Consorci AOC

# Codis de resposta de PSIS

Áurea Alcaide Izquierdo
20-4-2017

# Índex

# 1. *Result*

El camp "<*Result*>" de protocol DSS (Digital Signature Services) conté informació sobre el resultat del processat de la operació sol·licitada. Consta de tres elements fill que són:

<ResultMajor> → Aporta informació a alt nivell sobre el processat de la operació.

<ResultMinor> → Aporta informació sobre el resultat de la operació.

<Message> → És un camp opcional que pot aparèixer o no, i que en cas de ser-hi present aporta informació detallada en llenguatge entenedor, que pot ser utilitzada o no pel client per temes de log, debug, etc...

Els camps "<*ResultMajor*>" i "<*ResultMinor*>" sempre seran presents en totes les respostes de PSIS.

## 1.1 *ResultMajor*

Informa del processat o no de la operació sol·licitada pel client.

Els possibles valors que por prendre són:

| **urn:oasis:names:tc:dss:1.0:resultmajor:[valor]** | | |
|---|---|---|
| **Valor** | **Tipus** | **Descripció** |
| *Success* | OK | Petició processada correctament. |
| *RequesterError* | Error | El missatge que conté la petició del client es incorrecte, ja sigui sintàctica o semànticament. |
| *ResponderError* | Error | La petició no s'ha pogut processar correctament per un error en el servidor. |

## 1.2 *ResultMinor*

Aporta informació sobre el resultat de la operació.

En cas de que no s'hagi pogut processar la petició per error tant en la part de client com en la de servidor, el camp *ResultMinor* aportarà informació sobre l'error produït.

### 1.2.1 Genèrics

Els següents codis d'error són generals, i el servidor pot retornar-los per qualsevol de les operacions que es poden realitzar amb PSIS.

Quan el camp *ResultMajor* és *RequesterError*, PSIS pot retornar els següents valors pel camp *ResultMinor*:

| **urn: oasis:names:tc:dss:1.0:resultminor:[valor]** | | |
|---|---|---|
| **Valor** | **Tipus** | **Descripció** |
| *NotAuthorized* | Error | El client no està autoritzat a realitzar la operació especificada. |
| *NotSupported* | Error | No es suporta o reconeix la petició sol·licitada pel client. |
| *InvalidSignatureObject* | Error | El contingut de l'element *SignatureObject* de la petició no és correcte. |
| *InvalidOptionalInput* | Error | L'*OptionalInput* especificat no està suportat pel perfil de la petició o pel servidor. |
| *XMLDocumentNotValid* | Error | No es pot validar el document contra el seu esquema. |

| | | |
|---|---|---|
| *NotParseableXMLDocument* | Error | No es pot *parsejar* el document com a un XML vàlid. |
| *XPathEvaluationError* | Error | El resultat d'avaluar l'expressió XPath indicada és erroni. |
| *InvalidCertificateAttribute* | Error | S'ha demanat un atribut inexistent per a ésser extret del certificat. |
| *invalid:InvalidHashLength* | Error | La longitud del hash proporcionat no coincideix amb la de l'algorisme de hash especificat. |

Quan el camp *ResultMajor* és *ResponderError*, PSIS pot retornar el següent valor al camp *ResultMinor*:

| **urn: oasis:names:tc:dss:1.0:resultminor:[valor]** | | |
|---|---|---|
| **Valor** | **Tipus** | **Descripció** |
| *InternalServerError* | Error | S'ha produït un error intern en el servidor. |

### 1.2.2 Validació de certificats

En el cas de les operacions de validació de certificats, els codis que pot retornar PSIS són:

| **urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:valid:certificate:[valor]** | | |
|---|---|---|
| **Valor** | **Tipus** | **Descripció** |
| *Definitive* | Vàlid | El certificat d'entitat final enviat a validar es vàlid. |
| *Temporal* | Vàlid | El certificat d'entitat final enviat a validar es vàlid però el servidor no té certesa absoluta de que aquesta validesa sigui definitiva. |

| **urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:invalid:certificate:[valor]** | | |
|---|---|---|
| **Valor** | **Tipus** | **Descripció** |
| *OnHold* | Invàlid | El certificat d'entitat final enviat a validar està en estat suspès. |
| *Revoked* | Invàlid | El certificat d'entitat final enviat a validar està revocat. |
| *Expired* | Invàlid | El certificat d'entitat final enviat a validar ha expirat. |
| *NotYetValid* | Invàlid | El certificat d'entitat final enviat a validar encara no ha començat el seu període de validesa. |
| *CertificatePolicyNotSupported* | Invàlid | El certificat enviat està estampat seguint una política de certificació no suportada pel servidor. |
| *QualifiedCertificateRequired* | Invàlid | El servidor requeria que el certificat a validar fos qualificat i l'enviat no ho és. |

| **urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:unknown:certificate:[valor]** | | |
|---|---|---|
| **Valor** | **Tipus** | **Descripció** |
| *CertificateNotEE* | Error | El certificat enviat a validar no és un certificat d'entitat final. |
| *Status_NoCertificatePathFound* | Error | El servidor no ha pogut construir una cadena de certificats vàlida a partir del certificat d'entitat final a validar. Això pot ser degut a que no disposa d'accés als certificats de les autoritats de certificació intermitges, a la informació de revocació d'aquests certificats, o bé a l'arrel de confiança en la què finalitza la cadena. |
| *PathValidationFails* | Error | No s'ha pogut validar la cadena de certificats del certificat d'entitat final a validar. |
| *RevocationStatusInfoNotFound* | Error | El servidor no pot trobar la informació de revocació d'algun dels certificats de la cadena. |

| | | |
|---|---|---|
| *UntrustedRevocationStatusInfo* | Error | El servidor pot trobar la informació de revocació però no confia en ella donat que no és vàlida criptogràficament o bé el seu període de validesa ha expirat. |
| *BadCertificateFormat* | Error | El certificat a validar no està codificat correctament. |
| *BadCertificateSignature* | Error | La signatura que protegeix el certificat no és vàlida. |

### 1.2.3 Validació de signatures i segells de temps

En el cas de les operacions de validació de signatures i segells de temps, els codis que pot retornar PSIS són:

| **urn:oasis:names:tc:dss:1.0:resultminor:valid:signature:[valor]** | | |
|---|---|---|
| **Valor** | **Tipus** | **Descripció** |
| *OnAllDocuments* | Vàlid | Signatura o segell de temps vàlids. |
| *onTransformedDocuments* | Vàlid | Signatura o segell de temps vàlids sobre documents enviats amb transformacions no especificades pel client. |
| *notAllDocumentsReferenced* | Vàlid | Signatura o segell de temps vàlids sobre algun dels documents enviats pel client, però no tots els documents adjunts dins dels *InputDocuments* estan referenciats per la signatura. |
| *allNecessaryIdentifiersNotPresent* | Vàlid | Signatura o segell de temps vàlids, però no hi són presents tots els identificadors en els elements de la signatura (per exemple un segell d'arxiu sense atribut *Id*, etc...) |

| **urn:oasis:names:tc:dss:1.0:resultminor:invalid:[valor]** | | |
|---|---|---|
| **Valor** | **Tipus** | **Descripció** |
| *refencedDocumentNotPresent* | Invàlid | La petició de validació no conté algun dels documents referenciats per la signatura. |
| *signatureNotPresent* | Invàlid | El document PDF enviat a validar no conté cap signatura. |
| *incorrectSignature* | Invàlid | La signatura no és correcta, ja sigui perquè s'ha generat incorrectament, o perquè ha sigut modificada. |
| *indeterminateKey* | Invàlid | El servidor no pot determinar la validesa del certificat de la signatura. Això pot ser degut a que no pot construir el path fins a una arrel de confiança, o bé que no pot validar aquest path. La no validació ve causada normalment per l'absència d'informació de revocació vàlida. |
| *untrustedKey* | Invàlid | El servidor no considera que el certificat de la signatura sigui vàlid. Això vol dir que està revocat o *suspès*. |

| **urn:oasis:names:tc:dss:1.0:resultminor:[valor]** | | |
|---|---|---|
| **Valor** | **Tipus** | **Descripció** |
| *ValidMultiSignatures* | Vàlid | Totes les signatures són vàlides. |
| *InvalidMultiSignature* | Invàlid | Alguna o totes les signatures són invàlides. |
| *CannotDeterminePDUValidity* | Error | Impossible determinar la validesa de la PDU. |
| *InvalidTransformURI* | Error | L'URI de transformada especificada no és vàlida o no està suportada. |
| *CannotPerformTransform* | Error | El servidor no pot dur a terme la transformació. |
| *InvalidSignatureCheckDetails* | Error | La signatura és invàlida. Consultar els detalls de validació per determinar les causes. |
| *inappropiate:signature* | Error | La signatura no és correcta en el context actual. Per exemple, si el servidor considera que l'associació entre la signatura i la política de signatura o la semàntica no és satisfactòria. |

| | | |
|---|---|---|
| *indetermined:checkOptionalOutput* | Error | El client haurà de verificar la resposta obtinguda en l'element *ProcessingDetails* per a determinar l'error. |
| *InvalidDocumentProvided* | Error | El document proporcionat no és vàlid. |
| *CannotDetermineSignatureValidity* | Error | El servidor no pot determinar la validesa de la signatura. Per exemple, si no pot validar algun atribut de la signatura. |
| *InvalidTimestampProvided* | Error | El segell de temps proporcionat en la petició no és correcte. |
| *InvalidSignatureType* | Error | Tipus de signatura no suportat. Els tipus suportats són, actualment:<br>Signatures:<br>CMS (urn:ietf:rfc:3852, urn:ietf:rfc:3369)<br>CAdES (http://uri.etsi.org/01733/v1.6.3#, http://uri.etsi.org/01733/v1.7.3#)<br>XMLDSig (urn:ietf:rfc:3275)<br>XAdES (http://uri.etsi.org/01903/v1.2.2#, http://uri.etsi.org/01903/v1.3.2#)<br>Segells de temps:<br>CMS (urn:ietf:rfc:3161)<br>XML (oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken) |
| *SignaturePolicyNotFound* | Error | La política de signatura no està carregada en PSIS. |
| *InvalidSignatureAttribute* | Error | S'ha demanat un atribut inexistent per a ésser extret de la signatura. |

### 1.2.4 Creació de signatures i segells de temps

| **urn:oasis:names:tc:dss:1.0:resultminor:[valor]** | | |
|---|---|---|
| **Valor** | **Tipus** | **Descripció** |
| *NotAuthorized* | Error | El client no està autoritzat a signar amb la clau especificada. |
| *MoreThanOneRefUriOmitted* | Error | En el cas de signatures detached s'ha adjuntat més d'un document amb URI nul·la (no permès pel protocol DSS). |
| *KeySelectorNotProvided* | Error | La petició no inclou informació sobre la clau amb la que signar. |
| *SignatureFormsNotSupported* | Error | S'ha sol·licitat la generació d'un format de signatura no suportat pel servidor. Els formats suportat són:<br>urn:oasis:names:tc:dss:1.0:profiles:XAdES:forms:BES<br>urn:oasis:names:tc:dss:1.0:profiles:XAdES:forms:EPES<br>urn:oasis:names:tc:dss:1.0:profiles:XAdES:forms:ES-T<br>urn:oasis:names:tc:dss:1.0:profiles:XAdES:forms:ES-C<br>urn:oasis:names:tc:dss:1.0:profiles:XAdES:forms:ES-X-Type-1<br>urn:oasis:names:tc:dss:1.0:profiles:XAdES:forms:ES-X-Type-2<br>urn:oasis:names:tc:dss:1.0:profiles:XAdES:forms:ES-X-L-Type-1<br>urn:oasis:names:tc:dss:1.0:profiles:XAdES:forms:ES-X-L-Type-2<br>urn:oasis:names:tc:dss:1.0:profiles:XAdES:forms:ES-A |

## 1.3 *ResultMessage*

El camp *ResultMessage* és un camp descriptiu que pot incloure detalls del resultat de la operació en llenguatge entenedor. L'idioma del missatge és l'anglès.

Aquest camp és susceptible de canviar, per la qual cosa el client no haurà de prendre el literal com a valor fix. Per exemple, en molts casos aquest camp podrà incloure text provinent de la gestió d'excepcions de java.

### 1.3.1 Creació de signatures i segells de temps

En aquest cas, si la signatura o el segell de temps s'ha generat correctament, PSIS retorna:

| | |
|---|---|
| ResultMajor | urn:oasis:names:tc:dss:1.0:resultmajor:Success |
| ResultMessage | Signature created |

### 1.3.2 Validació externa

En el cas de validacions de certificats i signatures on el certificats està estampat segons una política no classificada pel Consorci AOC, validacions que PSIS realitza recolzant-se en el servei d'@firma, sí que s'ha seguit una sintaxi concreta per aquest camp, segons s'especifica al quadre següent:

| **Validació de certificats: política de certificat no suportada** | |
|---|---|
| ResultMajor: | urn:oasis:names:tc:dss:1.0:resultmajor:Success |
| ResultMinor: | urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:invalid:certificate:CertificatePolicyNotSupported |
| ResultMessage: | Problems retrieving revocation information from @Firma: The requested certificate policy is not supported by @Firma. |
| **Validació de signatures: política de certificat no suportada** | |
| ResultMajor: | urn:oasis:names:tc:dss:1.0:resultmajor:Success |
| ResultMinor: | urn:oasis:names:tc:dss:1.0:resultminor:NotSupported |
| ResultMessage: | Problems retrieving revocation information from @Firma: The requested certificate policy is not supported by @Firma. |
| **Validació de certificats i signatures: no és possible validar la cadena de certificació** | |
| ResultMajor: | urn:oasis:names:tc:dss:1.0:resultmajor:Success |
| ResultMinor: | urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:unknown:certificate:PathValidationFails |
| ResultMessage: | Certification path could not be validated. Problems retrieving revocation information from @Firma: *{missatge excepció}* |
| **Validació de certificats i signatures: problemes amb el consum del servei @Firma** | |
| ResultMajor: | urn:oasis:names:tc:dss:1.0:resultmajor:Success |
| ResultMinor: | urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:unknown:certificate:PathValidationFails |
| ResultMessage: | Problems retrieving revocation information from @Firma: *{missatge excepció}* |

On *{missatge excepció}* és el text de l'excepció java.