Política de gestió de claus 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 gestió de claus criptogràfiques aplicables als sistemes d'informació que ofereixen suport a procediments acadèmics i de gestió electrònics de la Universitat Oberta de Catalunya (UOC).

Nota: Una política de gestió de claus criptogràfiques és un document que especifica normes d'ús en relació amb les claus criptogràfiques, d'acord amb la política de seguretat criptogràfica.

Aquesta política s'ha establert d'acord amb els requisits de seguretat i proporcionalitat corresponents als sistemes electrònics de suport a procediments acadèmics i de gestió electrònics, definits en les normes que regulen l'ús dels mitjans electrònics en els serveis públics.

Els continguts d'aquesta política de gestió de claus 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 Publicació Especial 800-57, parts 1 i 2, de l'Institut Nacional d'Estàndards i Tecnologia (National Institute of Standards and Technology, NIST) dels Estats Units.

Aquesta política general de gestió de claus criptogràfiques s'aplica en l'ús de claus pròpies de la Universitat Oberta de Catalunya en les normatives següents:

- Política de certificació digital.
- Política d'autenticació electrònica.
- Política de signatura electrònica.
- Política de xifratge.

2. Continguts generals de la política de gestió de claus

2.1. Identificació de la política de gestió de claus

Aquesta política de gestió de claus s'identifica amb el següent identificador d'objecte: 1.3.6.1.4.1.43653.1.2

2.2. Vigència

Aquesta política de gestió entra en vigor l'endemà de ser aprovada.

2.3. Àmbit d'aplicació

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

3. Cicle de vida de les claus criptogràfiques

El cicle de vida de les claus criptogràfiques és format per totes les accions i esdeveniments relatius a les claus, des que es generen fins que es destrueixen.

El cicle de vida de la gestió de les claus es divideix en quatre fases:

– Fase **prèvia** a l'operativa. En aquesta fase, les claus i la resta del material criptogràfic no són disponibles per a l'operativa normal. Les claus potser encara no s'han generat o es poden trobar en l'estat previ a l'activació. En aquesta fase es configuren els sistemes.

– Fase **operativa**. En aquesta fase les claus són en fase activa i es poden emprar per a protegir informació, processar informació protegida o totes dues funcions.

– Fase **posterior** a l'operativa. En aquesta fase, les claus i la resta del material criptogràfic deixen de ser disponibles per a fer-ne un ús normal, però es pot accedir a les claus en algunes circumstàncies determinades per a processar informació protegida. Les claus poden ser en els estats de desactivació o compromís. En aquesta fase, les claus estan arxivades, mentre no s'utilitzen per a processar informació protegida.

– Fase de **destrucció**. En aquesta fase, les claus ja no són disponibles i els registres que hi estan relacionats poden haver estat destruïts. Les claus són en l'estat de destrucció o destrucció de clau compromesa, tot i que és possible que es conservin alguns atributs determinats de la clau (com el nom).

  Una clau es pot trobar, al llarg del seu cicle de vida, en diverses fases, però no pot tornar a una fase anterior en cap cas.

4. Normes aplicables en la fase prèvia a l'operació

Les gestions en la fase prèvia a l'operació criptogràfica inclouen les següents:

– El registre de l'usuari. En aquest procediment, es determina la identitat de l'usuari de la clau.

– La inicialització del sistema criptogràfic. En aquest procediment, es configura i es posa en funcionament el maquinari i programari criptogràfic, de manera general.

– La inicialització de l'usuari. En aquest procediment, es configuren les dades de l'usuari del maquinari i programari criptogràfic.

– La instal·lació del material criptogràfic. En aquest procediment, es fa la càrrega de les claus i d'altres paràmetres en el maquinari i programari criptogràfic, excepte l'establiment de les claus.

– L'establiment de les claus criptogràfiques. En aquest procediment, es porta a terme la generació i la distribució de les claus i d'altre material criptogràfic.

– El registre de les claus criptogràfiques. En aquest procediment, s'estableix la vinculació entre l'usuari i les claus.

4.1. Registre de l'usuari

El registre de l'usuari consisteix en la determinació de la identitat de l'usuari, perquè ell mateix pugui obtenir i utilitzar claus criptogràfiques i, quan escaigui, els certificats corresponents. És una de les gestions més importants, ja que una identificació de qualitat garanteix la imputació de la qualitat d'autor a la persona que signa electrònicament els documents, per exemple.

La UOC ha d'identificar i enregistrar els usuaris als quals s'assignen qualssevol tipus de claus criptogràfiques, en els termes previstos per la legislació de signatura electrònica, i ha de documentar suficientment els procediments de registre d'usuari.

La UOC ha de documentar en la seva *política de certificació* el procediment de registre mínim aplicable a la sol·licitud d'emissió, renovació i revocació de certificats.

Quan s'adquireixin certificats en entitats de certificació, la UOC ha de garantir que els procediments de registre establerts per aquestes entitats de certificació són equivalents o superiors als procediments instituïts per la Universitat per a l'emissió, renovació i revocació de certificats.

4.2. Inicialització del sistema

La inicialització del sistema consisteix en la configuració del programari i maquinari criptogràfic, per tal que operi amb seguretat.

La UOC ha de documentar els procediments per a la inicialització dels sistemes i dispositius que componen la infraestructura criptogràfica, considerant els aspectes següents:

– La configuració adequada dels dominis de seguretat, d'acord amb la documentació dels proveïdors, i amb les restriccions d'ús del programari i maquinari que estigui certificat com a segur.

– La creació dels rols d'administració i operació dels components de programari i maquinari.

– La selecció dels algorismes criptogràfics i de les claus i els paràmetres de configuració corresponents.

– La configuració de les normatives i polítiques de seguretat i de confiança necessàries per a donar compliment a les normatives d'autenticació, signatura electrònica i xifratge de la UOC.

4.3. Inicialització de l'usuari

La inicialització de l'usuari consisteix en el procediment d'instal·lació, configuració i activació del maquinari i programari criptogràfic subministrat a l'usuari, incloent-hi l'obtenció de les claus corresponents a punts de confiança, paràmetres, algorismes i polítiques.

La UOC ha de documentar els procediments d'inicialització dels usuaris, d'acord amb els manuals i les instruccions tècniques dels proveïdors del programari i maquinari criptogràfic corresponent.

4.4. Instal·lació del material criptogràfic

La instal·lació del material criptogràfic consisteix en la càrrega de les claus i altres paràmetres en el maquinari i programari criptogràfic, en les situacions següents:

– Configuració inicial del programari i maquinari criptogràfic, mitjançant la funció d'establiment de les claus.

– Addició de material criptogràfic suplementari, mitjançant la funció d'establiment de les claus..

– Substitució de material criptogràfic, mitjançant les funcions de regeneració de claus, actualització de claus o derivació de claus.

La UOC ha de documentar els procediments d'instal·lació del material criptogràfic, d'acord amb els manuals i les instruccions tècniques dels proveïdors del programari i maquinari criptogràfic corresponent.

El procediment per a la instal·lació inicial del material criptogràfic ha d'incloure obligatòriament la protecció del material criptogràfic durant el procés de càrrega al maquinari i programari criptogràfic, d'acord amb els nivells de seguretat adequats.

En cap cas no s'ha d'emprar per a fer operacions cap material criptogràfic que vingui carregat pel proveïdor del maquinari i programari criptogràfic. Aquest material només es pot utilitzar per a fer proves.

4.5. Establiment de les claus criptogràfiques

L'establiment de les claus criptogràfiques consisteix en la generació i distribució, o en la negociació, de material criptogràfic per a la protecció de les informacions.

La generació de claus de tots els tipus s'ha de portar a terme en mitjans aïllats dels sistemes d'explotació.

Es recomana generar les claus que es fan servir en els següents procediments i activitats acadèmics i de gestió electrònics de la UOC emprant maquinari criptogràfic certificat d'acord amb els estàndards indicats en la secció 4.5 de la política de seguretat criptogràfica de la Universitat:

– Claus de les seus electròniques, perfil del contractant, de nivell mitjà o superior.

– Claus dels certificats de persona jurídica a nom de la UOC, de nivell mitjà o superior.

– Claus dels certificats digitals de personal al servei de la UOC, quan s'hagin d'emprar en sistemes de nivell mitjà o superior.

En tot cas, s'han d'aplicar a les claus criptogràfiques les mesures de seguretat que s'identifiquen en la *política de seguretat criptogràfica* de la UOC, tant quan estiguin en trànsit, com quan estiguin emmagatzemades en el maquinari i programari criptogràfic.

La UOC ha d'aprovar un *estàndard tècnic de paràmetres i longituds de claus*, aplicable als procediments d'establiment de claus.

4.5.1. Generació i distribució de claus asimètriques

Les claus asimètriques s'han de generar d'acord amb les especificacions dels estàndards criptogràfics aprovats en la *política de seguretat criptogràfica* de la UOC

La generació de les claus es pot fer de les maneres següents:

– Directament per l'usuari titular de les claus. En aquest cas, la clau no s'ha de distribuir a cap altra entitat, amb excepció de la clau privada d'un parell de claus emprada per a xifratge, que podrà ser emmagatzemada per la UOC.

– Mitjançant una instal·lació segura, que lliurarà les claus a l'usuari.

– En col·laboració entre l'usuari i la instal·lació segura.

Es recomana que les claus que es fan servir per a la signatura electrònica siguin sempre generades directament pels usuaris, per tal de facilitar la irrefutabilitat dels seus actes.

4.5.1.1. Distribució de claus públiques estàtiques

Les claus públiques estàtiques corresponents a les claus privades s'han de distribuir oferint les garanties mínimes següents:

– El titular de la clau és conegut, excepte en els casos en què és acceptable l'anonimat.

– El propòsit i l'ús de la clau són coneguts.

– La clau pública és vàlida.

– L'usuari posseeix la clau privada corresponent.

El principal mecanisme per a distribuir claus públiques estàtiques és l'ús de certificats digitals, dins d'una infraestructura de clau pública (PKI).

4.5.1.1.1. Distribució de les claus del punt de confiança de la PKI

Les infraestructures de clau pública (PKI) exigeixen que la UOC obtingui garanties suficients en relació amb la identitat de les entitats de certificació que emeten certificats digitals, mitjançant un procediment de distribució segura de les claus del punt de confiança de la PKI:

– La distribució inicial de la clau pública d'un punt de confiança s'hauria de fer dins del procediment de sol·licitud del certificat de l'usuari, en forma de certificat arrel autosignat. S'han d'establir mesures addicionals de seguretat per a garantir la identitat i la fiabilitat de l'entitat de certificació, mesures que cal obtenir prèviament i fora de línia (per exemple, establint una relació amb l'entitat de certificació).

– El procés anterior ha de protegir la informació del punt de confiança que se subministra a l'usuari.

Els *estàndards tècnics d'autenticació, de signatura electrònica, de xifratge i d'evidència electrònica* han de determinar els punts fiables exactes acceptats per a cada ús.

4.5.1.1.2. Enviament de les claus públiques a l'entitat de registre o a l'entitat de certificació

Les claus públiques de l'usuari s'han d'enviar a l'entitat de registre o a l'entitat de certificació perquè les certifiquin, la qual cosa permetrà distribuir la clau pública de cada usuari protegida i de manera fiable.

La identificació de l'usuari s'ha d'haver establert d'acord amb el que disposa la secció 4.1 d'aquesta política per a subministrar el certificat a l'usuari. La identificació ha de ser única per a cada usuari d'un domini concret.

Amb aquesta finalitat, s'han d'establir mecanismes de prova de possessió de la clau privada per part de l'usuari, d'acord amb les instruccions de cada entitat de certificació. Els mètodes acceptables són els següents:

– Lliurament presencial de la clau pública i altres informacions per part de l'usuari, o per part d'un representant de l'usuari (identificació presencial).

– Lliurament remot de la clau pública i altres informacions per part de l'usuari, que s'autentica amb un valor secret subministrat per l'entitat de registre o l'entitat de certificació a un representant de l'usuari (identificació remota).

Aquest mètode permet la generació de lots d'identificadors, que es distribuiran als usuaris que han d'obtenir certificats.

Si el valor secret es genera en presència de l'usuari, no han de passar més de 24 hores fins que es faci servir per a obtenir el certificat.

– Lliurament remot de la clau pública i altres informacions per part de l'usuari, identificat amb un certificat ja existent (encadenament de sol·licituds).

– Lliurament remot de la clau pública i altres informacions per part de l'usuari, o per part d'un representant de l'usuari, sense comprovació prèvia d'identitat (identificació diferida). En aquest cas, l'entitat de registre o l'entitat de certificació lliuren un valor

secret a l'usuari, emprant un intermediari fiable, com el servei de correu postal certificat.

4.5.1.1.3. Distribució de les claus criptogràfiques al públic

Les claus públiques es poden distribuir al públic en general emprant diversos mètodes:

– Distribució manual de la clau pública per part de l'usuari, per exemple, lliurada presencialment o fent servir un intermediari fiable. En aquest cas no hi ha certificats digitals.

– Distribució manual o electrònica del certificat digital que conté la clau pública per part de l'usuari o d'un repositori de certificats.

– Distribució electrònica de la clau pública emprant un protocol de comunicacions que en protegeix la integritat i l'autenticitat. En aquest cas no hi ha certificats digitals.

4.5.1.2. Distribució de claus públiques efímeres

Quan s'utilitzin, les claus efímeres s'han de distribuir fent servir un protocol segur de negociació de claus, que ha de donar als destinataris les garanties que s'indiquen en la secció 4.5.1 d'aquesta política.

4.5.1.3. Distribució de parells de claus generades de manera centralitzada

La generació centralitzada de parells de claus s'ha de fer emprant maquinari criptogràfic certificat d'acord amb el que estableix la *política de seguretat criptogràfica* de la UOC.

Aquestes claus no s'han de fer servir per a produir signatures electròniques dels usuaris, ja que no ofereixen garanties suficients d'irrefutabilitat.

Les claus generades de manera central s'han de lliurar exclusivament als usuaris, protegint la confidencialitat de les claus privades i l'autenticació de l'usuari en el moment de lliurar-les-hi. El parell de claus es pot distribuir mitjançant procediments manuals o electrònics, amb les mateixes proteccions que per a una clau simètrica.

Quan s'utilitzin procediments de coneixement compartit per a la distribució manual del parell de claus, s'ha de dividir la clau en components, amb les mateixes propietats de seguretat que la clau original.

4.5.2. Generació i distribució de claus simètriques

Les claus simètriques s'han de generar d'acord amb les especificacions dels estàndards criptogràfics aprovats en la *política de seguretat criptogràfica* de la UOC.

Les claus simètriques han de ser, alternativament:

– Generades i distribuïdes manualment, o utilitzant un mecanisme de transport de clau pública, o fent servir una clau de xifratge prèviament acordada o distribuïda.

– Establertes mitjançant un mètode de negociació de claus (la generació i la distribució es duen a terme en un mateix procés).

– Determinades per un procés d'actualització de claus.

– Derivades d'una clau mestra.

4.5.2.1. Generació de claus

Les claus simètriques determinades per generació de claus s'han de produir utilitzant un generador de nombres aleatoris aprovat per la UOC, o s'han de crear a partir d'una clau prèvia durant un procés d'actualització de claus, o derivades d'una clau mestra utilitzant una funció de derivació de claus aprovada per la Universitat.

Quan s'utilitzin procediments de coneixement compartit per a la distribució manual de la clau, s'ha de dividir la clau en components, amb les mateixes propietats de seguretat que la clau original.

4.5.2.2. Distribució de claus

Les claus següents s'han de distribuir de manera manual o electrònica:

– Claus generades per a xifrar altres claus (embolcallament de claus).

– Claus generades com a clau inicial d'una actualització de claus.

– Claus generades com a clau mestra per a derivar altres claus.

– Claus generades per a la protecció d'informacions.

Les claus generades per a protegir informació emmagatzemada no s'haurien de distribuir, excepte per causa de còpia de seguretat o per a lliurar-les a altres entitats autoritzades a accedir-hi.

4.5.2.2.1. Distribució manual de claus

Les claus distribuïdes de manera manual s'han de protegir durant el procés de distribució. Les claus secretes s'han de xifrar o protegir mitjançant proteccions físiques adequades. Addicionalment, es poden fer servir procediments de coneixement compartit.

El procediment ha de garantir que:

– La distribució de la clau l'ha iniciat una font autoritzada.

– Qualsevol entitat que distribueix claus en text net és fiable per a l'entitat que genera les claus i per a l'entitat que les rep.

– Les claus estan protegides.

– Les claus són rebudes pel destinatari autoritzat.

Quan les claus es distribueixin xifrades, s'ha d'utilitzar un mecanisme d'embolcallament de clau, amb una clau que s'ha d'emprar només per a aquesta finalitat, o un mecanisme de transport de clau basat en una clau pública del destinatari, en tots dos casos aprovats per la UOC. Les claus d'embolcallament o de transport s'han d'haver distribuït prèviament d'acord amb aquesta política.

Quan es facin servir procediments basats en el coneixement compartit, cada component de la clau s'ha de xifrar o distribuir de manera separada per canals segurs a destinataris diferents. Es recomana utilitzar procediments de seguretat física per a protegir cada component de la clau, com a informació sensible.

Quan les claus es distribueixin en text net, es recomana aplicar mesures de registre d'accions i auditoria en el procediment de distribució, d'acord amb el que estableixen les seccions 7.1 i 7.2 d'aquesta política.

4.5.2.2.2. Distribució electrònica de claus / transport de claus

Quan les claus es distribueixin electrònicament, s'ha d'emprar un mecanisme d'embolcallament de clau, amb una clau que s'ha de fer servir només per a aquesta finalitat, o un mecanisme de transport de clau basat en clau pública del destinatari, en tots dos casos aprovats per la UOC.

Les claus d'embolcallament o de transport s'han d'haver distribuït prèviament d'acord amb aquesta política.

4.5.2.3. Negociació de claus

Només es poden utilitzar mecanismes de negociació de claus aprovats per la UOC.

Els mecanismes de negociació de claus poden emprar les claus següents:

– Claus simètriques de xifratge.

– Claus asimètriques estàtiques.

– Claus asimètriques efímeres.

– Combinació de les anteriors.

Els parells de claus s'han de generar i distribuir d'acord amb el que estableix la secció 4.5.1 d'aquesta política. El material criptogràfic produït s'ha de protegir d'acord amb el que disposa la *política de seguretat criptogràfica* de la UOC.

El mecanisme de negociació de claus ha de garantir que:

– Cada entitat en el procés de negociació de claus coneix l'identificador de la resta d'entitats participants.

– Les claus emprades estan associades correctament amb les entitats participants en el procés de negociació de claus.

– Les claus derivades són correctes.

4.5.3. Generació i distribució d'altre material criptogràfic

Les claus criptogràfiques habitualment es generen de manera conjunta o utilitzant altres materials criptogràfics, que s'han de protegir d'acord amb la *política de seguretat criptogràfica* de la UOC.

4.5.3.1. Paràmetres de domini

Els paràmetres de domini, que són utilitzats per alguns algorismes de clau pública per a la generació de claus, es poden distribuir de manera similar a les claus públiques a les quals estan associats, o bé publicant-los en un lloc específic.

S'ha d'obtenir una garantia de la validesa dels paràmetres de domini abans d'utilitzar-los, en els termes publicats per cada entitat de certificació a la seva normativa o Declaració de pràctiques de certificació.

4.5.3.2. Vectors d'inicialització

Els vectors d'inicialització, que són utilitzats per alguns algorismes de clau simètrica per a diversos modes d'operació de xifratge, i per a l'autenticació, es poden distribuir de la mateixa manera que les claus a les quals estan associats, o amb la informació que utilitza el vector com a part del mecanisme de xifratge o autenticació.

4.5.3.3. Secrets compartits

Els secrets compartits, que es fan servir durant el procés de negociació de claus per a la derivació de claus, s'han de generar d'acord amb el mecanisme de negociació de claus i no s'han de distribuir.

4.5.3.4. Llavors de generadors de nombres aleatoris

Les llavors, que s'utilitzen conjuntament amb generadors deterministes de nombres aleatoris, s'han de protegir quan siguin distribuïdes.

4.5.3.5. Resultats intermedis

Els resultats intermedis, que es generen durant algunes operacions criptogràfiques específiques, no s'han de distribuir en cap cas.

4.6. Registre de les claus criptogràfiques

El registre de les claus criptogràfiques consisteix en la vinculació del material criptogràfic amb alguns atributs determinats de l'usuari, com ara la seva identificació, l'ús previst per a la clau, el nivell de confiança, informació de l'autorització o altres dades.

El registre es pot fer mitjançant qualsevol mecanisme fiable que utilitzi la criptografia com a mecanisme de protecció de la vinculació, com, per exemple, servidors de domini Kerberos (que es valen de la criptografia simètrica) o certificats digitals emesos per una entitat de certificació (que es valen de la criptografia asimètrica). La UOC ha de determinar el procediment de registre de les claus criptogràfiques.

5. Normes aplicables en la fase d'operació

Les gestions en la fase d'operació criptogràfica inclouen les següents:

– L'emmagatzematge ordinari de les claus criptogràfiques. En aquest procediment, el material criptogràfic està emmagatzemat per a fer-ne un ús normal, amb les mesures de protecció determinades en la *política de seguretat criptogràfica* de la UOC i en aquesta política.

– La continuïtat de les operacions criptogràfiques. En aquest procediment, per a oferir continuïtat en les operacions, el material criptogràfic s'ha de poder recuperar, mitjançant còpies de seguretat o recreació de les claus.

– La substitució de les claus criptogràfiques. En aquest procediment, al final del període criptogràfic, les claus s'han de substituir i destruir, mitjançant diferents mecanismes de substitució de claus.

– La derivació de claus criptogràfiques. En aquest procediment, es generen noves claus a partir de claus ja existents, que s'apliquen a usos diferents de les claus originals.

5.1. Emmagatzematge ordinari de les claus criptogràfiques

L'emmagatzematge ordinari de les claus consisteix en la custòdia de les claus per a fer-ne un ús normal, que es pot portar a terme en la memòria d'un maquinari criptogràfic, en un mitjà accessible de manera immediata per un maquinari criptogràfic, o en un suport de sistema operatiu o aplicació.

5.1.1. Emmagatzematge en un dispositiu o mòdul criptogràfic

El material criptogràfic es pot emmagatzemar en el dispositiu o mòdul criptogràfic que fa les operacions criptogràfiques (protecció, verificació o remoció de protecció criptogràfica de la informació), amb les mesures de protecció que s'indiquen en la *política de seguretat criptogràfica* de la UOC.

5.1.2. Emmagatzematge en un mitjà accessible de manera immediata

El material criptogràfic es pot emmagatzemar en un mitjà que sigui accessible de manera immediata pel dispositiu o mòdul criptogràfic, amb les mesures de protecció que s'indiquen en la *política de seguretat criptogràfica* de la UOC.

5.1.3. Emmagatzematge en un sistema operatiu o aplicació

El material criptogràfic es pot emmagatzemar en un sistema operatiu o en una aplicació concreta, per a utilitzar-lo en sistemes d'informació de fins a categoria mitjana.

5.2. Continuïtat de les operacions criptogràfiques

La continuïtat de les operacions criptogràfiques consisteix en la possibilitat de mantenir el sistema operatiu en cas d'incidents que afectin el material criptogràfic (pèrdua, corrupció i altres), mitjançant una còpia de seguretat o la recuperació sense còpia prèvia.

El compromís de les claus afecta la continuïtat de les operacions, i s'ha de fer una avaluació de les claus afectades i una nova generació de tot el material criptogràfic compromès, d'acord amb la secció 4.5 d'aquesta política.

5.2.1. Còpia de seguretat de les claus criptogràfiques

S'han de fer còpies de seguretat de les claus criptogràfiques de les aplicacions de la UOC que tinguin requisits d'alta disponibilitat, per a garantir-ne la recuperació en el temps mínim en cas de desastre; i també còpies de seguretat de les claus emprades en serveis de confidencialitat utilitzats en sistemes de categoria mitjana o superior.

La taula següent estableix les claus de les quals es pot fer còpia de seguretat:

Tipus de clau	Possibilitat de fer còpia de seguretat
Clau privada de signatura	No s'admet en el cas de claus de signatura electrònica d'usuaris, ja que afecta la irrefutabilitat de les operacions. Es pot admetre en relació amb claus de signatura d'entitats de certificació.
Clau pública de signatura	S'admet. Es pot desar el certificat digital que la contingui.
Clau simètrica d'autenticació	S'admet.
Clau privada d'autenticació	S'admet, si ho requereix una aplicació.
Clau pública d'autenticació	S'admet. Es pot desar el certificat digital que la contingui.
Clau simètrica de xifratge de dades	S'admet.
Clau simètrica d'embolcallament de claus	S'admet.
Clau (simètrica i asimètrica) de generació de nombres aleatoris	No és necessària i no es recomana.
Clau mestra simètrica	S'admet.
Clau privada de transport de clau	S'admet.
Clau pública de transport de clau	S'admet. Es pot desar el certificat digital que la contingui.
Clau simètrica de negociació de clau	S'admet.
Clau privada estàtica de negociació de clau	No s'admet, excepte quan es necessiti per a la reconstrucció durant la recuperació de claus.
Clau pública estàtica de negociació de clau	S'admet. Es pot desar el certificat digital que la contingui.
Clau privada efímera de negociació de clau	No s'admet.
Clau pública efímera de negociació de clau	S'admet si es necessita per a la reconstrucció durant la recuperació de claus.
Clau simètrica d'autorització	S'admet.

Clau privada d'autorització	S'admet.
Clau pública d'autorització	S'admet. Es pot desar el certificat digital que la contingui.

La taula següent estableix la resta de material criptogràfic del qual es pot fer còpia de seguretat:

Tipus de material	Possibilitat de fer còpia de seguretat
Paràmetres de domini	S'admet.
Vectors d'inicialització	S'admet, si se n'acredita la necessitat.
Secrets compartits	No s'admet.
Llavors de generadors de nombres aleatoris	No s'admet.
Altra informació pública	S'admet.
Resultats intermedis	No s'admet.
Informació de control de claus	S'admet.
Nombre aleatori	Depèn de l'aplicació o de l'ús del generador.
Contrasenya	S'admet.
Informació d'auditoria	S'admet.

5.2.2. Recuperació de les claus criptogràfiques

S'ha de fer una anàlisi del material criptogràfic que cal preservar per tal de poder-lo recuperar posteriorment, cas per cas. La decisió s'ha de basar en els criteris següents:

– El tipus de clau, ja que recuperar claus privades té més implicacions que recuperar claus públiques.

– L'aplicació en què la clau s'ha d'emprar.

– Si la clau és propietat d'una part, de l'altra o compartida.

– El rol de l'usuari en una comunicació electrònica.

– L'algorisme o computació en la qual s'ha d'utilitzar la clau.

Quan es recuperi una clau, s'han de fer les actuacions següents:

– Si la clau s'ha perdut amb la possibilitat d'haver estat compromesa, s'ha de substituir tan aviat com sigui possible després d'haver-la recuperat, per a limitar l'exposició de la clau recuperada i de les dades protegides. S'ha de tornar a protegir la informació amb

una nova clau, que no ha de ser una clau relacionada de cap manera amb la clau compromesa (no pot ser una actualització de la clau).

– Si la clau que s'ha perdut no ha estat compromesa, es pot recuperar i no cal fer cap acció addicional.

5.3. Substitució de les claus criptogràfiques

La substitució de les claus criptogràfiques consisteix a canviar una clau per una altra que fa la mateixa funció, per diferents motius:

– La clau que es vol substituir pot haver estat compromesa.

– El període criptogràfic de la clau arriba a l'acabament.

– Es vol limitar la quantitat d'informació protegida amb una única clau.

Les claus es poden substituir mitjançant una regeneració de les claus criptogràfiques o mitjançant una actualització de les claus criptogràfiques.

5.3.1. Regeneració de les claus criptogràfiques

En la regeneració de les claus criptogràfiques, s'ha de crear una nova clau, que no ha de tenir cap mena de relació amb la clau que es vol substituir, per a la qual cosa s'ha d'utilitzar un dels mètodes previstos en la secció 4.5 d'aquesta política.

La regeneració de claus s'ha de fer servir en els casos de possible compromís de la clau que es vol substituir, o d'acabament del període criptogràfic de la clau que es vol substituir.

5.3.2. Actualització de les claus criptogràfiques

En l'actualització de les claus criptogràfiques, la clau que s'ha de crear depèn de la clau que es vol substituir, i s'ha de fer aplicant una funció irreversible a la clau i la resta de material criptogràfic que es vol substituir.

S'ha de limitar el nombre de vegades que es poden actualitzar les claus criptogràfiques i cal regenerar periòdicament les claus.

L'actualització de les claus criptogràfiques es pot fer servir en cas de voler limitar la quantitat d'informació protegida amb una clau, i no s'ha de fer servir per a substituir una clau compromesa.

5.4. Derivació de claus criptogràfiques

La derivació de claus criptogràfiques consisteix en l'obtenció de claus a partir de claus prèviament existents, dedicades a usos diferents dels usos de les claus originals.

La funció de derivació ha de ser una funció irreversible que garanteixi que les claus secretes no es puguin saber a partir de les claus derivades. No ha de ser possible saber una clau derivada a partir d'una altra clau derivada.

Els mètodes de derivació de claus poden ser els següents:

– Dues parts deriven claus comunes a partir d'un secret compartit.

– Una clau individual es deriva d'una clau mestra.

– Una clau individual es deriva d'una clau mestra i de la contrasenya de l'usuari.

– Una clau individual es deriva de la contrasenya de l'usuari.

6. Normes aplicables en la fase posterior a l'operació

Les gestions en la fase posterior a l'operació criptogràfica inclouen les següents:

– L'emmagatzematge d'arxiu i la recuperació de les claus criptogràfiques. En aquest procediment s'arxiven les claus que ja no són operatives, per a accedir-hi posteriorment en cas que faci falta.

– La baixa de l'usuari. En aquest procediment es retiren les autoritzacions de l'usuari en relació amb les claus.

– La baixa de les claus criptogràfiques. En aquest procediment es retiren les autoritzacions d'ús de les claus i el material criptogràfic associat.

– La destrucció de les claus criptogràfiques. En aquest procediment es destrueixen les claus que ja no es necessiten.

– La revocació de les claus criptogràfiques. En aquest procediment es revoquen les claus abans del seu període criptogràfic ordinari.

6.1. Emmagatzematge d'arxiu i recuperació de les claus criptogràfiques

L'emmagatzematge d'arxiu i recuperació de claus criptogràfiques permet custodiar el material criptogràfic que ja no és operatiu, però que es pot necessitar en el futur.

L'arxiu de claus i material criptogràfic ha d'oferir integritat i control d'accés, i també ha d'implantar les mesures de protecció que s'indiquen en la *política de seguretat criptogràfica* de la UOC.

Les dades arxivades s'haurien d'emmagatzemar de manera separada d'altres dades operatives i s'haurien d'arxivar en mitjans aïllats dels mitjans d'explotació.

S'hauria de disposar de diverses còpies de seguretat de l'arxiu de claus. Els arxius de claus que protegeixen informació crítica s'han de distribuir geogràficament.

Les claus i la resta de material criptogràfic s'haurien d'arxivar abans de l'acabament del seu període criptogràfic. Quan no siguin necessàries, les claus s'han de destruir.

La taula següent estableix les claus que es poden arxivar:

Tipus de clau	Possibilitat d'arxivament i període de retenció
Clau privada de signatura	No s'admet.
Clau pública de signatura	S'admet, mentre sigui necessària per a verificar dades signades amb la clau privada associada.
Clau simètrica d'autenticació	S'admet, mentre sigui necessària per a autenticar dades.
Clau privada d'autenticació	No s'admet.
Clau pública d'autenticació	S'admet, mentre sigui necessària per a verificar dades signades amb la clau privada associada.

Clau simètrica de xifratge de dades	S'admet, mentre sigui necessària per a desxifrar dades xifrades amb aquesta clau.
Clau simètrica d'embolcallament de claus	S'admet, mentre sigui necessària per a desxifrar claus xifrades amb aquesta clau.
Clau (simètrica i asimètrica) de generació de nombres aleatoris	No s'admet.
Clau mestra simètrica	S'admet, mentre sigui necessària per a derivar altres claus de dades arxivades.
Clau privada de transport de clau	S'admet, mentre sigui necessària per a desxifrar claus xifrades amb aquesta clau.
Clau pública de transport de clau	No s'admet.
Clau simètrica de negociació de clau	S'admet.
Clau privada estàtica de negociació de clau	No s'admet, excepte que es necessiti per a reconstruir claus.
Clau pública estàtica de negociació de clau	S'admet, mentre sigui necessària per a reconstruir claus.
Clau privada efímera de negociació de clau	No s'admet.
Clau pública efímera de negociació de clau	S'admet.
Clau simètrica d'autorització	No s'admet.
Clau privada d'autorització	No s'admet.
Clau pública d'autorització	No s'admet.

La taula següent estableix la resta de material criptogràfic que es pot arxivar:

Tipus de material	Possibilitat d'arxivament i període de retenció
Paràmetres de domini	S'admet, fins que tot el material de claus, signatures i dades signades que utilitzen els paràmetres de domini siguin eliminats.
Vectors d'inicialització	S'admet, mentre siguin necessaris per a processar les dades protegides.
Secrets compartits	No s'admet.
Llavors de generadors de nombres aleatoris	No s'admet.
Altra informació pública	S'admet, mentre sigui necessària per a processar dades emprant-la.
Resultats intermedis	No s'admet.
Informació de control de claus	S'admet, fins que la clau associada s'elimini.
Nombre aleatori	No s'admet.
Contrasenya	Només s'admet per a detectar la reutilització de contrasenyes repetides, mentre sigui necessari.
Informació d'auditoria	S'admet, mentre sigui necessària.

6.2. Baixa de l'usuari

S'han de donar de baixa els usuaris que deixen de tenir autoritzacions en relació amb les operacions criptogràfiques i les claus que es fan servir per a aquestes operacions, per a impedir a altres usuaris que confiïn en aquest usuari.

Tots els registres de l'usuari i les seves associacions s'haurien de marcar per a indicar que aquest usuari ha estat donat de baixa, tot i que els registres no s'han d'esborrar.

No s'han de reutilitzar els identificadors dels usuaris donats de baixa.

6.3. Baixa de les claus criptogràfiques

S'haurien de donar de baixa les claus i la resta de material criptogràfic quan no són necessaris o quan la informació associada esdevé invàlida.

Tots els registres de claus i material criptogràfic s'haurien de marcar per a indicar que s'han donat de baixa.

En el cas de les claus asimètriques públiques certificades, la baixa s'ha de fer mitjançant la revocació del certificat digital corresponent.

6.4. Destrucció de les claus criptogràfiques

Totes les claus simètriques i les claus asimètriques privades s'han de destruir per a reduir el risc de compromís.

Tots els suports en què s'emmagatzemin materials criptogràfics en text net que requereixin protecció de confidencialitat, s'han d'esborrar d'una manera tal que no quedin rastres del material criptogràfic que siguin recuperables per mitjans físics o electrònics.

6.5. Revocació de les claus criptogràfiques

S'han de documentar els procediments de revocació de totes les claus criptogràfiques emprades per la UOC. Si la clau que s'ha de revocar s'utilitza en una relació bilateral, la part que la revoqui ho ha de comunicar a l'altra part. Si la clau que s'ha de revocar s'ha registrat en una infraestructura (per exemple, una PKI), la part ha d'informar la infraestructura que la clau s'ha de revocar (sol·licitud de revocació) i la infraestructura ha de donar de baixa la clau.

7. Altres normes

7.1. Registre d'accions

S'han de registrar les principals accions relacionades amb les claus i altre material criptogràfic i, en particular, l'accés de tots els usuaris que tenen accés a claus en text net.

7.2. Auditoria

S'haurien de fer les auditories periòdiques següents:

– Auditoria trimestral de les accions dels usuaris humans que utilitzen i mantenen, i hi operen, el maquinari i programari criptogràfic centralitzat, per a detectar esdeveniments molt poc usuals que puguin comprometre la seguretat.

– Auditoria anual del pla de seguretat i dels procediments de gestió de claus, per a garantir que ofereixen suport a la *política de seguretat criptogràfica* i a aquesta política.

– Auditoria anual dels mecanismes de protecció de les claus i altre material criptogràfic, d'acord amb el nivell de seguretat necessari per a cada clau, per a garantir que ofereixen suport a la *política de seguretat criptogràfica* i a aquesta política.

En la realització de les auditories s'han de tenir en compte els nous desenvolupaments tecnològics i les noves tipologies d'atacs.

8. Annex. Llista de procediments de gestió de claus

Fase prèvia a l'operació:

- Procediment/s de registre d'usuaris.
- Procediment/s d'inicialització de sistemes criptogràfics.
- Procediment/s d'inicialització d'usuaris.
- Procediment/s d'instal·lació de material criptogràfic.
- Procediment/s de generació i distribució de claus.
- Procediment/s de registre de claus.

Fase d'operació:

- Procediment/s d'emmagatzematge ordinari de les claus criptogràfiques.
- Procediment/s de continuïtat de les operacions criptogràfiques.
- Procediment/s de substitució de les claus criptogràfiques.
- Procediment/s de derivació de claus criptogràfiques.

Fase posterior a l'operació:

- Procediment/s d'emmagatzematge d'arxiu i recuperació de les claus criptogràfiques.
- Procediment/s de baixa d'usuaris.
- Procediment/s de baixa de claus criptogràfiques.
- Procediment/s de destrucció de claus criptogràfiques.
- Procediment/s de revocació de claus criptogràfiques.