Consorci
Administració Oberta
de Catalunya

Client Java d'exemple pel consum de productes de la plataforma PCI

Generalitat
de Catalunya

Consorci de governs locals
per a la societat de la informació

Història del Document

Versió: **1.0** *Descripció*: Versió inicial.

Elaborat per:	**Toni Llebaria Seoane**	*Data*: **10/01/2018**
Revisat per:	**Albert Ciffone**	*Data*: **17/05/2021**
Aprovat per:	**-**	*Data*: **-**

Índex

1 Introducció

Aquest document explica com cal parametritzar el client Java d'exemple pel consum de productes de la PCI, en funció de les dades de l'organisme requeridor que desitja integrar-se. Per poder fer proves en nom de l'organisme requeridor, és imprescindible fer la parametrització del client java amb les dades de l'ens requeridor.

El client Java d'exemple dóna la possibilitat de consumir els serveis via MTOM o no (més endavant parlarem d'aquesta casuística, a l'apartat 3 – Política de seguretat).

NOTA IMPORTANT: A partir de 2018 les integracions que requereixin l'enviament d'adjunts caldrà utilitzar l'enviament via MTOM de manera obligatòria.

2 Distribució

La distribució de l'exemple del client java té la següent estructura:

```
prjSIRISwatClientMTOM - java
        |
        | - src/main/java: Codi java d'exemple.
        | - src/main/resources
                        |
                        | - wsdl: wsdl del SIRI.
                        | - config: Fitxers de configuració.
                        | - keystore: claus de l'aplicació.
                        | - truststore: magatzem de confiança.
                        | - docs: peticions XML i adjunts d'exemple
```

L'exemple proporcionat utilitza el *framework apache-cxf*[1] com a motor de *webservices*, el propi motor incorpora les classes necessàries per a la implementació de les crides amb attachments *MTOM*[2] i per a la implementació del protocol de seguretat *WS-Security*[3]

S'utilitza la versió de java jdk1.8.0_111 per a la compilació i execució del client.

1 http://cxf.apache.org/
2 http://www.w3.org/TR/soap12-mtom/
3 http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

3 Requeriments d'accés als serveis

A continuació s'indiquen els requeriments necessaris per tal de poder consumir els productes d'interoperabilitat.

3.1 Sol·licitud d'autorització

- Sol·licitar al CAOC l'autorització per accedir al producte i modalitat de consum que es desitja en nom de l'organisme requeridor del qual som responsables i per a les finalitats que motiven l'accés al producte.

  Un cop l'autorització es faci efectiva, s'informarà a l'organisme requeridor la següent informació d'autorització que caldrà conèixer a l'hora d'invocar serveis d'interoperabilitat i que constarà al catàleg de serveis de la PCI:

  - Codi d'organisme requeridor
  - Codi/s de producte
  - Codi/s de modalitat de consum
  - Codi/s de finalitat

- Sol·licitar al CAOC l'autorització d'integració seguint les indicacions del portal de suport a integradors: Adjuntant el certificat CDA (Certificat Digital d'Aplicació) amb el que es signaran les peticions dirigides a la PCI via els frontals webservice (o com parlarem més endavant a l'apartat 3 – Política de seguretat, amb el qual s'autenticarà el client via capçaleres MTOM/XOP) i la IP que accedirà als serveis web entre d'altres dades.

4 Política de seguretat

4.1 Autenticació

Tota petició dirigida a la PCI via un frontal webService:

- Ha d'estar signada seguint l'estàndard WS-Security: signatura del cos i timestamp del missatge signat opcionalment.
    - El timestamp ha d'ajustar-se a aquests formats:

      yyyy-MM-dd'T'HH:mm:ss'Z'
      yyyy-MM-dd'T'HH:mm:ss'.'SSS'Z'

    - El certificat amb el que es signa la petició ha de ser vàlid (la validació es realitza contra la plataforma PSIS de CATCert), ha d'estar autoritzat a la plataforma PCI i associat al codi d'organisme que realitza la petició (element IdentificadorSolicitante del missatge).
- En cas de consumir els serveis que requereixen funcionalitats de transferència de fitxers via MTOM, les peticions no s'han de signar seguint l'estàndard WS-Security. En aquest cas, la política d'autenticació es realitza presentant el certificat a l'hora d'establir el canal HTTPS. Anàlogament al cas anterior, el certificat a presentar ha de ser vàlid i ha d'estar autoritzat a la plataforma PCI (pot ser el mateix que s'usa per signar les peticions WS-Security en les integracions que no requereixen del suport MTOM d'enviament de fitxers adjunts).

4.2 Autorització

Per a que una petició sigui autoritzada en la plataforma PCI independentment del mètode d'autenticació emprat (WS-Security o MTOM):

- L'organisme que realitza la petició ha d'estar autoritzat a executar peticions del producte, modalitat de consum i finalitat sol·licitada.

5 Configuració del client Java

5.1 Certificat d'autenticació de client

És necessari prèviament que el certificat CDA amb el que es signaran les peticions dirigides a la PCI via els frontals webservice, estigui autoritzat dins la PCI.

Al client java, cal especificar el keystore que conté les claus del certificat CDA d'autenticació. Cal modificar el fitxer "**siri-crypto-keystore.properties**" amb les dades del CDA de l'ens requeridor:

```
org.apache.ws.security.crypto.provider=org.apache.ws.security.components.crypto.Merlin
org.apache.ws.security.crypto.merlin.file=keystore/keystore.jks
org.apache.ws.security.crypto.merlin.keystore.type=JKS
org.apache.ws.security.crypto.merlin.keystore.password=xxxxxxxxx
org.apache.ws.security.crypto.merlin.keystore.provider=SUN
org.apache.ws.security.crypto.merlin.keystore.alias=alies
org.apache.ws.security.crypto.merlin.alias.password=xxxxxxxxx
```

Cal substituir els valors en vermell, pels corresponents al CDA d'autenticació:

`org.apache.ws.security.crypto.merlin.file` → Path al keystore d'autenticació.
`org.apache.ws.security.crypto.merlin.keystore.password` → Password del keystore
`org.apache.ws.security.crypto.merlin.keystore.alias` → Àlies de la clau privada del certificat de signatura
`org.apache.ws.security.crypto.merlin.alias.password` → Password de la clau privada de signatura

5.2 Magatzem de certificats de confiança

Configuració del keystore de certificats de confiança contra el qual es validarà el certificat de la signatura de les capçaleres WS-Security de la resposta i el CDS del establiment del canal segur SSL. [**siri-crypto-truststore.properties]**

- `org.apache.ws.security.crypto.merlin.file`: ruta del fitxer keystore que conté els certificats de confiança.
- `org.apache.ws.security.crypto.merlin.keystore.type`: tipus de keystore (PKCS12 o JKS).
- `org.apache.ws.security.crypto.merlin.keystore.password`: password del keystore que conté els certificats de confiança.
- `org.apache.ws.security.crypto.merlin.keystore.provider`: SUN si el tipus de keystore és JKS o BC (Bouncy Castle) en cas que sigui PKCS12. (En cas de utilitzar BC s'ha d'haver afegit prèviament aquest proveïdor.

siri-crypto-truststore.properties (exemple)

```
org.apache.ws.security.crypto.provider=org.apache.ws.security.components.crypto.Merlin
org.apache.ws.security.crypto.merlin.file=truststore/truststore-SIRI-pre.jks
org.apache.ws.security.crypto.merlin.keystore.type=JKS
org.apache.ws.security.crypto.merlin.keystore.password=caoc
org.apache.ws.security.crypto.merlin.keystore.provider=SUN
```

5.3 Fitxer de configuració per a la invocació del servei

[siri-swat.properties]

- `siriswat.endpoint.url`: URL del endpoint del webservice.
- `siriswat.cds.validate`: Boolean que indica si s'ha de verificar l'autenticitat del CDS del servei. En cas de producció ha d'estar a true, per a preproducció o desenvolupament es pot utilitzar false en cas que el CDS del servei no estigui ben configurat.
- `siriswat.cds.checkCN`: Boolean que indica si s'ha de verificar que el nom del domini es correspon amb el nom especificat al CDS. Igual que en el cas anterior a producció ha d'estar a true, per a preproducció o desenvolupament pot estar a false en cas que el CDS del servei no estigui correctament configurat.

siri-swat.properties (exemple)

```
siriswat.endpoint.url =https://serveis3-pre.app.aoc.cat/siri-proxy/services/Sincron
siriswat.cds.validate = false
siriswat.cds.checkCN = false
```

Nota important: Addicionalment a modificar en aquest fitxer el camp corresponent del endpoint, cal informar la URL corresponent en el fitxer WSDL (si ataquem al frontal síncron [Sincron.wsdl] i si ataquem al frontal asíncron [Asincron.wsdl]):

Per exemple:

```
<wsdl:service name="Sincron">
      <wsdl:port name="SincronSOAP11port_http"
      binding="s0:SincronSOAP11Binding">
            <soap:address location="https://serveis3-
      pre.app.aoc.cat/siri-proxy/services/Sincron" />
      </wsdl:port>
</wsdl:service>
```

5.4 Peticions d'exemple

Cal actualitzar les peticions d'exemple amb les dades de l'ens requeridor. A totes les peticions, caldrà substituir els següents valors en vermell pels de l'ens:

```
<IdentificadorSolicitante>9821920002</IdentificadorSolicitante>
<NombreSolicitante>CAOC</NombreSolicitante>
```

En cas de que l'organisme requeridor no estigui donat d'alta als serveis d'exemple, caldrà també substituir els codis de producte i modalitat, així com la missatgeria específica, per tal que es correspongui amb la del servei que es desitja consumir (les casuístiques de la missatgeria de cada servei estan descrites al document d'integració del servei en qüestió). Independentment de la missatgeria específica, caldrà, en aquests casos, modificar els codis següents pels corresponents:

```
<CodigoProducto>CODI_PRODUCTE</CodigoProducto>
<CodigoCertificado>CODI_MODALITAT</CodigoCertificado>
```

`CODI_PRODUCTE` → Codi del producte a consumir

`CODI_MODALITAT` → Codi de la modalitat a consumir

També cal que reviseu les següents dades, ja que les peticions que adjuntem son d'exemple però vosaltres haureu d'utilitzaar dades reals.

- El bloc de dades ***Funcionario*** s'ha d'incloure quin funcionari realitza la consulta o qui es la persona responsable d'aquesta integració (tant a la petició com a les sol·licituds.

Reviseu també el document d'integració amb la PCI en el que s'especifíca la missatgeria per obtenir més informació de que cal informar a cada camp i també les missatgeries específiques dels serveis amb els que estigueu integrant.

5.5 Classes d'exemple

Les classes proporcionades amb l'exemple són les següents:

- *cat.aoc.pci.PCIPeticio*: Classe que encarna la petició que es farà a la PCI. Té un constructor *PCIPeticio(String requestPath)* que rep la ruta relativa al recurs del projecte on es troba la petició que es vol enviar. També disposa del mètode addAttachement(String id, InputStream contenido) que serveix per a enviar un adjunt amb la petició SOAP com a adjunt MTOM. Se li ha d'indicar l'id de l'arxiu contingut a la petició (Element id de la missatgeria de la PCI contingut

dins de l'element <Fichero xmlns="http://gencat.net/scsp/esquemes/peticion">) i un InputStream amb el contingut del fitxer que s'enviarà com a adjunt MTOM.

- `cat.aoc.pci.PCIInvoker`: Classe per a invocar a la PCI. Disposa del mètode *ProcesaResponse invoke(PCIPeticio client)* per a poder invocar la PCI, el mètode rep un objecte del tipus descrit anteriorment que conté la petició i retorna un objecte de tipus `org.openuri.ProcesaResponse` que conté la resposta de la PCI. Aquesta classe s'encarrega de gestionar l'enviament amb o sense MTOM en funció de la petició. Si la crida conté attachments la petició s'envia sobre canal SSL amb MTOM, per el contrari sinó conté attachments la petició s'envia sobre canal SSL amb capçaleres WS-Security.

- `cat.aoc.pci.utils.PWCallback`: Classe que permet recuperar la clau del keystore amb el que se signen les capçaleres del WS-Security.

- `cat.aoc.pci.utils.Util`: Classe amb diverses mètodes útils per a poder fer el marshall i el unmarshall dels objectes que implementen les peticions i respostes de les crides al webservice per a poder-les mostrar en format xml.

- `cat.aoc.pci.test.Test`: Classe que realitza la invocació de la PCI. Quan s'executa dóna l'opció de triar si la petició anirà amb documentació adjunta (capçaleres MTOM) o sense documentació adjunta; en funció de la selecció anterior podrem llançar peticions de diferents serveis adequats a aquesta selecció; finalment, segons el servei seleccionat, es consumirà de forma automàtica a un dels dos entorns disponibles (Síncron o Asíncron).

  En resum, disposa de tres mètodes d'exemple:

  1) Mètode `sendSampleRequestWithoutMTOM`: fa la petició sense attachments, està signada seguint l'estàndard WS-Security.

  2) Mètode `sendSampleRequestWithMTOM`: fa la petició amb attachments, no signa seguint l'estàndard WS-Security. En aquest cas, la política d'autenticació es realitza presentant el certificat a l'hora d'establir el canal HTTPS.

  3) Mètode `sendSampleRequestWithMTOM_Asincron`: fa la petició amb attachments, no signa seguint l'estàndard WS-Security igual que en el punt 2. En aquest cas, la diferència és que ataquem al frontal asíncron, cosa que fa que la resposta que rebem de la PCI no sigui la resolució directa a la nostra petició, sinó que ens informarà del temps d'espera estimat per tal de peticionar la resposta definitva.

Nota important: Tal i com hem indicat anteriorment, és necessari modificar en el fitxer WSDL corresponent al frontal (Síncron o Asíncron), el camp corresponent del endpoint; és a dir, cal informar la URL corresponent en el fitxer WSDL (si ataquem al frontal síncron [Sincron.wsdl] i si ataquem al frontal asíncron [Asincron.wsdl]).

6 URLs d'accés de pre-producció

6.1 Clúster d'interoperabilitat (IOP)

Tots els productes de Via Oberta, excepte DEV i TESTRA.

Frontal síncron	https://serveis3-pre.iop.aoc.cat/siri-proxy/services/Sincron
Frontal asíncron	https://serveis3-pre.iop.aoc.cat/siri-proxy/services/Asincron
Frontal asíncron-resposta	https://serveis3-pre.iop.aoc.cat/siri-proxy/services/AsincronResposta

WSDL frontal síncron	https://serveis3-pre.iop.aoc.cat/siri-proxy/wsdl/Sincron.wsdl
WSDL frontal asíncron	https://serveis3-pre.iop.aoc.cat/siri-proxy/wsdl/Asincron.wsdl
WSDL frontal asíncron-resposta	https://serveis3-pre.iop.aoc.cat/siri-proxy/wsdl/AsincronResposta.wsdl

6.2 Clúster d'aplicacions (APP)

Tots els productes que no s'engloben dins del servei Via Oberta, a més de DEV i TESTRA.

Frontal síncron	https://serveis3-pre.app.aoc.cat/siri-proxy/services/Sincron
Frontal asíncron	https://serveis3-pre.app.aoc.cat/siri-proxy/services/Asincron
Frontal asíncron-resposta	https://serveis3-pre.app.aoc.cat/siri-proxy/services/AsincronResposta

WSDL frontal síncron	https://serveis3-pre.app.aoc.cat/siri-proxy/wsdl/Sincron.wsdl
WSDL frontal asíncron	https://serveis3-pre.app.aoc.cat/siri-proxy/wsdl/Asincron.wsdl
WSDL frontal asíncron-resposta	https://serveis-pre3.app.aoc.cat/siri-proxy/wsdl/AsincronResposta.wsdl

7 URLs d'accés de producció

7.1 Clúster d'interoperabilitat (IOP)

Tots els productes de Via Oberta, excepte DEV i TESTRA.

Frontal síncron	https://serveis3.iop.aoc.cat/siri-proxy/services/Sincron
Frontal asíncron	https://serveis3.iop.aoc.cat/siri-proxy/services/Asincron
Frontal asíncron-resposta	https://serveis3.iop.aoc.cat/siri-proxy/services/AsincronResposta

WSDL frontal síncron	https://serveis3.iop.aoc.cat/siri-proxy/wsdl/Sincron.wsdl
WSDL frontal asíncron	https://serveis3.iop.aoc.cat/siri-proxy/wsdl/Asincron.wsdl
WSDL frontal asíncron-resposta	https://serveis3.iop.aoc.cat/siri-proxy/wsdl/AsincronResposta.wsdl

7.2 Clúster d'aplicacions (APP)

Tots els productes que no s'engloben dins del servei Via Oberta, a més de DEV i TESTRA.

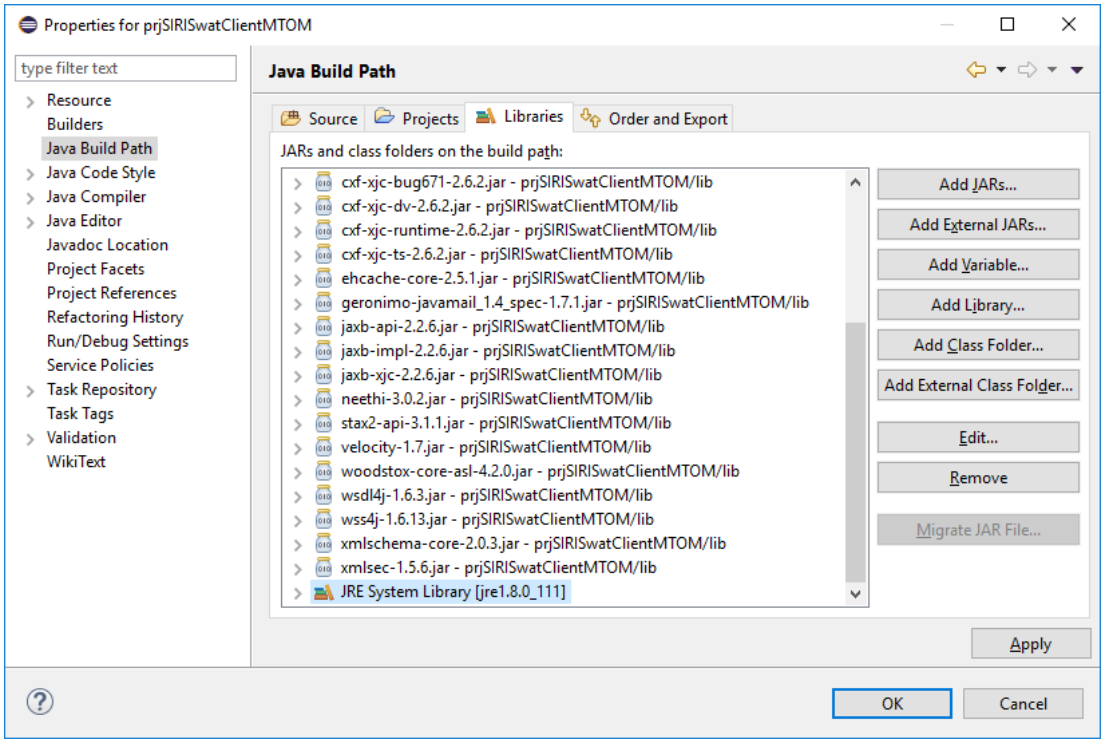
Frontal síncron	https://serveis3.app.aoc.cat/siri-proxy/services/Sincron
Frontal asíncron	https://serveis3.app.aoc.cat/siri-proxy/services/Asincron
Frontal asíncron-resposta	https://serveis3.app.aoc.cat/siri-proxy/services/AsincronResposta

WSDL frontal síncron	https://serveis3.app.aoc.cat/siri-proxy/wsdl/Sincron.wsdl
WSDL frontal asíncron	https://serveis3.app.aoc.cat/siri-proxy/wsdl/Asincron.wsdl
WSDL frontal asíncron-resposta	https://serveis3.app.aoc.cat/siri-proxy/wsdl/AsincronResposta.wsdl

8 Errors típics en la configuració del client

8.1 Revisió de versió de Java

Revisar les “properties” del Projecte Java, en l’apartat “Java Build Path” la llibreria corresponent:



8.2 Missatge: Keystore not available

```
Caused by: java.security.NoSuchAlgorithmException: P12 (per exemple)
KeyStore not available
```

En el fitxer “*siri-crypto-truststore.properties*” o “*siri-crypto-keystore.properties*”, la configuració del tipus de Keystore no és la correcta. Per tant, verificar que tenim configurat (en l’exemple es té configurat P12 i no és correcte):

org.apache.ws.security.crypto.merlin.keystore.type=JKS

8.3 Missatge: Keystore was tampered with, or password was incorrect

```
Exception in thread "main" java.io.IOException: Keystore was tampered
with, or password was incorrect
```

En el fitxer "*siri-crypto-truststore.properties*" o "*siri-crypto-keystore.properties*", la configuració del password del fitxer JKS no és la correcta. Per tant, verificar que tenim configurat:

org.apache.ws.security.crypto.merlin.keystore.password=caoc (o el que correspongui)

8.4 Missatge: no such provider

```
Caused by: java.security.NoSuchProviderException: no such provider: XXX
```

En el fitxer "*siri-crypto-truststore.properties*" o "*siri-crypto-keystore.properties*", la configuració del proveïdor criptogràfic no és la correcta. Per tant, verificar que tenim configurat:

org.apache.ws.security.crypto.merlin.keystore.provider=SUN

8.5 Missatge: General security error (revisar l'àlies del certificat)

```
Caused by: org.apache.ws.security.WSSecurityException: General security
error (No certificates for user XXXX were found for signature)
```

En el fitxer "*siri-crypto-keystore.properties*", la configuració de l'àlies del certificat amb el qual es vol fer l'autenticació, no és la correcta. Per tant, verificar que tenim configurat:

org.apache.ws.security.crypto.merlin.keystore.alias=àlies correcte del certificat

8.6 Missatge: Cannot recover key

```
Exception in thread "main" java.security.UnrecoverableKeyException: Cannot
recover key
```

En el fitxer "*siri-crypto-keystore.properties*", la configuració del password de l'àlies del certificat amb el qual es vol fer l'autenticació, no és la correcta. Per tant, verificar que tenim configurat:

org.apache.ws.security.crypto.merlin.alias.password=password correcte de l'àlies del cert.

9 Missatges típics en les peticions XML

9.1 Missatge: xmlObjectToString ... NullPointerException

`Error executing external function "xmlObjectToString" - "java.lang.NullPointerException"`

- Això és degut a que consumim un servei de Via Oberta atacant al clúster APP (Clúster d'Aplicació); és a dir, s'ataca a la URL https://serveis3-pre.app.aoc.cat/... quan la URL correcte per aquest servei és https://serveis3-pre.iop.aoc.cat/...
- O consumim un servei tipificat com d'aplicació (com per exemple ENOTUM, ETAULER, etc.) al clúster IOP (Clúster de Via Oberta); és a dir, s'ataca a la URL https://serveis3-pre.iop.aoc.cat/... quan la URL correcte per aquest servei és https://serveis3-pre.app.aoc.cat/...
- Aquestes URLs aniran configurades al fitxer corresponent Sincron.wsdl o Asincron.wsdl

9.2 Missatge: No es permet emprar autenticació WS-Security....

`"No es permet emprar autenticació WS-Security si estan activades les optimitzacions MTOM/XOP. Useu autenticació per certificat de client SSL."`

Tal i com s'ha detallat en l'apartat 4 – Política de Seguretat, per tal d'annexar documentació en la petició XML mitjançant capçaleres MTOM/XOP, no es pot emprar signatura WS-Security (com es fa amb les peticions XML cap a la PCI sense documentació annexa).

9.3 Missatge: Transmissió ja enregistrada al sistema

`"Transmissió ja enregistrada al sistema"`

El camp <*IdPeticion*> de la petició XML, ha de ser únic en les nostres plataformes. Per tant, aquest error es mostrarà cada vegada que les dades informades en aquest camp coincideixin amb una petició ja llançada en un altre moment. Des de l'AOC recomanem seguir un patró que diferencii clarament les peticions que venen del vostre ens.

Per exemple: *INE10-MODALITAT-YYY* on:

INE10: Codi INE10 de l'ens integrat
MODALITAT: Codi modalitat a consumir
YYY: autonumèric

9.4 Missatge: Modalitats [*XYZ*] no enregistrades

"Error en el procés d'autorització. Modalitats [*XYZ*] no enregistrades."

El camp <*CodigoCertificado*> de la petició XML no existeix en la nostra plataforma, és a dir, no s'ha informat correctament el codi Modalitat a consumir.

9.5 Missatge: Producte *XYZ* no enregistrat

"Error en el procés d'autorització. Producte *XYZ* no enregistrat."

El camp <*CodigoProducto*> de la petició XML no existeix en la nostra plataforma, és a dir, no s'ha informat correctament el codi del Servei a consumir.

9.6 Missatge: Organismes [*XYZ*] no enregistrats

"Error en el procés d'autorització. Organismes [*XYZ*] no enregistrats."

El camp <*IdentificadorSolicitante*> de la petició XML, que conté el codi INE10 de l'ens que consumeix el servei, no està donat d'alta a la nostra plataforma, és a dir, no s'ha informat correctament el codi INE10 del ens que s'està integrant.

9.7 Missatge: Organismes [*XYZ*] no autenticats ni amb .....

"Error en el procés d'autorització. Organismes [*XYZ*] no autenticats ni amb el CIF (XX) ni amb el certificat (CN=XX...) presentats."

El certificat utilitzat per l'autenticació a la PCI, no és el que l'ens integrador va facilitar a l'AOC per a que el configurés als seus entorns. Per tant, no es correla correctament el codi Organisme amb el certificat presentat en l'autenticació.

9.8 Missatge: Finalitats [*XYZ*] no enregistrades

"Error en el procés d'autorització. Finalitats [*XYZ*] no enregistrades."

El camp <*Finalidad*> de la petició XML no existeix en la nostra plataforma, és a dir, no s'ha informat correctament el codi Modalitat a consumir. Normalment, l'error és degut a que a l'entorn de PRO s'està informant la finalitat de PRE o al inrevés.

9.9 Missatge: La petició específica no compleix l'schema

"La petició específica no compleix l'schema"

Les dades específiques informades en la petició XML, no compleixen l'esquema específic del producte a consumir.

Per tal de revisar perquè no compleix l'esquema, el que recomanem es que a mesura que aneu avançant, valideu si l'XML que aneu fent es correcte, per exemple amb Notepad++ seguint el següent procediment:

- Obrir Notepad++
- Crear un arxiu nou: Archivo > Nuevo
- Posar-ho en format UTF-8: Codificación => Codificar en UTF-8
- Posar el contingut de les dades genèriques de la petició
- Anar a validar seleccionant la ruta del XSD : Plugins > XML Tools > Validate now
- Revisar els possibles errors de validació
- Fer el mateix amb les dades específiques

9.10 Missatge: Error en el procés d'autenticació. Certificat invàlid

"Error en el procés d'autenticació. Certificat invàlid [Cannot determine whether key is trusted or not., Cannot determine revocation status of the signing key., The signing key is outside its static validity interval.]"

El certificat utilitzat per realitzar la signatura en les capçaleres WSSecurity de la petició XML, no és vàlid degut a que està caducat o revocat.