



Consorci
Administració Oberta
de Catalunya

Digicert token: instal·lació, inicialització, i signatura

Signatura de codi amb Signador



LOCALRET

Índex

1	Objectiu	3
2	Compra i gestió del certificat	4
2.1	Compta de Digicert	4
2.2	Certificat actual	5
3	Token criptogràfic	7
3.1	Instal·lació i inicialització	7
3.2	Passwords	7
4	Signatura de codi	8
4.1	Signar llibreries java (jarsigner)	8
5	Annexes	10
5.1	Signador	10
5.2	Llibreries java (jarsigner)	10
5.3	Instal·lables (install4j v8.0.10)	12

1 Objectiu

El Consorci AOC utilitza un certificat de signatura de codi (*Code Signing Certificate*) per signar les llibreries java del Signador.

A partir de l'1 de juny de 2023 a les 00:00 UTC, els estàndards del sector exigeixen que les claus privades dels certificats de signatura de codi estàndard s'emmagatzemin en maquinari certificat com a FIPS 140 Nivell 2, Common Criteria EAL 4+ o equivalent. Aquest canvi reforça la protecció de la clau privada pels certificats de signatura de codi i l'alineja amb la protecció de la clau privada del certificat de signatura de codi EV (*Extended Validation*).

Fins ara fèiem servir certificat en software (p12 o pfx) per la signatura de codi. A partir d'ara cal fer-ho amb claus allotjades en un dispositiu criptogràfic hardware que aconsegueixi els requeriments anteriors.

El Consorci AOC ha adquirit un certificat de signatura de codi (en endavant CSC de *Code Signing Certificate*) a l'empresa Digicert. L'objectiu d'aquest document és la documentació dels passos que cal seguir per tal d'instal·lar el token criptogràfic, inicialitzar-lo, i un cop fet això, per signar codi amb ell.

Documentació de Digicert:

<https://docs.digicert.com/en/certcentral/manage-certificates/code-signing-certificates.html>

2 Compra i gestió del certificat

2.1 Compta de Digicert

El Consorci AOC disposa d'una compta de Digicert en CERTCENTRAL, que és la web d'administració que permet la gestió tant de les compres com dels certificats un cop emesos.

<http://www.digicert.com>

Usuari: consorciaocat@aoc.cat

Account manager: Marc Kayumba (marc.kayumba@digicert.com)

Dins de "Certificates" > "Orders", podem veure els certificats contractats, inclòs els ja caducats:

Order	Certificate name	Order status	Certificate validity	Order date	Order end date	Product
583052849 Quick View	Consorci Administració Oberta de Catalunya + 3 certificates	Issued	10 Jan 2024 - 25 Jan 2027	11 Dec 2023	25 Jan 2027 3 - year prepaid plan	Code Signing
85453059 Quick View	Consorci Administració Oberta de Catalunya	Renewed	19 Nov 2020 - 26 Jan 2024	10 Nov 2020	26 Jan 2024 3 - year prepaid plan	Code Signing
83586479 Quick View Alternate order # 1543495914	Consorci Administració Oberta de Catalunya	Renewed	12 Dec 2017 - 23 Dec 2020	06 Nov 2020	23 Dec 2020 3 - year prepaid plan	Code Signing

L'últim certificat emès és el primer CSC que hem contractat que segueix la nova normativa, és a dir, en token:

Si cliquem en la ordre, a la pantalla següent ens apareix el certificat que estem fent servir:

Order #583052849 Code Signing, 3 years	
Organization name Consorci Administració Oberta de Catalunya	Order status Issued
Certificate validity 10 Jan 2024 - 25 Jan 2027	Order validity 10 Jan 2024 - 25 Jan 2027 (3 year plan)
Details Certificate and order	Certificate history (4) Resissues and duplicates
Certificate information Additional certificate information	
Organization Consorci Administració Oberta de Catalunya (Organization ID: 1217559) Barcelona, Barcelona, ES +34932722500	Certificate validity 10 Jan 2024 - 25 Jan 2027
Organization units Tecnologia	Serial number 0a9d11c7928310de6b425b8ec73d06
Last renewed 10 Jan 2024 9:26 AM CET	Provisioning method Digicert provided Hardware Token
Certificate status Issued	On this page Certificate information Order details Notifications Order contacts Payment & billing Notes

A la pestanya “Certificate history” podem veure les diferents reemissions sol·licitades sobre el mateix certificat:

Details

Certificate and order

Certificate history (4)

New

Reissues and duplicates

You can only reissue the Primary certificate on the order. To replace expiring duplicate and reissued certificates, use the primary certificate.

Search

Q Search for

Search notes

Q Search for

Certificate status

Unissued

Certificate date

From

To

Go

Show archived certificates

Certificate id	Common name	SANs	Certificate status	Certificate validity	Notes	Certificate actions
> 611871930	Consorci Administració Oberta de Catalunya Primary certificate		Issued	10 Jan 2024 - 25 Jan 2027	-	Reissue
> 611867984	Consorci Administració Oberta de Catalunya Reissue		Rejected	12 Jan 2024 - 25 Jan 2027	-	
> 600176835	Consorci Administració Oberta de Catalunya Reissue		Rejected	12 Jan 2024 - 25 Jan 2027	-	
> 584378611	Consorci Administració Oberta de Catalunya Initial		Issued	27 Dec 2023 - 25 Jan 2027		Download

En aquest cas va succeir lo següent:

- 584378611: Vaig sol·licitar renovació del certificat anterior, el que caducava el 26 de gener de 2024, però al formulari vaig seleccionar “Use existent token”, perquè desconexia els canvis en la normativa. En intentar descarregar-me'l vaig veure que no tenia cap dispositiu, i des de Suport de Digicert em van informar de que necessitava un token.
- 600176835: Donat que no tenim cap HSM amb el que fer plug&play al meu portàtil, vaig sol·licitar la reemissió del certificat, en aquest cas demanant que Digicert ens fes arribar un token. Segons em van dir des de Suport, la diferència entre enviament *standard* i *expedited* era de només 2 dies. Així que vaig seleccionar *standard*.
- 611867984: Després de parlar amb Suport i que ja havien passat més de 10 dies i no ens enviaven el token, per fi vaig poder parlar amb el nostre *account manager*, el Marc Kayumba, i vam fer una nova sol·licitud de reemissió, aquest cop especificant enviament *expedited*.
- 611871930: Aleshores quedaven en la pantalla com 2 enviaments pendents, l'*standard* i el *expedited*. Així que vaig anul·lar un dels dos, i aleshores van desaparèixer els dos enviaments pendents. Per tant, vam haver de sol·licitar una nova reemissió, amb token, i enviament *expedited*.
- Un cop fet això, el token va arribar al dia següent (09/gener/2024).

2.2 Certificat actual

El certificat actual és aquest:

Show archived certificates						
Certificate id	Common name	SANs	Certificate status	Certificate validity	Notes	Certificate actions
611871930	Consorci Administració Oberta de Catalunya		Issued	10 Jan 2024 - 25 Jan 2027	-	<div>Release</div> <div>Archive certificate</div> <div>Revoke certificate</div> <div>Download certificate</div> <div>Hide certificate details</div>
Certificate information						
Common name	-	Certificate validity	2024-01-10 - 2027-01-25	Signature hash	sha256	
SANs	-	Serial number	0a9d11c7928310de6b423bf6cc73d06	Thumbprint	B6F5502F650FCD4AF1B578A1AA489302293ECBC3	
Organization	Consorci Administració Oberta de Catalunya Barcelona, Barcelona, ES +34932722500	CSR	-	Issuing CA	DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1	
Note	Add Note	Certificate id	611871930	Platform	SafeNet eToken S110 CC (RSA-4096 and ECC)	

Des de la pantalla anterior podem gestionar les diferents accions que es poden dur a terme (reemissió, revocació, o descàrrega).

3 Token criptogràfic

3.1 Instal·lació i inicialització

Connectar el token USB a l'ordinador.

Per tal de procedir a la instal·lació, a la pàgina del certificat a instal·lar, clicar al desplegable "Certificate Actions". En el nostre cas el token està buit, i per tant hem de fer "Install Certificate". En la plana que s'obre, trobarem el codi d'inicialització del token, i un parell de links des d'on descarregar l'instal·lador del hardware i els drivers safenet.

A partir d'aquí, seguir aquestes instruccions:



Set_Up_Your_DigiCert
_Provided_eToken.pdf

Font: <https://knowledge.digicert.com/solution/set-up-your-digicert-provided-etoken>

3.2 Passwords

El SafeNet eToken utilitza diverses contrasenyes per a l'autenticació. Si una contrasenya d'administrador s'introdueix incorrectament cinc vegades, l'eToken es bloquejarà permanentment.

El SafeNet eToken utilitza els passwords següents:

- Password d'administrador:
El password d'administrador predeterminat és "0" 48 vegades, tal com la proporciona el fabricant. Si es perd "aquest" password, l'eToken es bloquejarà permanentment i caldrà comprar-ne un de nou. DigiCert no configura aquest password.
- Password del token:
Aquest password s'utilitza per accedir al magatzem de certificats de l'eToken. Si es perd, podeu resetejar l'eToken i tornar a instal·lar el certificat.
- Clau de desbloqueig personal (PUK o *Personal Unlocking Key*): el PUK predeterminat és 000000.
DigiCert no utilitza el PUK en el nostre procés.

4 Signatura de codi

Un cop instal·lades les claus al token, ja podem signar. El password que haurem de fer servir és el del token, cada cop que ens ho demani.

4.1 Signar llibreries java (jarsigner)

Instruccions:



SIGN_JAVA
_JAR_FILES_WITH_HAR

Font: <https://knowledge.digicert.com/tutorials/sign-java-jar-files-with-a-hardware-token-based-code-signing-certificate-in-windows>

Bàsicament, lo que hem de fer és:

Anar a la nostra JDK, per exemple:
C:\Program Files\Java\jdk1.8.0_281\bin

I crear un arxiu de nom eToken.cfg, amb aquest contingut:

```
name=eToken  
library=c:\WINDOWS\system32\TPKCS11.dll
```

Comandes:

- Primer anem a la carpeta bin de la JDK:

cd C:\Program Files\Java\jdk1.8.0_281\bin

- Amb la següent comanda podem veure els certificats del token:

**keytool -list -keystore NONE -storetype PKCS11 -providerclass
sun.security.pkcs11.SunPKCS11 -providerArg .eToken.cfg**

```
Introduzca la contraseña del almacén de claves:  
Tipo de Almacén de Claves: PKCS11  
Proveedor de Almacén de Claves: SunPKCS11-eToken
```

```
Su almacén de claves contiene 1 entrada
```

```
Consorci Administració Oberta de Catalunya, PrivateKeyEntry,  
Huella de certificado (SHA-256):  
0E:CD:51:6A:48:CB:E4:1F:FE:B7:18:C0:9E:83:6F:61:80:F4:A3:0E:9F:AB:3C:AD:B4:C2:4F:8  
A:12:99:65:E5
```

L'àlies del certificat és:

Consorci Administració Oberta de Catalunya

Quan haguem de fer referència a ell, cal tenir escriure'l tal qual, amb el símbol "estrany".

- Per signar doncs un jar amb el token, afegint segell de temps (en aquest cas timestamp de DigiCert):

```
jarsigner -tsa http://timestamp.digicert.com -verbose -keystore NONE -storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg ./eToken.cfg "C:\path\to\file.jar" "Consorti Administració Oberta de Catalunya"
```

- I per comprovar les signatures (signatura i segell d'un jar, per exemple:

```
jarsigner -verify -verbose -certs "C:\E\SIGNADOR\area_treball\2024\appletCATCert.jar"
```

```
[.....]  
- Signed by "CN=Consorti Administració Oberta de Catalunya, OU=Tecnologia, O=Consorti Administració Oberta de Catalunya, L=Barcelona, ST=Barcelona, C=ES"  
  Digest algorithm: SHA-256  
  Signature algorithm: SHA256withRSA, 4096-bit key  
  Timestamped by "CN=DigiCert Timestamp 2023, O="DigiCert, Inc.", C=US" on mié ene 10 08:54:07 UTC 2024  
  Timestamp digest algorithm: SHA-256  
  Timestamp signature algorithm: SHA256withRSA, 4096-bit key
```

Podem veure que té la signatura del Consorci, i un segell de temps de DigiCert.

5 Annexes

5.1 Signador

5.2 Llibreries java (jarsigner)

Signatura dels jars del Signador:

=> Anem a la JVM on hem configurat el token (eToken.cfg):

```
cd C:\Program Files\Java\jdk1.8.0_281\bin
```

=> Comprovació certificats en token:

```
keytool -list -keystore NONE -storetype PKCS11 -providerclass  
sun.security.pkcs11.SunPKCS11 -providerArg ./eToken.cfg
```

=> Signatura (amb timestamp inclós) dels jars:

```
jarsigner -tsa http://timestamp.digicert.com -verbose -keystore NONE -storetype PKCS11 -  
providerClass sun.security.pkcs11.SunPKCS11 -providerArg ./eToken.cfg  
"C:\E\SIGNADOR\area_treball\2024\appletCATCert.jar" "Consorci Administraci3 Oberta de  
Catalunya"
```

```
jarsigner -tsa http://timestamp.digicert.com -verbose -keystore NONE -storetype PKCS11 -  
providerClass sun.security.pkcs11.SunPKCS11 -providerArg ./eToken.cfg  
"C:\E\SIGNADOR\area_treball\2024\apsa-light.jar" "Consorci Administraci3 Oberta de Catalunya"
```

```
jarsigner -tsa http://timestamp.digicert.com -verbose -keystore NONE -storetype PKCS11 -  
providerClass sun.security.pkcs11.SunPKCS11 -providerArg ./eToken.cfg  
"C:\E\SIGNADOR\area_treball\2024\CATCertCMSlib.jar" "Consorci Administraci3 Oberta de  
Catalunya"
```

```
jarsigner -tsa http://timestamp.digicert.com -verbose -keystore NONE -storetype PKCS11 -  
providerClass sun.security.pkcs11.SunPKCS11 -providerArg ./eToken.cfg  
"C:\E\SIGNADOR\area_treball\2024\CATCertPDFlib.jar" "Consorci Administraci3 Oberta de  
Catalunya"
```

```
jarsigner -tsa http://timestamp.digicert.com -verbose -keystore NONE -storetype PKCS11 -  
providerClass sun.security.pkcs11.SunPKCS11 -providerArg ./eToken.cfg  
"C:\E\SIGNADOR\area_treball\2024\librariesLinux_Firefox.jar" "Consorci Administraci3 Oberta de  
Catalunya"
```

```
jarsigner -tsa http://timestamp.digicert.com -verbose -keystore NONE -storetype PKCS11 -  
providerClass sun.security.pkcs11.SunPKCS11 -providerArg ./eToken.cfg  
"C:\E\SIGNADOR\area_treball\2024\librariesLinux_Firefox_v60.jar" "Consorci Administraci3  
Oberta de Catalunya"
```

```
jarsigner -tsa http://timestamp.digicert.com -verbose -keystore NONE -storetype PKCS11 -  
providerClass sun.security.pkcs11.SunPKCS11 -providerArg ./eToken.cfg  
"C:\E\SIGNADOR\area_treball\2024\librariesMacOS_Firefox.jar" "Consorci Administraci3 Oberta  
de Catalunya"
```

```
jarsigner -tsa http://timestamp.digicert.com -verbose -keystore NONE -storetype PKCS11 -  
providerClass sun.security.pkcs11.SunPKCS11 -providerArg ./eToken.cfg  
"C:\E\SIGNADOR\area_treball\2024\librariesMacOS_Firefox_v60.jar" "Consorci Administraci3  
Oberta de Catalunya"
```

```
jarsigner -tsa http://timestamp.digicert.com -verbose -keystore NONE -storetype PKCS11 -  
providerClass sun.security.pkcs11.SunPKCS11 -providerArg ./eToken.cfg  
"C:\E\SIGNADOR\area_treball\2024\librariesWin_Firefox.jar" "Consorci Administraci3 Oberta de  
Catalunya"
```

```
jarsigner -tsa http://timestamp.digicert.com -verbose -keystore NONE -storetype PKCS11 -  
providerClass sun.security.pkcs11.SunPKCS11 -providerArg ./eToken.cfg  
"C:\E\SIGNADOR\area_treball\2024\librariesWin_Firefox_v60.jar" "Consorci Administraci3 Oberta  
de Catalunya"
```

=> Comprovació de la signatura i el timestamp de tots els jars:

```
jarsigner -verify -verbose -certs "C:\E\SIGNADOR\area_treball\2024\appletCATCert.jar"  
jarsigner -verify -verbose -certs "C:\E\SIGNADOR\area_treball\2024\apsa-light.jar"  
jarsigner -verify -verbose -certs "C:\E\SIGNADOR\area_treball\2024\CATCertCMSlib.jar"  
jarsigner -verify -verbose -certs "C:\E\SIGNADOR\area_treball\2024\CATCertPDFlib.jar"  
jarsigner -verify -verbose -certs "C:\E\SIGNADOR\area_treball\2024\CATCertXMLlib.jar"  
jarsigner -verify -verbose -certs "C:\E\SIGNADOR\area_treball\2024\librariesLinux_Firefox.jar"  
jarsigner -verify -verbose -certs "C:\E\SIGNADOR\area_treball\2024\librariesLinux_Firefox_v60.jar"  
jarsigner -verify -verbose -certs "C:\E\SIGNADOR\area_treball\2024\librariesMacOS_Firefox.jar"  
jarsigner -verify -verbose -certs "C:\E\SIGNADOR\area_treball\2024\librariesMacOS_Firefox_v60.jar"  
jarsigner -verify -verbose -certs "C:\E\SIGNADOR\area_treball\2024\librariesWin_Firefox.jar"  
jarsigner -verify -verbose -certs "C:\E\SIGNADOR\area_treball\2024\librariesWin_Firefox_v60.jar"
```

5.3 Instal·lables (install4j v8.0.10)

A install4j cal configurar el token per la signatura dels instal·lables de Windows.

La llibreria PKCS#11 és:

c:\WINDOWS\system32\TPKCS11.dll

Un cop el programa detecta el token, un cop inicialitzat (ens demanarà el password), podem seleccionar al desplegable, el certificat amb què volem signar. En el nostre cas només hi ha un certificat.

