



## **Agència Catalana de Certificació**

PSIS: Web de validació

Referència: PSIS-WEB\_VALIDACIÓ  
Versió: 1.0  
Data: 06/02/2009

---

---

## Informació general

---

### Control documental

**Projecte:**

**Entitat de destinació:**

**Títol:** PSIS: Web de validació

**Codi de referència:**

**Versió:**

**Data:**

**Fitxer:** PSISWebValidacio.doc

**Eina/es d'edició:** Word 2002

**Autor/s:**

**Resum:**

### Drets d'ús

---

La present documentació és propietat de l'AGÈNCIA CATALANA DE CERTIFICACIÓ, és confidencial i no podrà ésser objecte de reproducció total o parcial, tractament informàtic ni transmissió de cap forma o per qualsevol mitjà, ja sigui electrònic, mecànic, per fotocòpia, registre o qualsevol altre. Tanmateix, tampoc no podrà ésser objecte de préstec, lloguer o qualsevol forma de cessió d'ús sense el consentiment previ i per escrit de l'AGÈNCIA CATALANA DE CERTIFICACIÓ, titular del dret d'autor (copyright). L'incompliment de les limitacions assenyalades per qualsevol persona que tingui accés a la documentació serà perseguida d'acord amb la llei.

---

### Estat formal

<b>Preparat per:</b>	<b>Revisat per:</b>	<b>Aprovat per:</b>
Nom: Àurea Alcaide Data: 06/02/2009	Nom: Data:	Nom: Data:

## Control de versions

Versió	Parts que canvien	Descripció del canvi	Data
1.0	Creació del document		06/02/2008

---

## Índex

---

<b>Informació general</b> .....	<b>2</b>
<b>Control documental</b> .....	<b>2</b>
<b>Drets d'ús</b> .....	<b>2</b>
<b>Estat formal</b> .....	<b>2</b>
<b>Control de versions</b> .....	<b>3</b>
<b>Índex</b> .....	<b>4</b>
<b>1. Introducció</b> .....	<b>5</b>
<b>1.0 Objecte i abast</b> .....	<b>5</b>
<b>1.1 URL d'accés</b> .....	<b>5</b>
<b>1.2 Glossari</b> .....	<b>5</b>
<b>2. Funcionalitats</b> .....	<b>6</b>
<b>2.0 Plana d'entrada</b> .....	<b>6</b>
<b>2.1 Validació de certificats</b> .....	<b>6</b>
<b>2.2 Validació de signatures</b> .....	<b>9</b>
2.2.0 Plana d'entrada a la validació de signatures.....	10
2.2.1 Validació de signatures XMLDSig/XAdES .....	11
2.2.1.0 Plana d'entrada a la validació de signatures XML .....	11
2.2.1.1 Signatura envoltada (enveloped) .....	11
2.2.1.2 Signatura envoltant (enveloping) .....	11
2.2.1.3 Signatura separada (detached) .....	12
2.2.2 Validació de signatures CMS/CADES.....	12
2.2.2.0 Plana d'entrada a la validació de signatures CMS/CADES .....	12
2.2.2.1 Signatura inclou les dades signades (attached).....	12
2.2.2.2 Signatura separada (detached) .....	13
2.2.2.3 Plana de resultats.....	13
<b>2.3 Validació de documents PDF signats</b> .....	<b>14</b>

---

## 1. Introducció

---

### 1.0 Objecte i abast

L'objecte del present document és descriure les funcionalitats de la web de validació contra la plataforma PSIS que CATCert posa a disposició dels seus clients.

La web de validació permet validar certificats i signatures simples i avançades mitjançant PSIS. Es descriu la manera de portar a terme aquestes operacions a través de la web, en funció de la tipologia de l'objecte a validar.

### 1.1 URL d'accés

La URL d'accés a la web de validació és:

<http://testvalidacio.catcert.cat/psiswebclient/>

### 1.2 Glossari

<PSIS>	Plataforma de Serveis d'Identificació i Signatura
<CMS>	Cryptographic Message Syntax
<CAAdES>	CMS Advanced Electronic Signatures
<XML>	Extensible Markup Language
<XMLDSig>	XML Signature Syntax and Processing
<XAdES>	XML Advanced Electronic Signatures
<IETF>	Internet Engineering Task Force
<W3C>	World Wide Web Consortium
<XPath>	XML Path Language

## 2. Funcionalitats

### 2.0 Pàgina d'entrada

La pàgina d'entrada a la web ens presenta les opcions per a validar certificats o signatures:



Assistència telefònica: 902 901 080

**CATCert** Agència Catalana de Certificació

### PSIS - PLATAFORMA DE SERVEIS D'IDENTIFICACIÓ I SIGNATURA

Quina operació vol realitzar?

- ▶ [Validació de certificats](#)
- ▶ [Validació de signatures](#)

**CATCert** Agència Catalana de Certificació

**AOC** Consorci Administració Oberta de Catalunya

Generalitat de Catalunya  
Consorci de governs locals per a la societat de la informació

Clicar l'enllaç corresponent a la operació que es desitgi realitzar.

### 2.1 Validació de certificats

Si entrem en la opció de validació de certificats, se'ns mostra la pantalla següent:

Assistència telefònica: 902 901 080

 Agència Catalana de Certificació

## PSIS - PLATAFORMA DE SERVEIS D'IDENTIFICACIÓ I SIGNATURA

---

**Validació de certificats:**

Seleccioni el certificat a validar:

NOM	EMISSOR	DATA DE CADUCITAT	ASSUMPTE	
PROVA PROVA PROVA	EC-IDCat	05/02/2012	CN=PROVA PROVA PROVA, ...	▲
Sonda de monitorització de s...	EC-SAFP	05/02/2010	SERIALNUMBER=MONIT-001...	☰
CEIXSA-1 Consorci Administr...	EC-SAFP	05/02/2012	OID.1.3.6.1.4.1.18838.1.1=77...	
CPISR-1 Usuaría Provesa De...	PREPRODUCCIO EC-SAFP	05/02/2011	SERIALNUMBER=12345678...	▼

Si desitja validar un certificat no inclòs a la llista anterior:

Un applet Java mostra els certificats carregats al magatzem de Windows.

Podem seleccionar un dels certificats que ens mostra l'applet, o bé indicar quin certificat volem validar, pujant el fitxer del certificat. El format del fitxer del certificat pot ser binari, Base64, o PEM.

Pantalla de resultats:

Ens mostra el resultat de la validació, el temps de resposta de PSIS, i una llista d'atributs del certificat validat. Aquests atributs s'obtenen mitjançant PSIS, a partir de la mateixa crida de validació.

Assistència telefònica: 902 901 080

## PSIS - PLATAFORMA DE SERVEIS D'IDENTIFICACIÓ I SIGNATURA

### Validació de certificats:

El certificat és VÀLID.

Temps de resposta de PSIS: 2.846 seg

Camps del certificat:

Camp	Valor
Polítiques de certificat	1.3.6.1.4.1.15096.1.3.1.91
Subjecte: Número de sèrie	MONIT-001
Emisor	CN=EC-SAFP,OU=Secretaria d'Administració i Funció Pública,OU=Vegeu https://www.catcert.net/verCIC-2 (c)03,OU=Serveis Públics de Certificació ECV-2,L=Passatge de la Concepció 11 08008 Barcelona,O=Agència Catalana de Certificació (NIF Q-0801176-I),C=ES
Vàlid fins a	2010-03-14T09:21:12.000Z
Subjecte: Algorisme de clau pública	RSA
Classificació	3
Vàlid des de	2006-03-14T09:21:17.000Z
Emisor: Nom	EC-SAFP
Subjecte: Nom	Sonda de monitorització de serveis de CATCert
Usos de la clau	digitalSignature,keyEncipherment
Departament	Àrea Tècnica
Subjecte: e-mail	sonda@catcert.net
Subjecte: Nom comú	Sonda de monitorització de serveis de CATCert
Versió	3
Subjecte: Organització	Agència Catalana de Certificació
Número de sèrie	24696375601767374882871793137824230633
Subjecte: País	ES
Algorisme de la signatura	1.2.840.113549.1.1.5

[Veure petició i resposta XML](#)

Per veure la petició enviada a PSIS per a la validació del certificat, així com la resposta de PSIS, clicar el botó "Veure petició i resposta XML":

## PSIS - PLATAFORMA DE SERVEIS D'IDENTIFICACIÓ I SIGNATURA

### Validació de certificats:

Petició enviada i resposta del servidor:

#### Petició:

```
<VerifyRequest Profile="urn:oasis:names:tc:dss:1.0:profiles:XSS"
xmlns="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:urn="urn:oasis:names:tc:dss:1.0:profiles:XSS"
xmlns:xd="http://www.w3.org/2000/09/xmlsig#">
  <OptionalInputs>
    <urn:ReturnX509CertificateInfo>
      <urn:AttributeDesignator
Name="urn:oasis:names:tc:dss:1.0:profiles:XSS:certificateAttributes:Version"/>
      <urn:AttributeDesignator
Name="urn:oasis:names:tc:dss:1.0:profiles:XSS:certificateAttributes:SerialNumber"/>
      <urn:AttributeDesignator
Name="urn:oasis:names:tc:dss:1.0:profiles:XSS:certificateAttributes:SignatureAlgorithm"
/>
      <urn:AttributeDesignator
Name="urn:oasis:names:tc:dss:1.0:profiles:XSS:certificateAttributes:IssuerDistinguished
Name"/>
      <urn:AttributeDesignator
Name="urn:oasis:names:tc:dss:1.0:profiles:XSS:certificateAttributes:NotBefore"/>
      <urn:AttributeDesignator
Name="urn:oasis:names:tc:dss:1.0:profiles:XSS:certificateAttributes:NotAfter"/>
```

#### Resposta:

```
<dss:VerifyResponse Profile="urn:oasis:names:tc:dss:1.0:profiles:XSS"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <dss:Result>
    <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>
    <dss:ResultMinor>urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:valid:certificate:
Definitive</dss:ResultMinor>
  </dss:Result>
  <dss:OptionalOutputs>
    <urn:X509CertificateInfo xmlns:urn="urn:oasis:names:tc:dss:1.0:profiles:XSS">
      <urn:Attribute
Name="urn:oasis:names:tc:dss:1.0:profiles:XSS:certificateAttributes:Version">
        <urn1:AttributeValue xsi:type="xs:integer"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:urn1="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">3</urn1:AttributeValue>
      </urn:Attribute>
      <urn:Attribute
Name="urn:oasis:names:tc:dss:1.0:profiles:XSS:certificateAttributes:SerialNumber">
```

## 2.2 Validació de signatures

Els diferents formats de signatura que podem validar contra PSIS, són els següents:

- Signatures simples CMS (Cryptographic Message Syntax).

Estàndard de l'IETF per missatgeria protegida criptogràficament, basat en la sintaxi PKCS#7. Es pot fer servir per signatura digital, autenticació, i encriptació de qualsevol tipus de dades digitals.

- Signatures simples XMLDSig (XML Digital Signature).

Estàndard de W3C que defineix la sintaxi i les regles de processat de signatures en format XML. La signatura XML proveeix serveis d'integritat, d'autenticació de missatge, i/o d'autenticació del signatari, per qualsevol tipus de dades, localitzades o no a la mateixa signatura.

- Signatures avançades XAdES (XML Advanced Electronic Signatures).

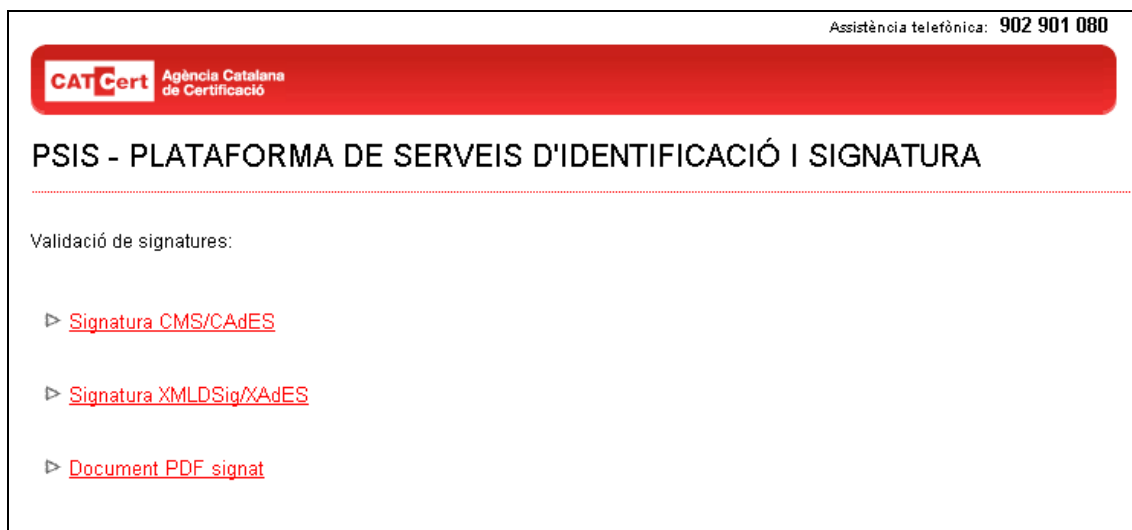
Estàndard de W3C que defineix la sintaxi i les regles de processat de signatures avançades en format XML. Aquest estàndard estén l'estàndard XMLDSig al domini del no rebuig, ampliant el format de la signatura electrònica per allargar la seva validesa al llarg del temps.

- Signatures avançades CAdES (CMS Advanced Electronic Signatures).

Estàndard de l'IETF que defineix la sintaxi i les regles de processat de signatures avançades en format CMS. Estén l'estàndard CMS al domini del no rebuig, ampliant el format de la signatura electrònica per allargar la seva validesa al llarg del temps.

## 2.2.0 Pàgina d'entrada a la validació de signatures

Si entrem a la validació de signatures, veurem aquesta pàgina:



Assistència telefònica: 902 901 080

**CATCert** Agència Catalana de Certificació

### PSIS - PLATAFORMA DE SERVEIS D'IDENTIFICACIÓ I SIGNATURA

---

Validació de signatures:

- ▶ [Signatura CMS/CAdES](#)
- ▶ [Signatura XMLDSig/XAdES](#)
- ▶ [Document PDF signat](#)

Les opcions que se'ns presenten són:

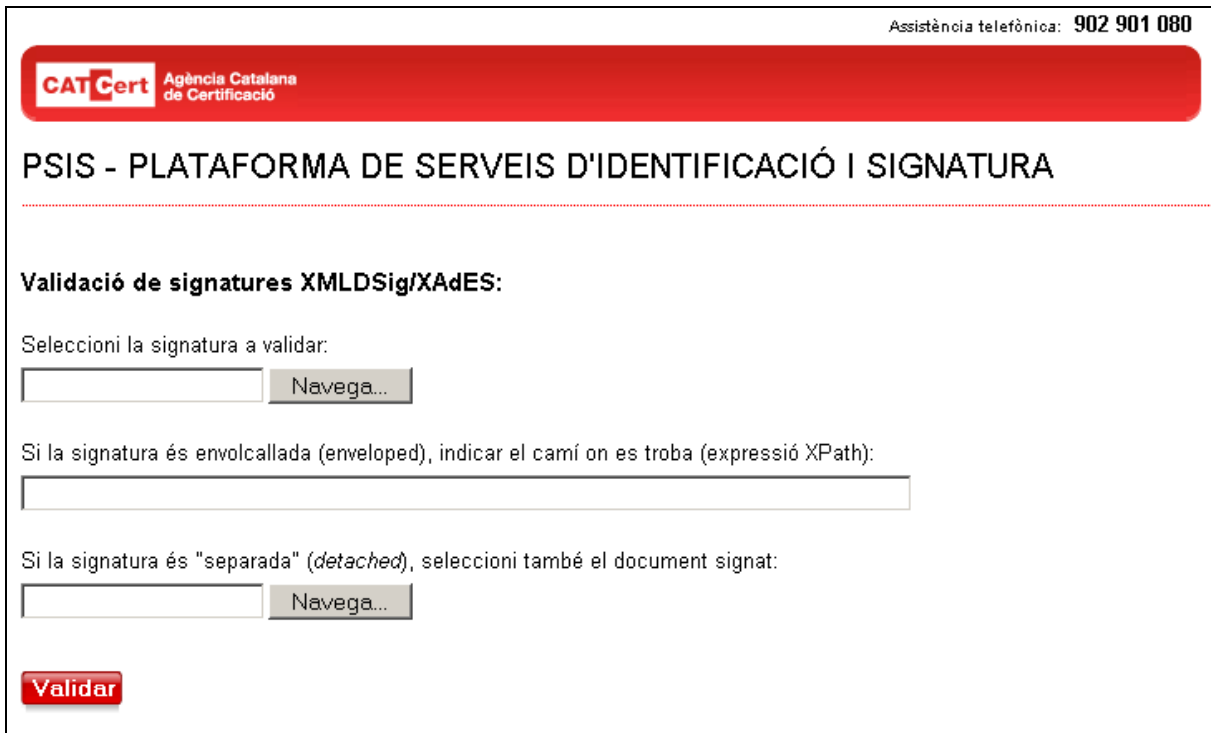
- Signatura CMS/CAdES: Validació de signatures CMS i CAdES.
- Signatura XMLDSig/XAdES: Validació de signatures XMLDSig i XAdES.
- Document PDF signat: Validació de les signatures contingudes en un document PDF.

## 2.2.1 Validació de signatures XMLDSig/XAdES

Per validar signatures XML, seguirem els següents passos. Aquests són independents de si la signatura és simple o avançada, doncs els detalls de la validació d'ambdós tipus són transparents al client.

### 2.2.1.0 Pàgina d'entrada a la validació de signatures XML

La pàgina de validació de signatures XML és:



Assistència telefònica: 902 901 080

**CATCert** Agència Catalana de Certificació

### PSIS - PLATAFORMA DE SERVEIS D'IDENTIFICACIÓ I SIGNATURA

---

**Validació de signatures XMLDSig/XAdES:**

Seleccioni la signatura a validar:

Si la signatura és envolcallada (enveloped), indicar el camí on es troba (expressió XPath):

Si la signatura és "separada" (detached), seleccioni també el document signat:

#### 2.2.1.1 Signatura envolcallada (enveloped)

Si una signatura s'utilitza per signar una part del document que la conté, aleshores és envolcallada.

Per a validar una signatura d'aquest tipus, hem de proporcionar el fitxer XML que conté la signatura. Ho farem al primer camp, allà on diu "Seleccioni la signatura a validar".

També cal especificar al servidor el path on es troba la signatura dins el document que la conté. És indispensable proporcionar-lo, per tal que PSIS sàpiga quina signatura volem actualitzar. Ho farem al segon camp (expressió XPath). Per a més informació sobre XPath, consultar: <http://www.w3.org/TR/xpath>

#### 2.2.1.2 Signatura envolcallant (enveloping)

Si la signatura conté les dades signades, aleshores és envolcallant.

Per a validar una signatura d'aquest tipus, hem de proporcionar el fitxer XML que conté la signatura. Ho farem al primer camp, allà on diu "Seleccioni la signatura a validar".

No és necessari proporcionar res més, doncs les dades signades formen, en aquest cas, part de la signatura.

### 2.2.1.3 Signatura separada (detached)

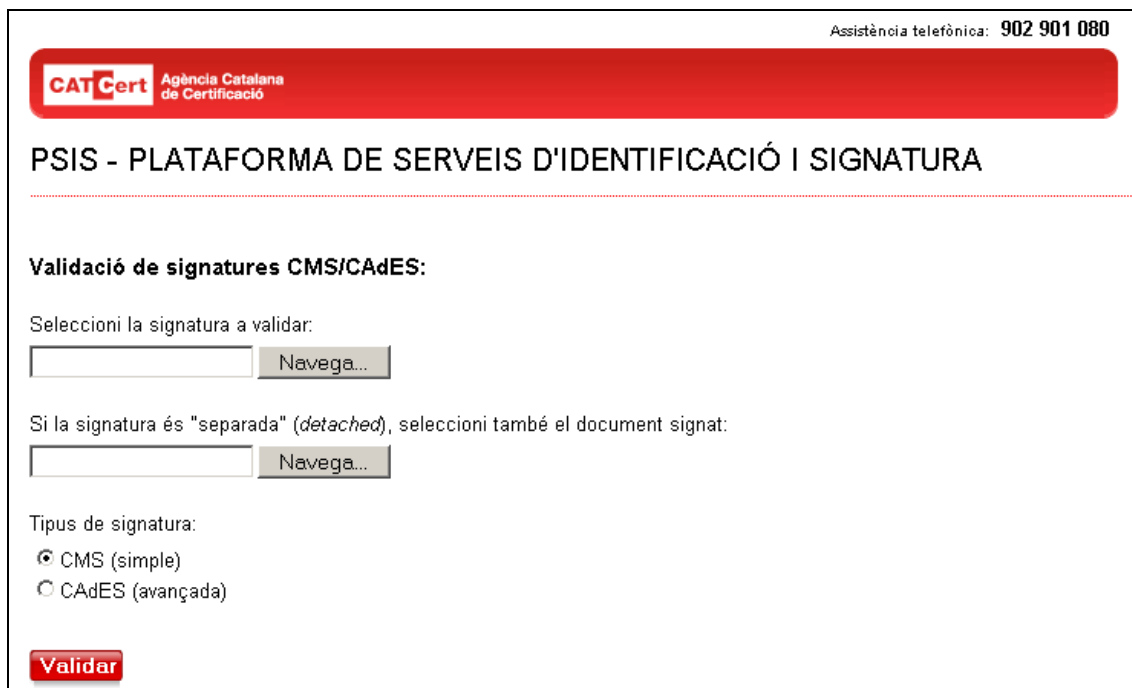
Quan la signatura no conté les dades signades, aleshores diem que és una signatura separada.

Per a validar una signatura separada, cal proporcionar la signatura i les dades signades. El fitxer que conté la signatura el proporcionarem al primer camp (on diu "Seleccioni la signatura a validar"). Les dades originals, a l'últim camp, on diu "Si la signatura és "separada" (detached), seleccioni també el document signat".

## 2.2.2 Validació de signatures CMS/CADES

Per a validar signatures CMS/CADES, seguirem els següents passos. En aquest cas, el format de la signatura no és independent de la manera en que haurem de validar-la.

### 2.2.2.0 Pàgina d'entrada a la validació de signatures CMS/CADES



Assistència telefònica: 902 901 080

**CATCert** Agència Catalana de Certificació

## PSIS - PLATAFORMA DE SERVEIS D'IDENTIFICACIÓ I SIGNATURA

---

**Validació de signatures CMS/CADES:**

Seleccioni la signatura a validar:

Si la signatura és "separada" (*detached*), seleccioni també el document signat:

Tipus de signatura:

CMS (simple)

CADES (avançada)

### 2.2.2.1 Signatura inclou les dades signades (attached)

En aquest cas, la signatura conté les dades signades.

Només cal proporcionar el fitxer amb la signatura al primer camp, on diu “*Selecioni la signatura a validar*”.

També és imprescindible especificar el tipus de la signatura, és a dir, si es tracta d'una signatura simple o avançada. Per defecte està marcada la opció de signatura simple. Si intentem validar una signatura avançada, i no especifiquem que ho és, aleshores es validarà com a simple, i no es validaran els atributs propis que la signatura contingui, com a signatura avançada. Això és així perquè PSIS no pot detectar a priori de quin tipus de signatura es tracta, de manera que si no s'indica el contrari, el validador considera que la signatura és simple.

#### 2.2.2.2 Signatura separada (detached)


Quan la signatura no conté les dades signades, aleshores diem que és una signatura separada.

En aquest cas, a més de proporcionar el fitxer amb la signatura i el tipus de signatura, cal proporcionar les dades signades. Això ho farem mitjançant el camp on diu “*Si la signatura és "separada" (detached), seleccioni també el document signat*”.

#### 2.2.2.3 Pàgina de resultats

La pantalla del resultat de la validació d'una signatura, ens mostra el resultat de la validació, i el temps de resposta de PSIS:

Assistència telefònica: **902 901 080**

Agència Catalana  
de Certificació

## PSIS - PLATAFORMA DE SERVEIS D'IDENTIFICACIÓ I SIGNATURA

---

**Validació de signatures CMS/CADES:**

La signatura és VÀLIDA.

Temps de resposta de PSIS: 1,389 seg

**Veure petició i resposta XML**

Al igual que amb els certificats, podem accedir a la pàgina que ens mostra la petició de validació de signatura enviada contra PSIS, i la resposta d'aquest, clicant al botó “Veure petició i resposta XML”.

## 2.3 Validació de documents PDF signats

La validació de la/es signatura/es incloses en un document PDF es porta a terme amb les llibreries de codi obert iText.


La validació del certificat del signatari es realitza contra PSIS.

En cas de que la signatura contingui un segell de temps, es valida també contra PSIS.

- Valida totes i cadascuna de les signatures incloses dins d'un PDF.
- Valida també les certificacions del document, si n'hi ha.
- En cas de que la signatura contingui un segell de temps vàlid, la validació del certificat es realitza en la data continguda al segell de temps.
- En cas de no incloure segell de temps, o que aquest sigui invàlid o no s'hagi pogut determinar la validesa, aleshores la data de validació per defecte és la data actual.
- Mostra un missatge general informant de si totes les signatures incloses al document són o no són vàlides.
- Mostra els detalls del resultat de la validació de cadascuna de les signatures incloses al document.

Podem validar les signatures incloses dins d'un document PDF, simplement proveint el document PDF:

Assistència telefònica: 902 901 080

Agència Catalana  
de Certificació

### PSIS - PLATAFORMA DE SERVEIS D'IDENTIFICACIÓ I SIGNATURA

---

**Validació d'un document PDF signat:**

Seleccioni el document PDF signat a validar:

La pantalla de resposta ens mostra el nom del fitxer PDF que s'ha validat, el resultat general de la validació, més els detalls de validació de cadascuna de les signatures incloses al document:

## PSIS - PLATAFORMA DE SERVEIS D'IDENTIFICACIÓ I SIGNATURA

---

### Validació d'un document PDF signat:

DOCUMENT PDF: inscripcio\_3\_firmado.pdf

TOTES LES SIGNATURES SÓN VÀLIDES.

#### DETALLS:

Nom de la signatura: formulari[0].#subform[16].signatura[0].signaturaCamp[0]

La signatura cobreix tot el document: NO

Revisió del document: 1 de 2

Document modificat: NO

Data de validació: 12/02/2009 10:10:59

Estat del certificat: VÀLID

SubjectDN CN: EMPRESA DE PRUEBAS

SubjectDN SN (NIF): Q0000001

LA SIGNATURA ES VÀLIDA.