Política de seguretat criptogràfica de la Universitat Oberta de Catalunya

Text aprovat pel Comitè de Direcció Executiu el 5 de febrer de 2015, actuant per delegació del Consell de Govern.

Universitat Oberta de Catalunya

SUMARI

I. Introducció

Aquest document conté les normes de seguretat criptogràfica 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 seguretat criptogràfica és un document que especifica normes d'ús amb relació a la criptografia, i inclou estàndards per a la seva implantació en l'organització. Alguns dels usos de la criptografia inclouen els mecanismes d'autenticació, signatura electrònica i irrefutabilitat, confidencialitat o integritat.

Aquesta política és conforme amb els requisits de seguretat i proporcionalitat corresponents als sistemes electrònics de suport a procediments administratius, establerts en les normes que regulen l'ús dels mitjans electrònics en els serveis públics.

Els continguts d'aquesta política de seguretat criptogràfica s'han estructurat per a cobrir els controls que preveu la norma internacional ISO/IEC 27002:2006 i les recomanacions contingudes en les Guies de Seguretat de les TIC CCN-STIC-405 i CCN-STIC-807 del Centre Criptològic Nacional.

II. Continguts generals de la Política de seguretat criptogràfica

1. Identificació

Aquesta política de seguretat criptogràfica s'identifica amb l'identificador d'objecte (OID) següent: 1.3.6.1.4.1.43653.1.1.

2. Data d'emissió

Aquesta política ha estat emesa en data de 5 de febrer de 2015, moment a partir del qual entra en vigor.

3. Identificació de l'emissor de la Política de seguretat criptogràfica

Aquesta política ha estat emesa pel Comitè de Direcció Executiu, actuant per delegació del Consell de Govern d'acord amb el que estableix l'article 13.2 de les NOF (Acord GOV /140/2010, de 3 d'agost), l'article 4 del Reglament del Consell de Govern i l'Acord de Consell de Govern de 15 de juliol de 2013.

4. Àmbit d'aplicació de la Política de seguretat criptogràfica

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

III. Utilització de la criptografia a la UOC

1. Serveis de seguretat basats en criptografia

La UOC empra la criptografia per a oferir els serveis de seguretat següents:

- Serveis de confidencialitat
- Serveis d'integritat de dades
- Serveis d'autenticació
- Serveis d'autorització
- Serveis d'irrefutabilitat
- Serveis accessoris

Els serveis de seguretat fan ús dels algorismes criptogràfics aprovats en aquesta política.

Les normatives de desplegament d'aquesta política han d'indicar l'aplicació de criptografia en cada cas i escenari concrets:

- Signatura electrònica
- Autenticació electrònica
- Xifratge
- Prova electrònica

2. Algorismes criptogràfics aprovats

Els algorismes criptogràfics aprovats per a l'ús per la UOC són els següents.

- Algorismes de resum aprovats

  - SHA-1,[1] definit en la norma internacional ISO/IEC 10118-3 (2004): «Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions» i en la norma FIPS 180-2 (2002): «Secure Hash Standard».

    SHA-1 és l'algorisme més usat actualment, tot i que es recomana no emprar-lo, sempre que la infraestructura tecnològica ho permeti.

  - SHA-224,[2] definit en la norma FIPS 180-2 (2002): «Secure Hash Standard» (change notice 1, de 2004).

  - SHA-256,[3] definit en la norma internacional ISO/IEC 10118-3 (2004): «Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions» i en la norma FIPS 180-2 (2002): «Secure Hash Standard».

[1] Secció 1.2.1k) CCN STIC 807

[2] Secció 1.2.1 k) CCN STIC 807

- SHA-384,[4] definit en la norma FIPS 180-2 (2002): «Secure Hash Standard».
- SHA-512,[5] definit en la norma FIPS 180-2 (2002): «Secure Hash Standard».

- Algorismes simètrics aprovats

  - AES,[6] definit en la norma FIPS 197 (2001): «Specification for the Advanced Encryption Standard (AES)».
  - TDEA[7] (per exemple, Triple DES), definit en l'especificació NIST SP 800-67 (2004, revisat el 2008): «Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher», amb la recomanació d'emprar tres claus diferents.

    Es recomana emprar els modes criptogràfics d'operació definits en l'especificació NIST SP 800-38A (2001): «Recommendation for Block Cipher Modes of Operation - Methods and Techniques».

- Algorismes asimètrics aprovats

  - RSA,[8] definit en l'especificació tècnica IETF RFC 3447 (2003): «Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1».
  - DSA,[9] definit en la norma internacional ISO/IEC 14888-3 (2006): «Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms» i en la norma FIPS 186-2 (2000): «Digital Signature Standard».
  - EC-DSA,[10] en les seves dues variants E(Fp) i E(F2m), definit en la norma internacional ISO/IEC 14888-3 (2006): «Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms».
  - EC-GDSA, en les seves dues variants E(Fp) i E(F2m), definit en la norma internacional ISO/IEC 15946-2 (2002): «Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures».

- Algorismes d'establiment de claus aprovats

  - Algorismes DLC, definits en l'especificació NIST SP 800-56A (2007): «Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography».
  - Algorisme de transport de claus RSA.

---

[3] Secció 1.2.1 k) CCN STIC 807
[4] Secció 1.2.1 k) CCN STIC 807
[5] Secció 1.2.1 k) CCN STIC 807
[6] Secció 1.2.1 b) CNN STIC 807
[7] Secció 1.2.1 a) CNN STIC 807
[8] Secció 1.2.1 i) CNN STIC 807
[9] Secció 1.2.1 g) CNN STIC 807
[10] Secció 1.2.1 h) CNN STIC 807

- Algorismes d'embolcallament de claus amb clau simètrica.

3. Requisits de protecció de claus criptogràfiques

Les claus criptogràfiques han d'estar disponibles operativament tant temps com ho requereixi el servei criptogràfic corresponent. Les claus es poden mantenir en un equipament criptogràfic mentre s'utilitzen, o es poden emmagatzemar de manera externa —amb les mesures de seguretat adequades— i recuperar-les quan sigui necessari.

A més, algunes de les claus s'han d'arxivar durant un termini superior a l'inicialment previst per a l'ús de l'emissor.

La taula següent indica, per a cada tipus de clau, els requisits de protecció corresponents.

Tipus de clau	Servei de seguretat	Protecció de seguretat	Dades associades a protegir	Garantia requerida	Període de protecció
Clau privada de signatura	Autenticació Integritat Irrefutabilitat	Integritat Confidencialitat	Ús o aplicació Paràmetres de domini Clau pública de signatura	Possessió	Des que es genera fins que s'acaba el període de la seva validesa criptogràfica
Clau pública de signatura	Autenticació Integritat Irrefutabilitat	Arxiu Integritat	Ús o aplicació Propietari del parell de claus Paràmetres de domini Clau privada de signatura Dades signades	Validesa	Des que es genera fins que no sigui necessari verificar les dades protegides
Clau simètrica d'autenticació	Autenticació Integritat	Arxiu Integritat Confidencialitat	Ús o aplicació Altres entitats autoritzades Dades autenticades	No aplica	Des que es genera fins que s'acaba el període de la seva validesa criptogràfica
Clau privada d'autenticació	Autenticació Integritat	Integritat Confidencialitat	Ús o aplicació Clau pública d'autenticació Paràmetres de domini	Possessió	Des que es genera fins que s'acaba el període de la seva validesa criptogràfica
Clau pública d'autenticació	Autenticació Integritat	Arxiu Integritat	Ús o aplicació Propietari del parell de claus Dades	Validesa	Des que es genera fins que no sigui necessari autenticar els dades protegides

			autenticades Clau privada d'autenticació Paràmetres de domini		
Clau simètrica de xifratge de dades	Confidencialitat	Arxiu Integritat Confidencialitat	Ús o aplicació Altres entitats autoritzades Dades xifrades Dades en clar	No aplica	Des que es genera fins que s'acaba la vida de les dades o s'acaba el període de validesa criptogràfica
Clau simètrica d'embolcallament de claus	Suport	Arxiu Integritat Confidencialitat	Ús o aplicació Altres entitats autoritzades Claus xifrades	No aplica	Des que es genera fins que s'acaba el període de la seva validesa criptogràfica o fins que les claus embolcallades no necessitin protecció, el més llarg dels dos períodes
Clau (simètrica i asimètrica) de generació de nombres aleatoris	Suport	Integritat Confidencialitat	Ús o aplicació	Possessió de la clau privada, quan s'utilitza	Des que es genera fins a la seva reposició
Clau mestra simètrica	Suport	Arxiu Integritat Confidencialitat	Ús o aplicació Altres entitats autoritzades Claus derivades	No aplica	Des que es genera fins que s'acaba el període de la seva validesa criptogràfica o de les claus derivades, el més llarg dels dos períodes
Clau privada de transport de clau	Confidencialitat Integritat	Arxiu Integritat Confidencialitat	Ús o aplicació Claus xifrades Paràmetres de domini Clau pública de transport de claus	Possessió	Des que es genera fins que s'acaba el període de protecció de totes les claus transportades
Clau pública de transport de clau	Confidencialitat Integritat	Arxiu Integritat	Ús o aplicació Propietari del parell de claus Clau privada de transport de claus	Validesa	Des que es genera fins que s'acaba el període de la seva validesa criptogràfica
Clau simètrica de negociació de clau	Suport	Arxiu Integritat Confidencialitat	Ús o aplicació Altres entitats autoritzades	No aplica	Des que es genera fins que s'acaba el període de la seva validesa criptogràfica o fins que no sigui necessària en relació amb una clau determinada, el més llarg dels dos períodes

Clau privada estàtica de negociació de clau	Suport	Arxiu Integritat Confidencialitat	Ús o aplicació Paràmetres de domini Clau pública de negociació de clau estàtica	Possessió	Des que es genera fins que s'acaba el període de la seva validesa criptogràfica o fins que no sigui necessària en relació amb una clau determinada, el més llarg dels dos períodes
Clau pública estàtica de negociació de clau	Suport	Arxiu Integritat	Ús o aplicació Propietari del parell de claus Paràmetres de domini Clau privada de negociació de clau estàtica	Validesa	Des que es genera fins que s'acaba el període de la seva validesa criptogràfica o fins que no sigui necessària en relació amb una clau determinada, el més llarg dels dos períodes
Clau privada efímera de negociació de clau	Suport	Integritat Confidencialitat	Ús o aplicació Paràmetres de domini Clau pública de negociació de clau efímera	No aplica	Des que es genera fins que s'acaba el procés de negociació de claus, amb destrucció immediata
Clau pública efímera de negociació de clau	Suport	Integritat	Ús o aplicació Propietari del parell de claus Paràmetres de domini Clau privada de negociació de clau efímera	Validesa	Des que es genera fins que s'acaba el procés de negociació de claus, amb destrucció immediata
Clau simètrica d'autorització	Autorització	Integritat Confidencialitat	Ús o aplicació Altres entitats autoritzades	No aplica	Des que es genera fins que s'acaba el període de la seva validesa criptogràfica
Clau privada d'autorització	Autorització	Integritat Confidencialitat	Ús o aplicació Paràmetres de domini Clau pública d'autorització	Possessió	Des que es genera fins que s'acaba el període de la seva validesa criptogràfica
Clau pública d'autorització	Autorització	Integritat	Ús o aplicació Propietari del parell de claus Paràmetres de domini Clau privada d'autorització	Validesa	Des que es genera fins que s'acaba el període de la seva validesa criptogràfica

4. Requisits de protecció d'altre material criptogràfic

Tipus de material	Servei de seguretat	Protecció de seguretat	Dades associades a protegir	Període de protecció
Paràmetres de domini	Depèn de la clau associada als paràmetres de domini	Arxiu Integritat	Ús o aplicació Claus privada i pública	Des que es generen fins que no siguin necessaris per a generar claus o verificar signatures
Vectors d'inicialització	Depèn de l'algorisme	Arxiu Integritat	Dades protegides	Des que es generen fins que no siguin necessaris per a processar dades protegides
Secrets compartits	Suport	Confidencialitat Integritat	No aplica	Des que es generen fins que s'acaba la transacció. Es destrueixen quan s'acaba el període de protecció
Llavors de generadors de nombres aleatoris	Suport	Confidencialitat Integritat	Ús o aplicació	S'utilitzen una vegada i es destrueixen
Altra informació pública	Suport	Arxiu Integritat	Ús o aplicació Altres entitats autoritzades Dades processades en relació amb valors únics de missatge	Des que es genera fins que no sigui necessària per a processar dades que en depenen
Resultats intermedis	Suport	Confidencialitat Integritat	Ús o aplicació	Des que es generen fins que no siguin necessaris, moment en què s'han de destruir
Informació de control de claus	Suport	Arxiu Integritat	Clau	Des que es genera fins que la clau associada és destruïda
Nombre aleatori	Suport	Integritat Confidencialitat (depèn de l'ús)	No aplica	Des que es genera fins que no sigui necessari, moment en què s'ha de destruir
Contrasenya	Autenticació	Integritat Confidencialitat	Ús o aplicació Entitat propietària	Des que es genera fins que sigui substituïda o no sigui necessària per a autenticar l'entitat
Informació d'auditoria	Suport	Arxiu Integritat Autorització d'accés	Esdeveniments auditats Informació de control de claus	Des que es genera fins que no sigui necessària

5. Mètodes de protecció de seguretat

Les dues taules anteriors determinen diverses proteccions de seguretat amb relació a les claus criptogràfiques i altres materials:

- Integritat
- Confidencialitat
- Arxiu

A continuació es determinen els mètodes acceptables per a aconseguir les proteccions d'integritat i de confidencialitat, tant quan la informació criptogràfica està en trànsit com quan és al seu lloc d'operació. Els estàndards d'infraestructura per a la protecció en la custòdia i l'arxiu de les claus i la resta de material criptogràfic es detallen en l'apartat 5 del punt IV d'aquest document.

5.1. Protecció de la informació criptogràfica en trànsit

La informació criptogràfica en trànsit inclou tota la informació en processos de distribució de claus o de còpia de seguretat i el trasllat a localitzacions diferents del lloc d'operació. Alguns exemples són les claus certificades per terceres entitats de certificació, que viatgen des d'aquesta entitat fins a la destinació d'operació, o les claus que ja han arribat a la fi del seu període d'operació, i que són arxivades de manera definitiva en un tercer proveïdor de seguretat.

La protecció de la integritat d'informació criptogràfica en trànsit s'ha d'aconseguir mitjançant algun dels mecanismes següents:

- En cas de distribució manual, amb protecció física, es pot emprar un mecanisme de control CRC de la informació criptogràfica, pactat entre emissor i receptor, o comprovar que el format de la informació criptogràfica rebuda correspon al que estava previst rebre.

  Exemple: la integritat d'una clau privada de signatura electrònica reconeguda d'una persona es garanteix, durant el seu trànsit, per la protecció física de la targeta criptogràfica que la conté.

- En cas de distribució electrònica, es pot emprar un mecanisme MAC o de signatura digital, sobre la informació criptogràfica o sobre el missatge que la transporta, o comprovar que el format de la informació criptogràfica rebuda correspon al que estava previst rebre.

  Exemple: la integritat d'una clau pública de segell electrònic que es transmet a una entitat de certificació per a la generació del corresponent certificat digital es garanteix mitjançant la signatura del missatge de sol·licitud amb la clau privada del sol·licitant.

La protecció de la confidencialitat d'informació criptogràfica en trànsit s'ha d'aconseguir mitjançant algun dels mecanismes següents:

- En cas de distribució manual, mitjançant protecció física, xifrant la informació criptogràfica amb un algorisme aprovat d'acord amb aquesta política o dividint la informació criptogràfica en components distribuïts per agents o vies independents.

Exemple: la confidencialitat d'una clau privada de signatura electrònica reconeguda d'una persona es garanteix, durant el seu trànsit, per la protecció física de la targeta criptogràfica que la conté.

- En cas de distribució electrònica, xifrant la informació criptogràfica amb un algorisme aprovat d'acord amb aquesta política.

Exemple: la confidencialitat d'una clau privada d'un certificat de signatura de programari generada per l'entitat de certificació es garanteix, durant el seu trànsit, mitjançant el seu lliurament en un contenidor xifrat.

Si es detecta una fallada en la protecció de la seguretat de la informació criptogràfica en trànsit, la UOC ha de fer el següent:

- No emprar la informació criptogràfica rebuda.
- Reintentar l'operació, amb un nombre màxim de tres vegades.
- Generar una incidència, en el seu cas amb l'entitat de certificació participant.

5.2. Protecció de la informació criptogràfica al lloc d'operació

La informació criptogràfica al lloc d'operació inclou tota la informació en dispositius i maquinari al lloc d'operació, i també la informació custodiada en espais d'arxiu o còpia de seguretat. Alguns exemples són el maquinari i el programari que donen suport a les seus electròniques i aplicacions de la UOC.

La protecció de la integritat d'informació criptogràfica al lloc d'operació s'ha d'aconseguir mitjançant algun dels mecanismes següents:

- Mecanismes físics, incloent-hi l'ús de maquinari criptogràfic validat, d'acord amb el que disposa l'apartat 5 del punt IV d'aquesta política; d'ordinadors que no estiguin connectats a altres sistemes, o dipòsits físics per a protegir dispositius o suports (com una caixa forta).

- Mecanismes criptogràfics, com per exemple l'ús de mecanismes MAC o de signatura digital de la informació criptogràfica emmagatzemada, o la comprovació de format de la informació criptogràfica que s'ha d'emprar.

La protecció de confidencialitat d'informació criptogràfica al lloc d'operació s'ha d'aconseguir mitjançant algun dels mecanismes següents:

- Xifratge de la informació emprant un algorisme aprovat d'acord amb aquesta política, en un maquinari criptogràfic validat, d'acord amb el que disposa l'apartat 5 del punt IV d'aquesta política.

- Ús de maquinari criptogràfic validat, d'acord amb el que disposa l'apartat 5 del punt IV d'aquesta política.

- Sistema d'emmagatzematge físic segur, amb garantia de control d'accés al dipòsit.

IV. Criteris per a l'ús de la criptografia

Els serveis criptogràfics s'han d'emprar d'acord amb les normes següents:

- Desenvolupament de la Política
- Separació de l'ús de claus
- Establiment de terminis de durada de les claus
- Establiment de procediments de gestió de claus
- Establiment d'estàndards d'implantació de tecnologia criptogràfica
- Compliment normatiu

1. Desenvolupament de la Política

Correspon l'aprovació de la Política de seguretat criptogràfica al Consell de Govern de la UOC, essent-ne responsable la Secretaria General.

Aquesta política de seguretat criptogràfica s'ha de desplegar mitjançant les normatives següents:

- Política de gestió de claus criptogràfiques de la UOC
- Política de certificació de la UOC
- Política d'autenticació de la UOC
- Política de signatura electrònica de la UOC
- Política de xifratge de la UOC

Correspon a l'Àrea de Tecnologia de la UOC el desenvolupament de la Política de seguretat criptogràfica per mitjà dels instruments indicats.

2. Separació de l'ús de claus

De manera general, una clau només s'ha de fer servir per a un ús concret —per exemple, signatura electrònica, xifratge de dades o autenticació, etc. — pels motius següents:

- L'ús d'una mateixa clau per a dos processos criptogràfics diferents pot debilitar la seguretat d'algun d'aquests processos.
- La limitació d'ús d'una clau permet controlar els danys causats en cas de compromís de la clau.
- Alguns usos de les claus generen problemes col·laterals, perquè tenen períodes de durada o conservació diferents.

Aquesta directriu no impedeix l'ús d'una mateixa clau per a processos que ofereixen més d'un servei criptogràfic. Per exemple: una clau de signatura digital es pot fer servir, d'acord amb aquesta directriu, per a serveis d'integritat, autenticitat i irrefutabilitat.

Es permet de manera expressa l'ús de la clau privada per a sol·licitar la certificació digital de la corresponent clau pública a una entitat de certificació.

3. Terminis de durada de les claus

De manera general, una clau s'ha de fer servir durant un termini concret, o període criptogràfic, pels motius següents:

- Es limita la quantitat d'informació protegida per una clau que està disponible per anàlisi criptogràfica.
- Es limita l'exposició en cas de compromís d'una clau.
- Es limita l'ús d'un algorisme particular al seu període estimat d'ús eficient.
- Es limita el temps disponible per a intentar penetrar els mecanismes d'accés lògic, físic i de procediment que protegeixen una clau de la seva divulgació no autoritzada.
- Es limita el període durant el qual la informació es pot comprometre per divulgació accidental de claus o material criptogràfic a entitats no autoritzades.

S'estableixen els períodes criptogràfics recomanats següents:

Tipus de clau	Període d'ús de l'emissor	Període d'ús del receptor
Clau privada de signatura	1-4 anys	
Clau pública de signatura	Diversos anys (depèn de la longitud de la clau)	
Clau simètrica d'autenticació	Fins a 2 anys	Fins a 3 anys addicionals
Clau privada d'autenticació	1-4 anys	
Clau pública d'autenticació	1-4 anys	
Clau simètrica de xifratge de dades	Fins a 2 anys	Fins a 3 anys addicionals
Clau simètrica d'embolcallament de claus	Fins a 2 anys	Fins a 3 anys addicionals
Clau (simètrica i asimètrica) de generació de nombres aleatoris	Fins a la generació de noves llavors	
Clau mestra simètrica	Fins a 1 any	
Clau privada de transport de clau	Fins a 2 anys	
Clau pública de transport de clau	1-2 anys	
Clau simètrica de negociació de clau	1-2 anys	
Clau privada estàtica de negociació de clau	1-2 anys	
Clau pública estàtica de negociació de clau	1-2 anys	
Clau privada efímera de negociació de clau	Una transacció	
Clau pública efímera de negociació de clau	Una transacció	
Clau simètrica d'autorització	Fins a 2 anys	
Clau privada d'autorització	Fins a 2 anys	

Clau pública d'autorització	Fins a 2 anys

Per a la decisió concreta dels períodes aplicables, s'ha de fer una anàlisi de risc, considerant els factors següents:

- La fortalesa dels mecanismes criptogràfics emprats
- La protecció dels mecanismes emprant equipament criptogràfic segur
- L'entorn d'operació (instal·lacions d'accés controlat, equipament d'oficina o terminal d'accés públic)
- El volum d'informació o el nombre de transaccions que cal protegir
- La classificació de seguretat de les dades
- La funció de seguretat involucrada (xifratge de dades, signatura digital, producció, negociació o protecció de claus)
- El mètode de regeneració de les claus
- El mètode d'actualització o de derivació de les claus
- El nombre de nodes de xarxa que eventualment comparteixen una clau
- El nombre de còpies d'una clau i de distribució de les còpies
- Les amenaces a la seguretat de les claus

Cal també considerar de manera particular les restriccions derivades de les normes i polítiques de les entitats de certificació externes, ja que en molts casos són les entitats de certificació les que fixen els períodes criptogràfics.

En aquest sentit, s'autoritza l'acceptació de períodes criptogràfics superiors als recomanats, sempre que es tracti de claus garantides en certificats reconeguts emesos complint la legislació de signatura electrònica.

4. Procediments de gestió de les claus

S'han d'establir els procediments següents amb relació als aspectes següents:

- Generació de claus per diferents sistemes criptogràfics i aplicacions.
- Generació i obtenció de certificats de clau pública.
- Distribució de claus als usuaris, incloent-hi l'activació una vegada hagin estat rebudes. Emmagatzematge de claus, incloent-hi com obtenen accés a les claus els usuaris autoritzats.
- Canvi o actualització de claus, incloent-hi normes sobre quan s'han de canviar o actualitzar, i quin és el procediment aplicable.
- Gestió de claus compromeses.
- Revocació de claus, incloent-hi la seva retirada o desactivació.
- Arxivament de claus, especialment en cas d'informació xifrada que hagi estat arxivada.
- Destrucció de claus.
- Registre i auditoria d'operacions relatives a la gestió de claus.

S'han de definir períodes d'activació i desactivació de les claus per a reduir el risc de compromís, de manera que les claus només es puguin emprar durant un termini concret, d'acord amb les circumstàncies i l'anàlisi de risc.

S'han de definir procediments per a garantir l'autenticitat de les claus públiques, mitjançant l'ús de les entitats de certificació que siguin adequades.

En cas que hi hagi tercers prestadors de serveis relacionats amb la criptografia, s'han d'establir acords de nivell de servei que considerin de manera específica les qüestions de responsabilitat, la fiabilitat dels serveis i els temps de resposta garantits.

5. Estàndards d'implantació de tecnologia criptogràfica

S'ha de definir i implantar una infraestructura comuna i adequada de tecnologia criptogràfica que presti els serveis criptogràfics identificats en aquesta política a les diferents aplicacions de la UOC, considerant almenys les següents.

- La seu electrònica de la UOC.
- La realització d'actes automatitzats basats en l'ús de segells de la UOC i dels seus òrgans.
- La realització d'actes manuals i altres accions que tinguin plasmació documental, per part del personal de la UOC quan utilitzin signatura electrònica.
- Maquinari criptogràfic dedicat
  - ISO 15408 (2005): «Information technology - Security techniques - Evaluation criteria for IT security», nivell EAL 4 o superior, d'acord amb un objectiu d'avaluació o perfil de protecció adequat a l'anàlisi de risc duta a terme.

    En concret, es consideren adequats els perfils de protecció següents:

    - CEN CWA 14167-2 (2004): «Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP», amb relació a les operacions de signatura de certificats i altres documents, amb còpia de seguretat.
    - CEN CWA 14167-3 (2004): «Cryptographic module for CSP key generation services - Protection profile - CMCKG-PP», amb relació a les operacions de generació de claus.
    - CEN CWA 14167-4 (2003): «Cryptographic module for CSP signing operations - Protection profile - CMCSO PP», amb relació a les operacions de signatura de certificats i altres documents.

  - FIPS 140-2, nivell 3 o superior.

- Targetes i altres dispositius criptogràfics mòbils, i programari criptogràfic
  - FIPS 140-2, nivell 3 o superior.
  - ISO 15408 (2005): «Information technology - Security techniques - Evaluation criteria for IT security», nivell EAL 4 o superior, d'acord amb un objectiu d'avaluació o perfil de protecció adequat a l'anàlisi de risc duta a terme.

    En concret, es consideren adequats els perfils de protecció següents:

    - CEN CWA 14169 (2004): «Secure signature-creation devices “EAL 4+”, amb relació als dispositius de signatura electrònica.
    - CEN CWA 14365-2 (2004): «Guide on the Use of Electronic Signatures - Part 2: Protection Profile for Software Signature Creation Devices», amb relació al programari de signatura electrònica.

En la definició de la infraestructura s'han d'incloure els aspectes següents:

- Identificació detallada d'aplicacions i serveis específics que necessiten serveis criptogràfics.
- Identificació del catàleg de requisits criptogràfics, que ha de garantir el compliment d'aquesta política. S'ha de considerar de manera particular el següent.
    - El volum d'operacions i la topologia de xarxa interna, a l'efecte del càlcul del nombre d'equipaments criptogràfics necessaris.
    - L'anàlisi del xifratge per a la protecció d'informacions sensibles en trànsit o que siguin fora de les instal·lacions de la UOC (transportades mitjançant dispositius mòbils, amb mitjans o dispositius que es poden extreure o per línies de comunicació).
    - L'anàlisi de l'impacte de l'ús de la criptografia sobre els controls basats en la inspecció de continguts, com per exemple els programes antivirus.
- Desenvolupament d'una especificació de gestió de claus, que ha de descriure els components de gestió de claus requerits per a operar els dispositius i les aplicacions criptogràfiques durant el seu cicle de vida. El seu contingut ha de considerar el següent.
    - L'aplicació criptogràfica per als dispositius criptogràfics
    - L'entorn de comunicacions dels dispositius criptogràfics
    - Els requisits dels components de gestió de claus dels dispositius criptogràfics
    - La distribució dels components de gestió de claus dels dispositius criptogràfics
    - El control d'accés als dispositius criptogràfics
    - El registre d'activitats relatives a la gestió de claus dels dispositius criptogràfics
    - La gestió de compromisos i recuperació dels dispositius criptogràfics
    - La recuperació de claus

6. Compliment normatiu

Els serveis criptogràfics s'han d'emprar d'acord amb la legislació vigent en cada moment.

V. Rols i responsabilitats amb relació a la criptografia

El responsable per a la implantació d'aquesta política és l'Àrea de Tecnologia de la UOC.

El responsable per a la gestió de claus, incloent-hi la generació de claus i l'operació de la infraestructura criptogràfica és el responsable de seguretat. Aquest pot delegar en altres unitats internes o externes, fins i tot en empreses, els aspectes de gestió de claus que estiguin justificats.