Consorci
Administració Oberta
de Catalunya

Manual d'usuari Signasuite

Generalitat
de Catalunya

LOCALRET

Índex

1 Què és? 1

2 Quí pot fer servir Signasuite? 1

3 Com s'hi pot accedir? 1

4 Pantalla incial 1

5 Validació 2

5.1 Certificats 2

5.1.1 Resultat 2

5.2 Signatura 3

5.2.1 Resultats 4

5.3 Documents PDF 5

5.4 Seu electrònica 5

5.4.1 Resultat 6

6 Signatura 6

7 Preservació 9

1 Què és?

El SignaSuite és una aplicació web que permet als seus usuaris portar a terme qualsevol de les operacions relacionades amb la creació, validació i preservació de signatures electròniques basades en certificats digitals. És el frontal web del Servei Validador que el Consorci AOC ofereix al conjunt de les Administracions Públiques Catalanes.

2 Qui pot fer servir Signasuite?

El portal de Signasuite és públic i accessible per tothom.

3 Com s'hi pot accedir?

Signasuite està accessible des de la següent adreça:

http://signasuite.aoc.cat

Un enllaç a Signasuite es troba disponible de de el menú d'Aplicacions de EACAT.

4 Pantalla inicial

La pantalla inicial de l'aplicació, que es mostra a la Figura 1, és força intuïtiva i mostra directament totes les funcionalitats que ofereix.

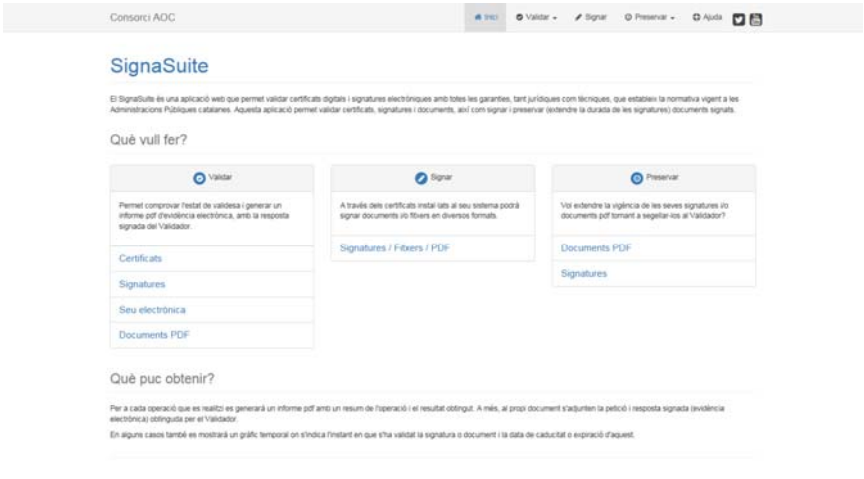

Figura 1. Pantalla principal de Signasuite

Les funcionalitats estan dividides en tres grups:

- Validar: Per validar tant document signats com certificats digitals
- Signar: Per produir signatures electròniques basades en certificats digitals

- Preservar: Per completar les signatures electròniques en format avançat amb informació que permeti allargar el seu període de vigència.

Com es pot observar, a la part superior es mostra un menú que permetrà accedir a totes aquestes funcions des de qualsevol de les pantalles del sistema.

5 Validació

Signasuite permet validar tant certificats com documents signats electrònicament. En concret, les opcions que es mostren són:

- Certificats
- Signatures
- Documents PDF
- Seu Electrònica

Per accedir a cadascuna de les opcions només cal seleccionar-la.

5.1 Certificats

Es permet la validació de certificats introduint la part pública del certificat en un fitxer amb extensió .cer codificat en base64. Aquest tipus de fitxer pot ser exportat des del magatzem de certificats de sistemes operatius i navegadors. No es permet la pujada de fitxers de certificats amb clau privada amb extensions .p12 i pfx.

El certificat enviat es valida emprant el Servei Validador del Consorci AOC, i que té en compte els perfils de certificats hi té classificats. El document de classificació del Consorci AOC es pot consultar a la següent adreça:

https://www.aoc.cat/serveis-aoc/validador/#1450087630072-d2a9bd43-debe

Val a dir que, per tal d'assegurar l'acceptació de tots els perfils qualificats, el Servei Validador envia a la plataforma de validació de l'estat @firma els certificats de perfils que no té classificats. Els prestadors i perfils acceptats per aquesta plataforma poden ser consultats al següent enllaç:

https://administracionelectronica.gob.es/ctt/afirma/descargas

5.1.1 Resultat

Com a resultat d'una operació de validació d'un certificat, Signasuite informa de:

- Resultat de l'operació. Pot ser vàlid, invàlid, caducat, revocat o error
- Si és vàlid, es dona informació sobre el certificat:
  - Urn del tiquet del Servei de Validació amb el resultat de l'operació.
  - Data en que s'ha produït l'operació de validació.
  - Data de caducitat del certificat.
  - Una taula amb els principals atributs del certificat validat
- També s'ofereix a l'usuari la possibilitat de descarregar un informe en pdf amb el resultat de l'operació.
- Com a ajuda a desenvolupadors que consultin Signasuite per comparar el seu funcionament amb el d'aplicacions de tercers, el sistema presenta tant la petició com la resposta en format xml que s'ha enviat i rebut del Servei Validador. Les peticions i respostes del Servei Validador

s'ajusten al format Digital Signature Services (DSS) de OASIS, i la seva sintaxi pot ser consultada al web:

https://www.oasis-open.org/committees/dss/

- En cas d'error es dona una descripció de l'error detectat

5.2 Signatura

Signasuite permet validar tant documents signats electrònicament com signatures separades del seu document (detached). El format acceptats concretament són:

La signatura està en XML:

- XML/XAdES Detached > si la signatura està separada en un altre fitxer (cal adjuntar 2 fitxers)
- XML/XAdES Enveloping > si la signatura embolcalla (inclou) al document, que també estarà en xml
- XML/XAdES Enveloped > si el document, també en xml, embolcalla (inclou) la signatura.

Si la signatura és binària en format PKCS#7, el format de document sempre es pren com a binari, i els formats podran ser:

- CMS/CAdES Detached > si la signatura està separada en un altre fitxer (cal adjuntar 2 fitxers).
- CMS/CAdES Attached > si la signatura inclou al document.

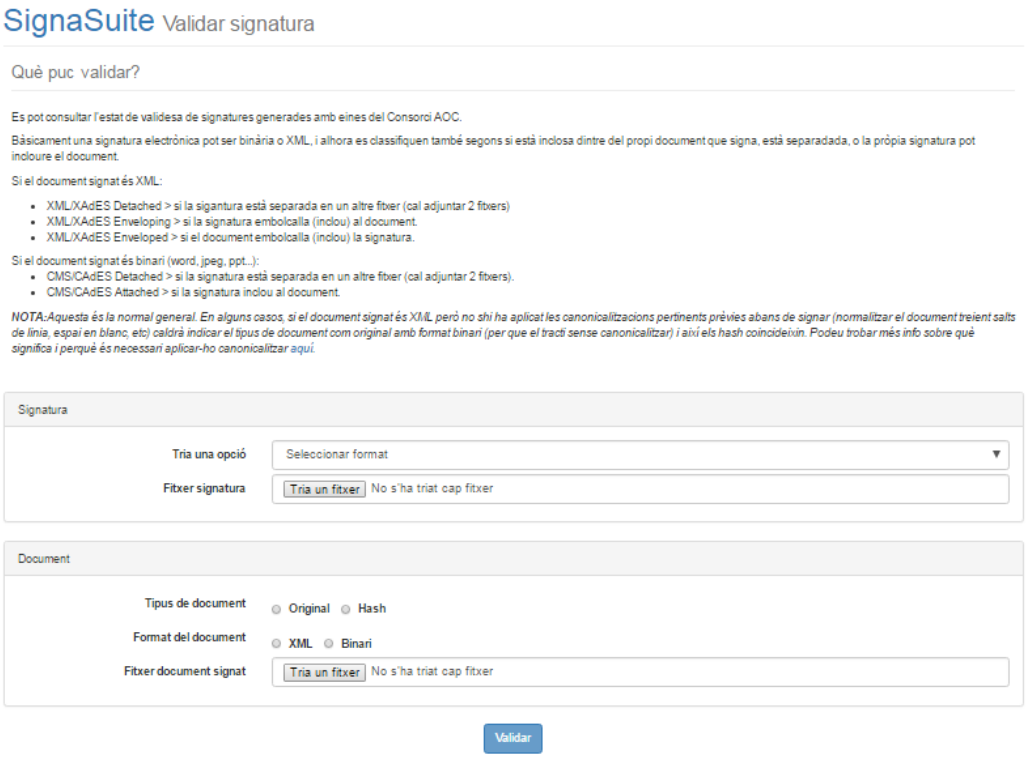

Figura 2. Pantalla de validació de signatures

Tant si els formats de signatura són XML/XAdes Enveloped, Enveloping o bé CMS/CAdES Attached, document i signatura estaran en el mateix fitxer, i només serà necessari escollir el fitxer de la caixa "Signatura". En els casos de formats "detached", es podrà escollir si pujar el document corresponent a la signatura o bé un fitxer de text que contingui el resum criptogràfic del document en base64. En cas de voler pujar el document signat, caldrà especificar si el fitxer signat és un binari o bé un xml.

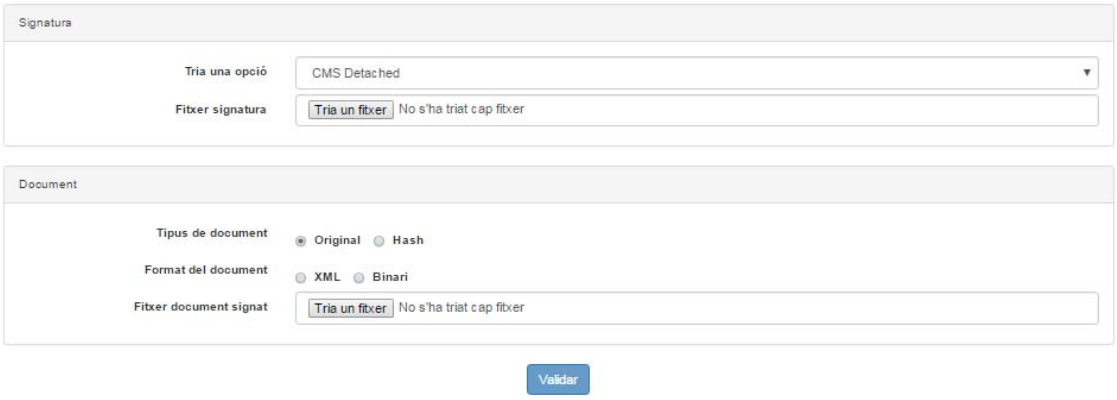

Figura 3. Detall de la pantalla per validar una signatura CMS Detached

És important especificar bé quin va ser el format de signatura que es va produir, especialment si estem tractant signatures detached, sobretot pel que fa al format del document. El resultat de la validació pot ser negatiu, si s'especifica un format incorrecte (per exemple dient que el format del document signat és un xml quan es va signar com a binari. Per altra banda, e*n alguns casos, si el document signat és XML però no s'han aplicat les canonicalitzacions pertinents prèvies abans de signar (normalitzar el document traient salts de línia, espai en blanc, etc) caldrà indicar el tipus de document com original amb format binari (per que el tracti sense canonicalitzar) per tal que els hash coincideixin*[1].

5.2.1 Resultats

Com a resultat, de manera similar al que s'obté en validar un certificat digital, Signasuite informa de:

- Resultat de l'operació.
- Si totes les signatures del document són vàlides
- vàlida, es dona informació sobre les signatures:
  - Urn del tiquet del Servei de Validació amb el resultat de l'operació.
  - Data en que s'ha produït l'operació de validació.
  - Data de caducitat del document signat electrònicament.
  - Format de les signatures
  - Una taula amb els principals atributs del certificats validats
- També s'ofereix a l'usuari la possibilitat de descarregar un informe en pdf amb el resultat de l'operació.
- Petició i resposta en format xml al Servei Validador.

[1] L'especificació del procés de canonicalització es pot consultar a: http://webservices.xml.com/pub/a/ws/2002/09/18/c14n.html

- Un gràfic temporal que mostra l'interval de validesa del c
- En cas d'error es dona una descripció de l'error detectat

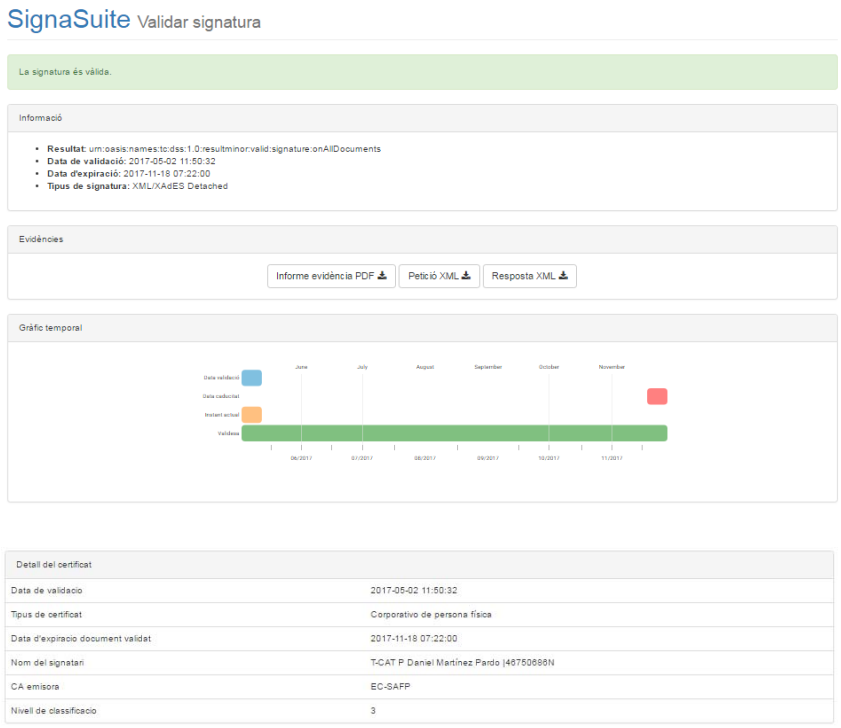

Figura 4. Resultat validació signatura electrònica

5.3 Documents PDF

De manera similar a la validació de la resta de signatures, els documents pdf també es poden enviar a validar amb uns resultats molt similars als ja descrits al punt 5.2. En aquest cas, només caldrà pujar el document signat, que no podrà tenir una grandària superior als 10MB.

5.4 Seu electrònica

Signasuite també ofereix un servei de validació de Seus Electròniques. Introduint l'adreça URL d'una seu, el sistema obté el certificat que garanteix la seva identitat i el valida fent servir el Servei Validador.

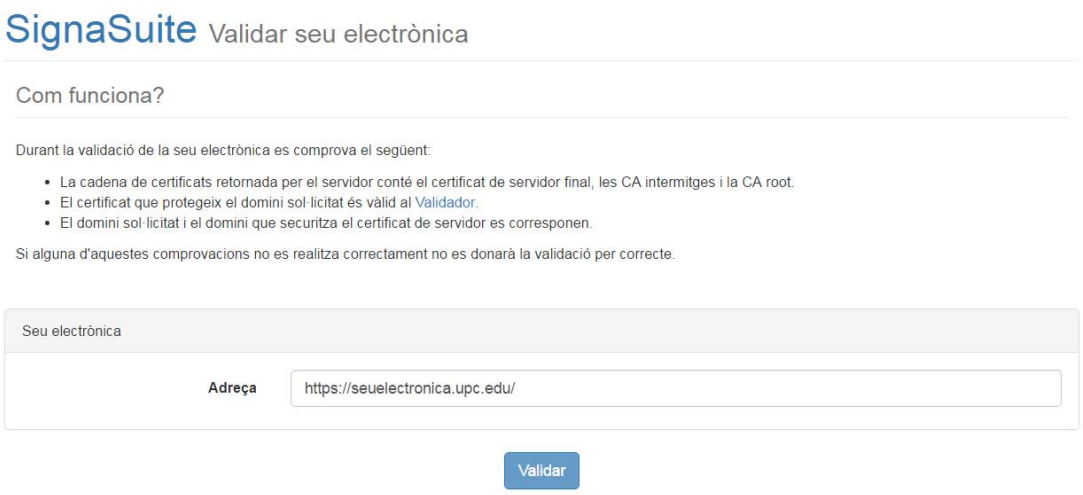

Figura 5. Pantalla de validació d'una Seu electrònica

5.4.1 Resultat

Si el resultat de la validació és correcte, Signasuite informa de la URL de la seu així com de la data d'exiració del certificat que la securitza.

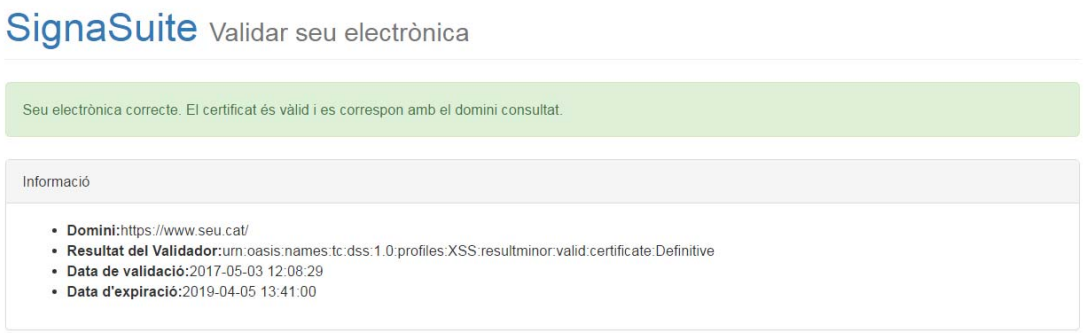

Figura 6. Pantalla de resultats de validació d'una Seu electrònica

6 Signatura

El sistema també ofereix una sistema per signar documents. Seleccionat l'opció "Signar", es mostra un formulari que, per defecte, serveix per signar documents pdf. Tal i com es mostra a la Figura 7, el formulari demana quin és l'arxiu a signar i la localtzació física de la signatura, que es posarà a la darrera pàgina del document. S'ofereix la opció de signar els documents d'una carpeta.

Tant en el cas de pujar un document, com si es vol pujar tot el contingut d'una carpeta, la mida del total no pot ser superior als 7MB.

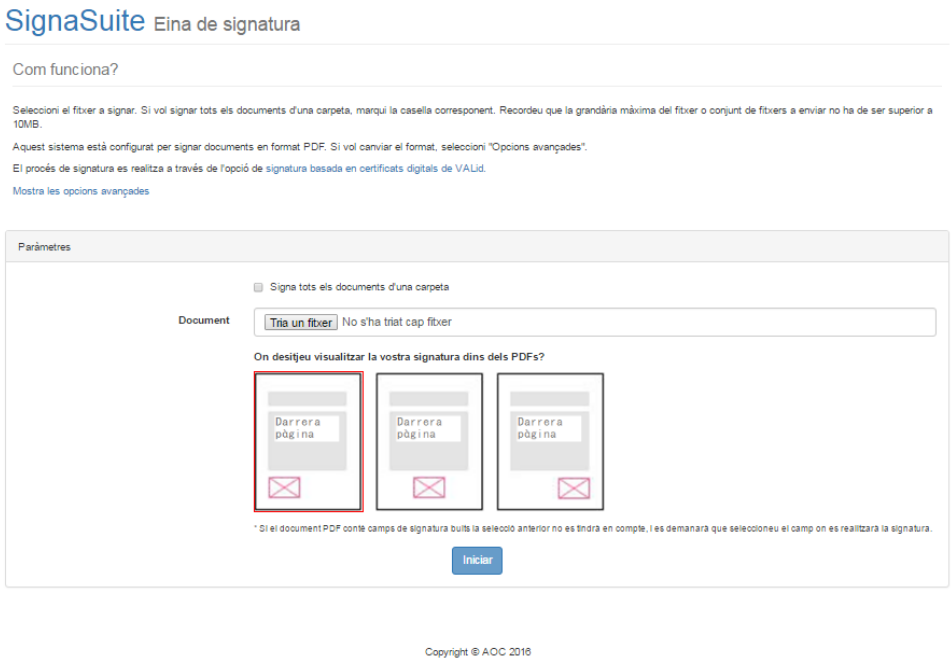

Figura 7. Pantalla Signatura de documents

En opcions avançades, es pot canviar el format de la signatura, que només podrà ser 'detached', ja sigui XAdES o CAdES. En ambdós casos, no es demanarà que es localitzi visualment la signatura, ja que aquesta no serà visualitzable.

6.1 Eina de signatura

Per tal de produir les signatures, el Signasuite fa servir les funcionalitats de signatura electrònica basada en certificats digitals de VALid. És un servei centralitzat que ofereix una alternativa als applets de java per la signatura de documents en entorns web. Podeu trobar més informació sobre el servei a:

https://signador.aoc.cat

Un cop seleccionat el document, o documents, a signar, Signasuite farà una petició a aquesta funcionalitat de VALid i redireccionarà a l'usuari per tal que porti a terme la signatura electrònica, oferint aquelles eines necessàries per fer-ho que estiguin disponibles.

6.2 Signatura sense aplicació de signatura instal·lada

Si l'usuari no té instal·lat cap programari especial per fer-ho, el sistema demanarà que l'usuari es descarregui un fitxer Java Web Start (jnlp) que executarà l'aplicació de signatura, tot mostrant unes instruccions detallades sobre les passes a portar a terme. En aquest cas, l'usuari necessitarà tenir una màquina virtual java i el seu certificat degudament instal·lats. L'usuari haurà de seguir les instruccions per pantalla amb cura.

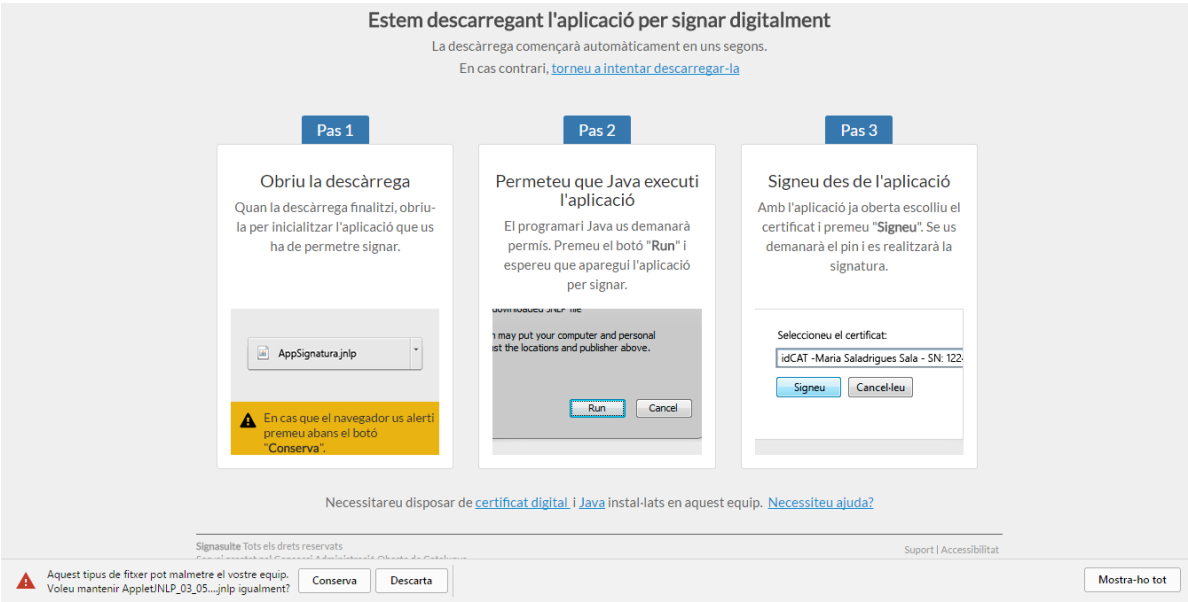

Figura 8. Instruccions per signar sense cap aplicació instal·lada.

Tal i com es veu a la Figura 8, les instruccions indiquen que s'ha generat un fitxer jnlp, que s'ha de descarregar i executar. Aquest fitxer és l'aplicació que portarà a terme la signatura del document. Són fitxers únics i diferents per cada operació de signatura.

Figura 9. Eina Web de signatura executada pel fitxer jnlp.

Executant el fitxer, es mostrarà una pantalla on l'usuari podrà escollir el certificat a emprar. Quan ho faci, l'usuari Signasuite mostrarà una pantalla que permetrà la descàrrega del document signat.

6.3 Signatura amb aplicació nativa

Per evitar que els usuaris s'hagin de descarregar un fitxer jnlp cada cop que vulguin executar un procés de signatura electrònica, des del Consorci AOC s'ha preparat una aplicació nativa instal·lable, i disponible per als sistemes operatius Microsoft Windows, Linux i Mac que substitueix la seva necessitat. Si un usuari té aquesta aplicació nativa instal·lada, el que farà el signador web de VALid en comptes d'oferir descarregar el fitxer jnlp serà mostrar, directament, la seva llista de certificats per produir la signatura.

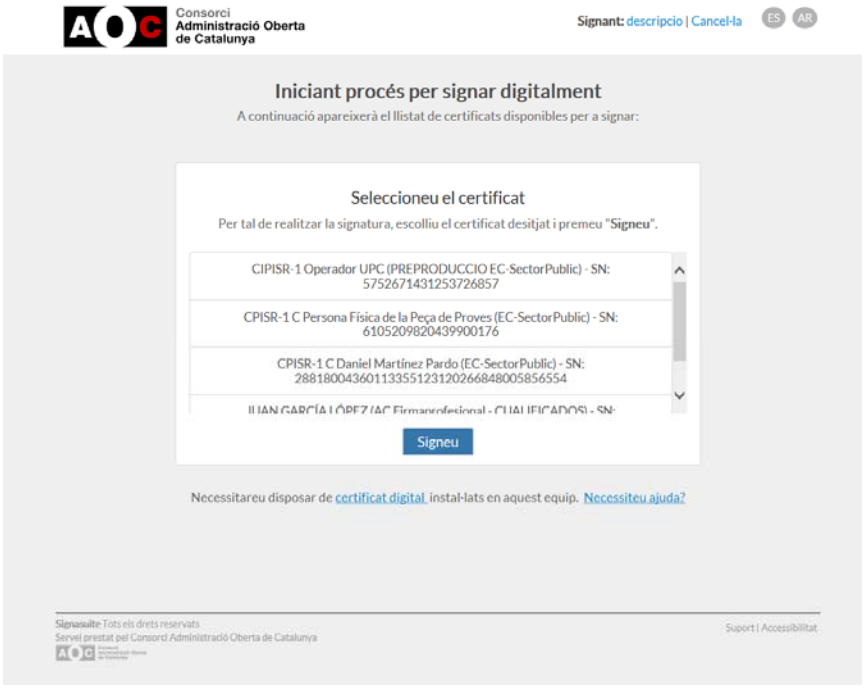

Figura 10. Pantalla de selecció de certificat per usuaris de l'aplicació nativa

El resultat de l'operació serà el mateix.

7 Preservació

Quan el format de signatura és avançat (XAdES, CAdES, PAdES), el Servei Validador del Consorci AOC ofereix la possibilitat d'ampliar la data de caducitat de les signatures electròniques incloent-hi un nou segell de temps. Val a dir que una signatura vàlida que inclou un segell de temps es podrà considerar vàlida fins que aquest segell caduqui. Per tant, el mecanisme de preservació de signatures electròniques consisteix en anar afegint-hi segells de temps progressivament. El Consorci AOC renova el certificat del Servei de Segell de temps anualment, de manera que la seva durada mínima serà de tres anys. Així, un mecanisme de preservació típic generalment consistirà en validar la signatura una vegada cada tres anys, demanat el seu completat.

Generalment aquestes operacions es porten a terme de forma automàtica fent servir els Serveis Web del Servei Validador, tot i que Signasuite permet executar aquestes operacions, escollint l'opció Preservar, que està disponible tant per fitxers pdf com per la resta de formats de signatura, de manera molt similar al que descriu el punt 5 d'aquest document pel que fa a la validació.

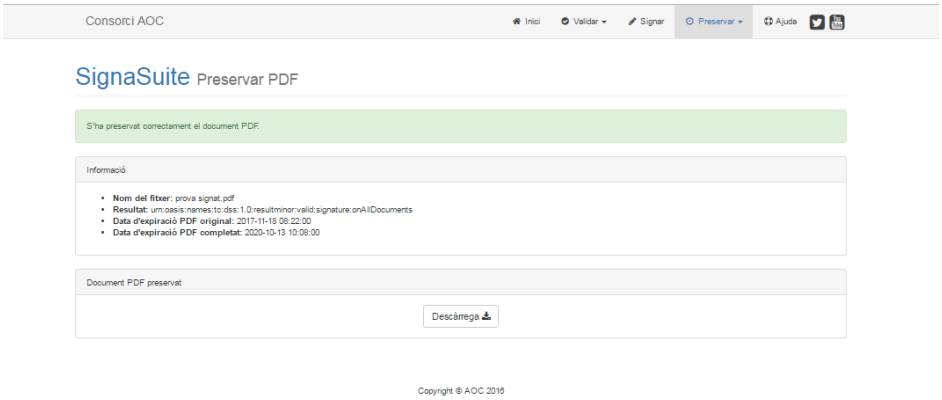

Figura 11. Resultat de la preservació d'un document pdf

La Figura 11 mostra el resultat de la Preservació d'un document pdf. Com es pot veure, el sistema informa de la d'ata d'expiració de la signatura original així com del document completat, i dona l'opció de descarregar el document amb la signatura completada. Aquesta nova versió del document serà la que caldrà guardar. En l'exemple mostrat, l'any 2020 caldrà tornar a executar aquesta funcionalitat si es vol continuar preservant la validesa de la signatura.