'acord amb les circumstàncies. Si les circumstàncies requereixen garanties addicionals, la UOC ha d'obtenir aquestes garanties per tal que la confiança sigui raonable.

5.4. Renovació de certificats sense renovació de claus

La UOC no ha de sol·licitar mai la renovació de certificats sense la renovació de claus.

5.5. Renovació de certificat amb renovació de claus

La UOC pot sol·licitar la renovació amb renovació de claus dels certificats corporatius, i també ho pot sol·licitar per a les entitats a les quals presta assistència.

El procediment de renovació i les responsabilitats són les previstes a les polítiques o declaracions de pràctiques del prestador de serveis de certificació corresponent.

5.6. Modificació de certificats

Qualsevol necessitat de modificació de certificats implica una sol·licitud en aquest sentit al prestador de serveis de certificació corresponent, d'acord amb la política o declaració de serveis de certificació aplicable.

En cas que la política o declaració de certificació no inclogui aquesta possibilitat, caldrà sol·licitar la revocació del certificat afectat i la nova emissió d'un certificat que incorpori les noves dades.

5.7. Revocació i suspensió de certificats

5.7.1. Causes de revocació de certificats

En general, les causes de revocació de certificats són les causes legalment establertes a la normativa vigent en matèria de signatura electrònica.

La UOC considera causa de revocació del certificat:

- L'ús fraudulent del certificat en qualsevol sistema informàtic de la Universitat i les causes que es puguin establir en les normes vigents.
- La modificació o extinció de la relació jurídica o causa que va provocar l'emissió del certificat al posseïdor de claus.
- La infracció per part del posseïdor de claus de les seves obligacions, responsabilitats i garanties, establertes en el document jurídic corresponent.

5.7.2. Legitimació per a sol·licitar la revocació

Quan la UOC detecti la concurrència d'alguna circumstància que podria donar lloc a la revocació d'un certificat, propi o de les entitats a les quals presta assistència, ho ha de comunicar al prestador de serveis de certificació corresponent, però ha de continuar emprant

el certificat mentre no sigui revocat, ja que és responsabilitat exclusiva del prestador decidir la finalització anticipada del període de vida del certificat.

La norma anterior no s'aplica en cas d'ús fraudulent del certificat en els sistemes de la UOC, que dóna lloc al bloqueig immediat de l'ús del certificat i a la sol·licitud posterior de revocació davant del prestador de serveis de certificació corresponent.

5.7.3. Obligació de consulta d'informació de revocació de certificats

La UOC s'obliga a consultar la informació de revocació de certificats, mitjançant els mecanismes aportats pels prestadors de serveis de certificació corresponents.

La UOC pot emprar serveis de validació delegada per a complir aquesta obligació, per exemple, el servei Validador (PSIS) de l'Agència Catalana de Certificació - Consorci AOC, entre altres.

5.7.4. Causes de suspensió de certificats

En general, les causes de suspensió de certificats seran les causes legalment establertes a la normativa vigent en matèria de signatura electrònica.

Addicionalment, la UOC considera causa de suspensió del certificat la sospita de l'ús fraudulent del certificat en qualsevol sistema informàtic de la Universitat.

5.7.5. Legitimació per a sol·licitar la suspensió

Quan la UOC detecti la concurrència d'alguna circumstància que podria donar lloc a la suspensió d'un certificat, propi o de les entitats a les quals presta assistència, ho ha de comunicar al prestador de serveis de certificació corresponent, però ha de continuar emprant el certificat mentre no sigui suspès, ja que és responsabilitat exclusiva del prestador decidir la finalització anticipada del període de vida del certificat.

La norma anterior no s'aplica en cas de sospita d'ús fraudulent del certificat en els sistemes de la UOC, que dóna lloc al bloqueig immediat de l'ús del certificat i a la sol·licitud posterior de suspensió davant del prestador de serveis de certificació corresponent.

5.8. Serveis de comprovació d'estat de certificats

5.8.1. Característiques dels serveis

Sempre que sigui possible, la Universitat ha de verificar els certificats mitjançant mecanismes en línia, que responguin en temps real, com, per exemple, el servei Validador (PSIS) de l'Agència Catalana de Certificació - Consorci AOC o, si aquest servei no és possible, servidors OCSP (protocol en línia d'estat de certificats).

Quan no sigui possible la consulta en línia, la UOC farà servir llistes de revocació de certificats emeses pel prestador de serveis de certificació corresponent.

Les instruccions generals d'autenticació, signatura electrònica, xifratge o evidència electrònica basades en l'ús dels certificats aprovades per la Universitat poden definir els requisits concrets dels serveis de comprovació d'estat de certificats que cal emprar en cada cas.

5.8.2. Disponibilitat dels serveis

Els serveis de comprovació d'estat de certificats, i els llocs web de publicació de les llistes de revocació de certificats, han d'estar disponibles 24 hores al dia, 7 dies la setmana, 365 dies l'any.

5.9. Finalització de la subscripció

La UOC pot sol·licitar l'acabament de la subscripció dels serveis, amb relació als certificats d'ús propi o de les entitats a les quals presta assistència, en els casos d'adquisició a tercers prestadors.

El procediment de finalització i les responsabilitats són les previstes en les polítiques o declaracions de pràctiques del prestador de serveis de certificació corresponent.

6. Perfils de certificats i llistes de revocació de certificats

Aquesta secció determina les normes aplicables als perfils dels certificats que cal adquirir o admetre, i també les llistes de revocació de certificats.

6.1. Perfils de certificats

6.1.1. Formats de noms

Els certificats han de contenir les informacions que siguin necessàries per a utilitzar-los, segons el que estableixi la *política d'autenticació, signatura electrònica, xifratge o evidència electrònica* corresponent.

En general, els certificats d'ús han de contenir la identitat de la persona que els rep, en el camp *SubjectName*, incloent-hi les dades següents:

- Nom i cognoms, separats, o amb la indicació de l'algorisme que en permet fer la separació de manera automàtica.
- Número d'identificació fiscal.

Aquesta norma no s'aplica als certificats amb pseudònim, que han d'identificar aquesta condició.

6.1.2. Restriccions de noms

La UOC pot establir restriccions de noms amb relació als certificats en la *política d'autenticació, signatura electrònica, xifratge o evidència electrònica* corresponent, sempre que aquestes restriccions siguin objectives, proporcionades, transparents i no discriminatòries.

6.2. Perfil de la llista de revocació de certificats

6.2.1. Llista de revocació de certificats i extensions d'elements de la llista

La UOC només admet llistes de revocació de certificats d'acord amb l'estàndard X.509v3 i l'RFC 5280 de la IETF.

Les llistes de revocació de certificats han de ser completes i, per tant, no s'admetran llistes parcials.

Les llistes de revocació de certificats han de ser directes; és a dir, han de ser signades pel prestador de serveis de certificació que va emetre els certificats suspesos o revocats, i no per terceres entitats, excepte en cas d'emergència.

7. Requisits legals

Aquesta secció estableix normes legals en relació amb l'ús dels certificats.

7.1. Obligacions i responsabilitat civil

7.1.1. Client

La UOC s'ha d'obligar a:

- Utilitzar el servei de certificació electrònica d'acord amb les instruccions, manuals o procediments subministrats pel prestador de serveis de certificació corresponent.
- Verificar les signatures i els certificats d'acord amb les condicions generals d'ús corresponents, o, quan se n'estigui mancat, d'acord amb la declaració de pràctiques de certificació.
- No utilitzar cap mena d'informació d'estat dels certificats o de cap altre tipus que hagi estat subministrada per un prestador de serveis de certificació per a fer cap transacció prohibida per la llei aplicable.
- Complir qualsevol llei i regulació que pugui afectar el seu dret a fer servir les eines criptogràfiques que utilitzi en l'ús dels certificats.

La UOC no es responsabilitza de què la informació continguda en un certificat admès, o la utilització d'un domini i/o altre tipus de nom o denominació, i la resta d'informació de sol·licitud dels certificats, eventualment infringeixi els drets de cap persona en cap jurisdicció amb respecte a les seves marques registrades, marques de servei, noms comercials o qualsevol altre dret de propietat intel·lectual o industrial.

La UOC tampoc no es responsabilitza del fet que el subscriptor del certificat admès pretengui utilitzar el domini i els nom distingits per a cap propòsit il·legal, incloent-hi, sense limitació, la infracció amb dol d'un contracte, o l'obtenció de possibles avantatges comercials, la competència deslleial, la lesió del dret a l'honor, i la confusió o engany d'una persona, tant física com jurídica.

7.1.2. Subscriptors de certificats admesos

El subscriptor d'un certificat admès s'ha d'obligar a:

- Utilitzar el servei de certificació digital d'acord amb les instruccions, manuals o procediments subministrats pel prestador del servei de certificació corresponent.
- Fer ús del certificat digital amb el caràcter de personal i intransferible i, per tant, assumir la responsabilitat per qualsevol actuació que es dugui a terme en contravenció d'aquesta obligació, i també complir les obligacions que siguin específiques de la normativa aplicable a les esmentades certificacions digitals.
- Autoritzar els òrgans de la UOC a fer el tractament de les dades personals contingudes en els certificats, en connexió amb les finalitats de la relació electrònica i, en tot cas, per a complir les obligacions legals de verificació de certificats.
- Responsabilitzar-se del fet que tota la informació inclosa, per qualsevol mitjà, en la sol·licitud del certificat i en el mateix certificat sigui exacta i completa per a la finalitat del certificat, i estigui actualitzada en tot moment.
- Informar immediatament la UOC de qualsevol inexactitud en el certificat detectada un cop s'hagi emès, i també dels canvis que es produeixin en la informació aportada per a l'emissió del certificat.
- Si es tracta de certificats en un dispositiu material, en cas que se'n perdi la possessió, posar-ho en coneixement fefaent de l'entitat que l'hagi emès en el termini més breu possible i, en tot cas, dins de les 24 hores següents al moment en què s'hagi produït aquesta circumstància, amb independència del fet concret que l'hagi originat o de les accions que eventualment pugui exercir.
- No utilitzar la clau privada, el certificat electrònic o qualsevol altre suport tècnic lliurat pel prestador de serveis de certificació corresponent o per la UOC per a fer cap transacció prohibida per la llei aplicable.
- Complir qualsevol llei i regulació que pugui afectar el seu dret a utilitzar les eines criptogràfiques que empri.

7.2. Protecció de dades personals

La UOC és conscient que els certificats digitals i les signatures electròniques contenen dades de caràcter personal i la titularitat dels subscriptors de certificats i, si s'escau, dels posseïdors de les claus corresponents.

En conseqüència, la UOC es compromet a utilitzar aquesta informació personal amb la finalitat exclusiva de verificar la identitat personal del subscriptor i les signatures electròniques dels seus missatges o documents.

En cap cas la UOC farà cap altre ús de les dades, sense consentiment exprés del subscriptor o del posseïdor de claus.

Així mateix, la UOC es compromet a protegir les dades personals d'acord amb el que estableix la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, i en especial s'obliga a establir les mesures de seguretat adequades, d'acord amb l'article 9 d'aquesta llei.

7.3. Conformitat amb la llei aplicable

La UOC ha de garantir la conformitat de tots els serveis de certificació que adquireixi o admeti amb la llei aplicable, que és la llei espanyola.

En cas que un servei de certificació deixi de ser conforme a la llei espanyola, la UOC haurà de deixar-lo d'emprar, en el mínim temps possible, i l'haurà de substituir per un servei que sigui conforme a la llei.

Annex. Llista de procediments de certificació de clau pública

Fase prèvia a l'operació

- Procediment/s d'admissió de certificats.
- Procediment/s d'adquisició de certificats.

Fase d'operació

- Procediment/s de suspensió i revocació de certificats.
- Procediment/s de renovació de certificats.
- Procediment/s de finalització de la subscripció.

Fase posterior a l'operació

- Procediment/s d'emmagatzematge d'arxiu de certificats.