



**Administració
Oberta de
Catalunya**

Guia bàsica pels integradors de PSIS

Documentació d'integració al servei de Validació i Segellat de Temps

Data: 26/07/2024



Localret

Control documental

Estat formal	
Elaborat per	Toni Marcos Cardona
Revisat per	David Garcia, Ramon Navalón, Josep Riudavets, Joan Mir, Pol Prats, Àurea Alcaide
Aprovat per	Joan Mir, Àurea Alcaide
Data de creació	15/8/2006
Nivell accés informació	Pública
Títol	Guia bàsica pels integradors de PSIS
Fitxer	Guia_basica_integradors_P SIS_v2.0.docx
Control de còpies	Només les còpies disponibles a la Seu electrònica del Consorci AOC garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades.
Drets d'autor	<p>Aquesta obra està subjecta a una llicència Reconeixement - No comercial- Sense obres derivades 3.0 Espanya de Creative Commons. Per veure'n una còpia, visiteu http://creativecommons.org/licenses/by-nc-sa/3.0/deed.ca o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.</p> 

Control de versions

Data:	16/07/2024
Descripció:	Creació del document.
Data:	2/08/2006
Descripció:	Reestructuració de continguts.
Data:	14/08/2006
Descripció:	Segon procés de refinament dels continguts. Canvis en els codis.
Data:	17/08/2006
Descripció:	Refinament i reestructuració dels apartats relatius a validacions de signatures. Afegits referències a <i>Timestamp Profile</i> . Canvis menors en els codis.

Data:	18/09/2006
Descripció:	Revisió global dels continguts amb canvi d'estructuració per a suportar futures funcionalitats. Afegit annex amb els esquemes DSS/XSS.
Data:	29/09/2006
Descripció:	Afegit validació signatures a documents PDF.
Data:	19/10/2006
Descripció:	Refinament dels continguts.
Data:	14/12/2006
Descripció:	Refinament dels continguts.
Data:	18/12/2006
Descripció:	Identificacions de versions.
Data:	03/01/2007
Descripció:	Millores explicatives.
Data:	06/02/2007
Descripció:	Completar exemples de validació de certificats.
Data:	09/02/2007
Descripció:	Servidors referenciats normalitzats a psisbeta.
Data:	08/05/2007
Descripció:	Autenticació. Clients Java, .NET i VB. Revisió global: millores, correcció errors.
Data:	03/10/2007
Descripció:	Millores explicatives.
Data:	21/01/2008
Descripció:	Millores explicatives.
Data:	09/06/2008
Descripció:	Eliminació URLs de QUA.
Data:	21/03/2011
Descripció:	Correcció segells temps.
Data:	26/07/2024
Descripció:	Actualització de la plantilla del document. Actualització de les URLs del servei. Revisió completa i actualització dels apartats 1 al 5, i annexos. Inserció de nou apartat 6 amb codis de resposta i eliminació com a annex.

Índex

Guia bàsica pels integradors de PSIS	1
Control documental	2
Control de versions	2
Índex.....	4
Glossari	6
Figures	7
1. Introducció	9
2. Prestació de servei	11
3. Arquitectura de PSIS	12
4. Missatgeria	13
5. Funcionalitats	20
5.1. Validació de certificats	20
5.2. Validació de signatures en format PKCS#7 / CMS i XML.....	27
5.3. Validació de signatures XAdES	41
5.4. Validació de documents PDF signats	48
5.5. Creació de segells de temps.....	51
5.5.1. Creació de segell de temps mitjançant protocol TCP	52
5.5.2. Creació de segell de temps amb missatgeria DSS	52
5.5.3. Validació de segells de temps amb missatgeria DSS	59
6. Codis de resposta	64
6.1. Result	64
6.1.1. ResultMajor.....	64
6.1.2. ResultMinor.....	64
6.1.3. ResultMessage	68
7. Requisits previs	70
7.1. Comunicacions	70
7.2. Software	71
7.3. WSDL.....	71

8. Creació del client	73
8.1. Java	73
8.2. .NET (C#)	80
8.3. Visual Basic 6	82
9. Creació de la missatgeria.....	87
9.1. Java	87
9.2. .NET (C#)	99
9.3. Visual Basic 6	111
10. Annexes	119
10.1. Referències.....	119
10.2. Atributs de consulta d'un certificat.....	119
10.3. Atributs de consulta d'una signatura	122
10.4. Esquema del protocol DSS i el seu perfil XSS.....	122

Glossari

CA	<i>Certificate Authority (Autoritat de Certificació)</i>
CAdES	<i>CMS Advanced Electronic Signatures</i>
CMS	<i>Cryptographic Message Syntax</i>
DSS	<i>Digital Signature Services</i>
JDK	<i>Java Developer Kit</i>
JRE	<i>Java Runtime Environment</i>
OASIS	<i>Organization for the Advancement of Structured Information Standards</i>
PDF	<i>Portable Document Format</i>
PKCS7	<i>Public Key Cryptography Standards</i>
PKI	<i>Public Key Infrastructure</i>
PSIS	<i>Plataforma de Serveis de Identificació i Signatura</i>
RFC	<i>Request For Comments</i>
SOAP	<i>Simple Object Access Protocol</i>
SSL	<i>Secure Sockets Layer</i>
TLS	<i>Transport Layer Security</i>
TSA	<i>Transportation Safety Administration</i>
URI	<i>Uniform Resource Identifier</i>
URL	<i>Uniform Resource Locator</i>
UTF	<i>Universal Transformation Format</i>
VA	<i>Validation Authority (Autoritat de Validació)</i>
VB6	<i>Visual Basic 6</i>
XSS	<i>eXtended Signature Services (XSS) Profile of the OASIS Digital Signature Service (DSS)</i>
WSDL	<i>Web Service Definition Language</i>
XAdES	<i>XML Advanced Electronic Signatures</i>
XML	<i>Extensible Markup Language</i>
XMLDSig	<i>XML Digital Signatures</i>
XSD	<i>XML Schema Definition</i>

Figures

Figura 1 Esquema d'invocació de clients a PSIS	9
Figura 2 Esquema d'invocació entre serveis de PSIS	12
Figura 3 Taula amb els diferents perfils de DSS	13
Figura 4 Missatge de validació d'un certificat X509	21
Figura 5 Missatge resposta d'una validació d'un certificat X509	25
Figura 6 Missatge de validació de signatura CMS attached.....	28
Figura 7 Missatge de validació de signatura CMS detached.....	29
Figura 8 Missatge de validació de signatura XML attached enveloping	30
Figura 9 Missatge de validació de signatura XML attached enveloped	31
Figura 10 Missatge de validació de signatura XML detached	32
Figura 11 Missatge de sortida per a una validació de signatura.....	37
Figura 12 Missatge de validació d'una signature XAdES	43
Figura 13 Missatge de resposta a una validació d'una signature XAdES.....	47
Figura 14 Missatge de validació d'un document PDF	49
Figura 15 Taula de compatibilitat entre formats de segells de temps i els continguts a estampar	53
Figura 16 Missatge de creació d'un segell de temps en format XML	54
Figura 17 Missatge de creació d'un segell de temps en format CMS.....	55
Figura 18 Missatge de resposta de creació d'un segell de temps	58
Figura 19 Missatge de validació d'un segell de temps en format XML	61
Figura 20 Missatge de validació d'un segell de temps en format CMS	62
Figura 21 Missatge de resposta d'una validació d'un segell de temps	63
Figura 22 Captura de pantalla amb una connexió correcta a la plataforma PSIS.....	70
Figura 23 Contingut del fitxer ant per generar el client Java de PSIS fent servir el fitxer WSDL	75
Figura 24 Contingut del fitxer ant per compilar el client Java generat a partir del fitxer WSDL	79
Figura 25 Exemple de creació de la connexió amb la plataforma PSIS en Java	80
Figura 26 Exemple de creació de la connexió amb la plataforma PSIS en .net.....	82
Figura 27 Exemple de creació de la connexió amb la plataforma PSIS en .net.....	85
Figura 28 Exemple de creació de la connexió amb la plataforma PSIS en .net (VB 9.0)....	86
Figura 29 Exemple en Java de validació de certificats.....	89
Figura 30 Exemple en Java de validació de signatura CMS	90

Figura 31 Exemple en Java de validació de signatura XML.....	91
Figura 32 Exemple en Java de validació de signatura XAdES.....	92
Figura 33 Exemple en Java de validació de documents PDF signats	94
Figura 34 Exemple en Java de creació de segell de temps	96
Figura 35 Exemple en Java de validació de segell de temps	97
Figura 36 Exemple en Java de validació certificats amb autenticació SSL	99
Figura 37 Exemple en .net de validació de certificats	100
Figura 38 Exemple en .net de validació de signatura CMS.....	102
Figura 39 Exemple en .net de validació de signatura XML	103
Figura 40 Exemple en .net de validació de signatura XAdES	104
Figura 41 Exemple en .net de validació de document PDF signat	106
Figura 42 Exemple en .net de creació de segell de temps.....	108
Figura 43 Exemple en .net de validació de segell de temps.....	110
Figura 44 Exemple en .net de validació de segell de temps.....	111
Figura 45 Exemple en Visual Basic de validació de certificats	112
Figura 46 Exemple en Visual Basic de signatura CMS	113
Figura 47 Exemple en Visual Basic de signatura XML.....	114
Figura 48 Exemple en Visual Basic de signatura XAdES.....	115
Figura 49 Exemple en Visual Basic de document PDF signat.....	116
Figura 50 Exemple en Visual Basic de creació de segell de temps.....	117
Figura 51 Exemple en Visual Basic de creació de segell de temps.....	118

1. Introducció

L'objectiu d'aquest document és descriure la invocació de funcionalitats de PSIS fent servir el protocol DSS. Per a agilitzar i simplificar el procés d'integració de clients amb la plataforma PSIS, el Consorci AOC proporciona als seus clients un fitxer WSDL (*Web Services Definition Language*) que descriu la missatgeria DSS en un format estandarditzat.

La plataforma PSIS ofereix una sèrie de serveis d'alt nivell que permeten realitzar un gran nombre de funcionalitats relacionades amb la PKI, com ara la validació de certificats, la creació, la validació i completat de signatures digitals, la validació i completat de documents PDF signats i la creació i validació de segells de temps.

La plataforma PSIS ofereix la possibilitat de comunicar-se amb les diverses funcionalitats mitjançant diferents tipus de mecanismes.

Aquests mecanismes de connexió als serveis oferts per PSIS són els següents:

- Peticions codificades segons DSS (protocol per a serveis de signatura digital sobre *web services*), segons el protocol de l'autoritat de validació del Consorci AOC (protocol propietari per a la validació de signatures i certificats en XML sobre *web services*)
- Protocols basats en missatgeria no XML com ara el protocol de creació de segells de temps o RFC 3161.

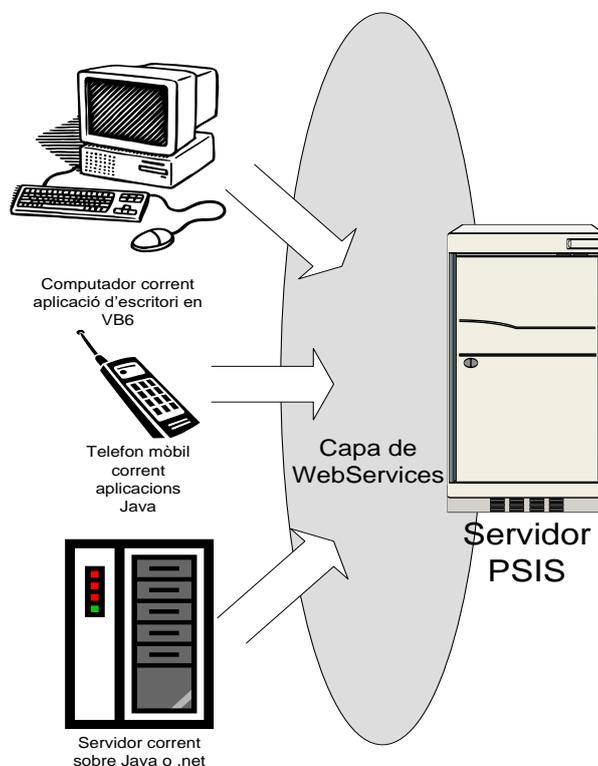


Figura 1 Esquema d'invocació de clients a PSIS

Per tant, aquest document està focalitzat en com els clients poden invocar qualsevol servei ofert per PSIS fent servir el protocol DSS. El document inclou tota la informació necessària per poder desenvolupar el software (llibries, objectes i classes) necessari per tal de poder fer ús dels serveis oferts per la plataforma PSIS.

El document està organitzat en un conjunt d'apartats on es pot trobar tota la informació necessària per a poder fer la integració amb la plataforma PSIS.

- En l'apartat 1, es dóna una visió global dels objectius que es volen assolir en quant a la integració amb els serveis oferts per PSIS.
- Dins l'apartat 3 s'introdueix breument, i amb l'ajuda d'un esquema, el sistema de prestació del servei ofert per la plataforma PSIS per a poder crear una connexió externa amb la mateixa.
- L'apartat 4, amb el suport d'un conjunt d'esquemes, descriu la missatgeria inclosa dins del protocol DSS, la qual permet tenir disponibles les comunicacions per a poder fer les operacions que es poden realitzar amb la plataforma PSIS.
- El conjunt de funcionalitats ofertes per la plataforma PSIS (validació de certificats digitals, validació de signatures digitals, validació de PDF's, validació i creació de segells de temps) es descriuen en l'apartat 5 documentant la missatgeria del protocol DSS que es necessita per tal de poder fer peticions a la plataforma PSIS i posteriorment fer el processament de la resposta i visualitzar els diferents *OptionalInputs* disponibles per a cada funcionalitat.
- Els requisits de connexió a la plataforma PSIS, el procés de creació dels mòduls necessaris per a la connexió, juntament amb exemples d'ús de cadascuna de les funcionalitats descrites en l'apartat anterior, es pot consultar en l'apartat 6. Tota aquesta informació es troba disponible en tres tecnologies diferents: Java, .NET(C#) i Visual Basic 6.
- Per a finalitzar, el document, a l'apartat 7, disposa d'un annex on s'inclouen referències, esquemes i informació que complementen i amplien els conceptes presentats en aquesta documentació.

NOTA: Per tal de poder desenvolupar el software necessari per a connectar la plataforma PSIS es fan servir tecnologies que només s'utilitzaran en algun procés descrit al present document. En aquest sentit, cal mencionar que l'objectiu d'aquest document no és el de documentar aquestes tecnologies. Per això, només es presentaran les dades necessàries per a poder fer cada procés, sense fer referència a punts tan diversos com poden ser: instal·lació (ex: Ant, Visual Basic 6, .NET), configuració (ex: configuració de nous projectes Visual Basic 6 amb referències a llibries externes), etc...

2. Prestació de servei

La plataforma PSIS presta els seus serveis en forma de serveis web (o WebServices) que són invocats mitjançant l'intercanvi de fitxers XML entre el client i el servidor que contenen les peticions de servei i les respostes del servidor a aquestes peticions.

Per tal de facilitar la creació de clients d'aquest servei la plataforma disposa d'un fitxer de definició WSDL (Web Services Definition Language) que descriu el servei, tant les estructures dels missatges intercanviats com les adreces dels propis serveis.

L'existència d'aquest fitxer permet que els clients puguin compilar-lo i generar automàticament el codi per a invocar PSIS. Per tal de poder dur a terme aquest procés, els clients només necessiten d'unes llibreries d'invocació de *web services* amb suport per a la invocació de serveis WEB fent servir *document/literal* (la majoria dels clients de *web services* incorporen aquest paradigma d'invocació). Els detalls del procés seran descrits posteriorment a l'apartat 5, ampliant la informació del procés necessari per a cadascuna de les tecnologies tractades.

D'aquesta manera, la complexitat de la lògica a desenvolupar pel client per tal de poder invocar els serveis queda reduïda a la construcció del missatge de petició, que conté les dades de la invocació, i a processar la resposta del servidor. En aquest cas, i donat que es fan servir clients de *web services*, els clients hauran de crear els *stubs* (o objectes generats a partir de la compilació del WSDL) corresponents a l'estructura del missatge i enviar-los (procés que el client del *web service* també encapsula).

Per a il·lustrar el funcionament, procedirem primer a especificar i detallar el format dels missatges a construir per tal de dur a terme les invocacions de servei (sintaxis dels XML's, adjuntant els seus *schemas* corresponents) i després, per a cada funcionalitat de la plataforma PSIS, s'inclouran exemples de com construir aquests missatges per a cada tecnologia concreta.

3. Arquitectura de PSIS

L'arquitectura de la plataforma PSIS va ésser creada fent servir un patró de components orientats a servei. Això vol dir que la plataforma està composta per multitud de serveis que s'orquestran i col·laboren entre sí per a poder donar servei, i que poden ser reutilitzats i recombinats per a donar diferents tipus de serveis.

Aquest model orientat a servei permet, tanmateix, disposar de diferents instàncies del mateix servei amb configuracions diferents. Aquesta *virtualització* del servei possibilita, per exemple, disposar de serveis, com ara diverses instàncies distingibles de serveis de validacions de certificats, que coexisteixen al mateix servidor; però que donat que disposen de configuracions diferents tenen comportaments totalment separats, tot i que el seu codi és idèntic.

Aquesta agrupació de components de grau gruixut (serveis) també permet que la composició dels mateixos no estigui lligada a codi, sinó que la relació *intra-servei* (com ara que un servei de validació de signatura X faci servir un servei de validació de certificats Y) és un paràmetre més a configurar, amb el què aquesta composició pot ésser alterada sense haver-ne de modificar codi.

Un altre avantatge d'aquest tipus d'arquitectura és que els serveis poden disposar de diferents tipus d'implementació (per exemple, un servei de signatura criptogràfica basat en llibreries *software* i un altre basat en dispositius *hardware*), sent cridats, però, per un únic servei que compleix un contracte (o interfície de servei). Això suposa un gran desacoblament entre serveis amb els següents avantatges:

- Coexistència de diferents versions de servei en el mateix servidor assignades a instàncies individuals de serveis.
- Existència de diferents implementacions per al mateix problema. Per exemple, solucions *software* vs. solucions *hardware*.

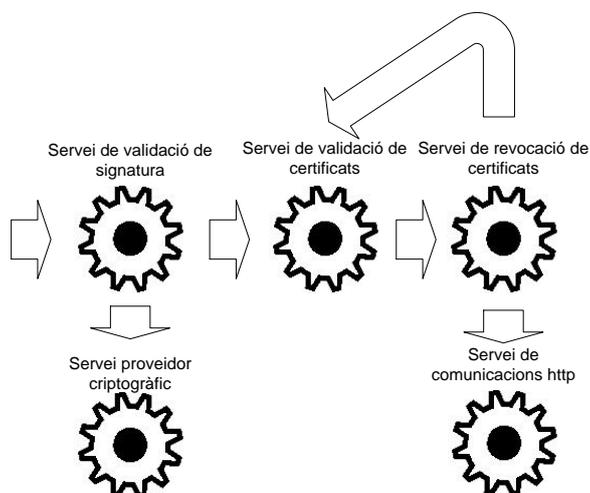


Figura 2 Esquema d'invocació entre serveis de PSIS

4. Missatgeria

Per a poder fer ús d'aquesta plataforma es requereix, com ja s'ha comentat, del desenvolupament d'uns clients que construiran missatges de petició i extrauran les respostes dels missatges provinents del servidor abstractant al client del procés d'invocació remota que es duu a terme.

Un dels protocols amb què treballa la plataforma és el DSS (*Digital Signature Services*), del consorci d'estandardització OASIS (*Organization for the Advancement of Structured Information Standards*), un protocol per a la prestació de serveis de signatura digital obert i extensible (mitjançant l'ús de perfils).

El protocol DSS Core conté una aproximació generalista als problemes derivats de la provisió de serveis de signatura electrònica. Els perfils de DSS són extensions del DSS Core que aporten més detalls i funcionalitats per a solucionar problemes més concrets.

De perfils es poden trobar diversos, però PSIS dona suport principalment a XSS (desenvolupat per CATCert i que amplia DSS permetent, entre d'altres, la validació de certificats X509), el perfil XAdES (que permet l'actualització de signatures) o el *Timestamp Profile* (que aporta més control i detalls en l'àmbit dels segells de temps sobre DSS).

També hi ha altres perfils, com el de PDF, que són suportats per PSIS i que proporcionen funcionalitats complementàries a les definides en aquesta documentació, com ara la validació de signatures sobre documents PDF (i completat a p. ex. el format PAdES-LTV).

Profiles	
DSS Protocol bàsic de creació i validació de signatures	urn:oasis:names:tc:dss:1.0:core:schema
XADES Ampliació de DSS que permet treballar amb signatures avançades XAdES i CAdES	urn:oasis:names:tc:dss:1.0:profiles:XAdES
XSS Ampliació de DSS que permet, entre d'altres validar certificats X509 de clau pública, extreure informació dels mateixos i fer servir polítiques de signatura.	urn:oasis:names:tc:dss:1.0:profiles:XSS
TIMESTAMP Defineix restriccions extres sobre la creació i validació de segells de temps via DSS.	urn:oasis:names:tc:dss:1.0:profiles:timestamping
DSS_PDF Permet validar documents PDF amb signatures PKCS#7 i signatures PAdES.	urn:oasis:names:tc:dss:1.0:profiles:DSS_PDF

Figura 3 Taula amb els diferents perfils de DSS

La documentació detallada del protocol i els seus perfils està disponible en el paquet distribuït pel Consorci AOC. Els esquemes del protocol DSS i el seu perfil XSS estan inclosos també a l'annex del present document com a informació complementària.

NOTA: Totes les descripcions d'estructures / elements que formen part de la missatgeria DSS contenen el nom del document on es pot trobar el detall de la descripció, juntament amb possibles comentaris particulars de la plataforma PSIS.

La missatgeria que intervé a la plataforma PSIS ve definida per l'estàndard DSS i funciona sota el protocol SOAP (*Simple Object Access Protocol*).

SOAP és un protocol estàndard sobre el qual es fonamenta la tecnologia de serveis web (*Web Services*). A diferència d'altres protocols de tipus binari com poden ser COM, COM+ o DCOM, els quals són propis de Microsoft, SOAP es basa en documents de text pla codificats en format XML. L'avantatge principal de codificar en XML és que els missatges són llegibles per éssers humans; però, per contra, aquests documents resultants són, en general, de tamany gran.

SOAP està dissenyat per funcionar sobre qualsevol protocol d'internet, tot i que l'ús més habitual és sobre HTTP. El fet d'utilitzar HTTP minimitza l'impacte de dispositius com Firewalls i similars, i fa accessible SOAP a pràcticament qualsevol tipologia de comunicació client-servidor.

Els missatges SOAP estan compostats per dos grans blocs funcionals: "Capçalera" (*envelope*) destinat a subministrar dades d'enrutament i "Cos" (*body*), el qual conté les dades del missatge d'usuari. Una explicació més detallada de SOAP no forma part de l'abast d'aquest document.

En aquest apartat es tracten els aspectes més importants involucrats en l'ús del protocol DSS. Tot i així, s'adjunta la referència on es pot consultar el document de l'estàndard corresponent per si fos necessària més informació sobre un apartat concret.

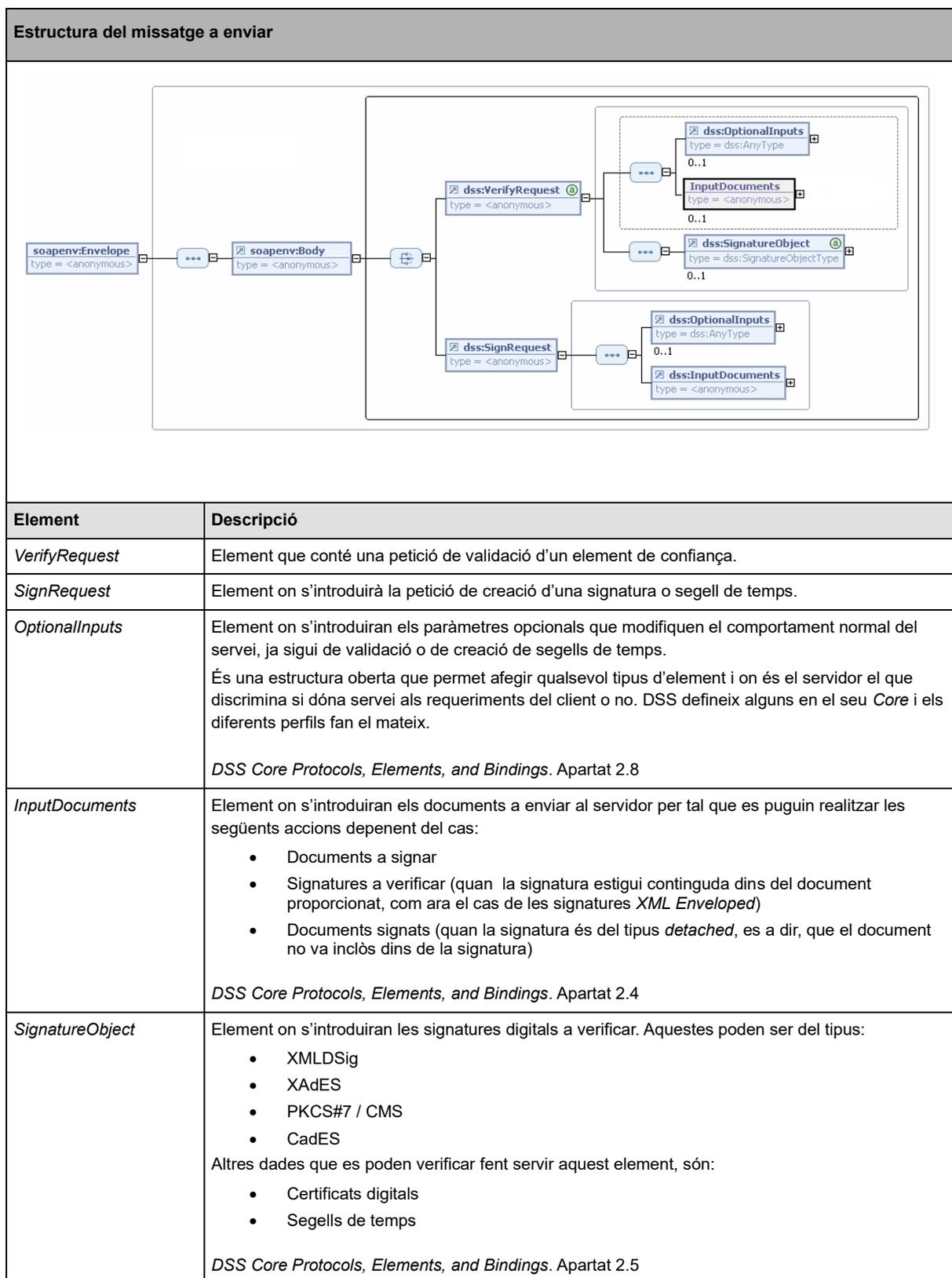
A més, es defineixen una sèrie de prefixos pels diferents espais de noms involucrats. El seu mapeig contra les URI's dels espais de noms és el següent:

- xd: <http://www.w3.org/2000/09/XMLDSig#>
- dss : urn:OASIS:names:tc:dss:1.0:core:schema
- xss : urn:OASIS:names:tc:dss:1.0:profiles:XSS
- pdf: urn:OASIS:names:tc:dss:1.0:profiles:DSS_PDF

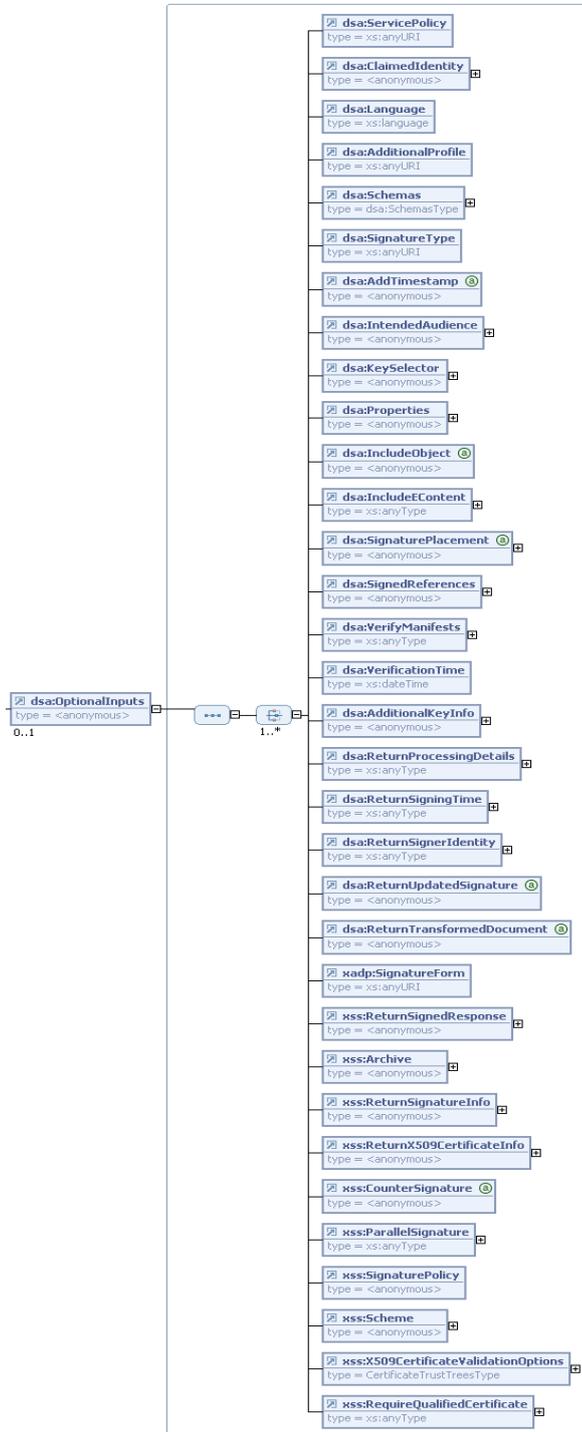
Aquí mostrem els dos tipus bàsics d'estructures que s'utilitzen al protocol DSS, juntament amb els elements bàsics que es faran servir per a compondre els missatges.

Els dos tipus principals de missatges que defineix DSS són *VerifyRequest* (per a peticions de validació) i *SignRequest* (per a peticions de signatura o estampació de segell de temps).

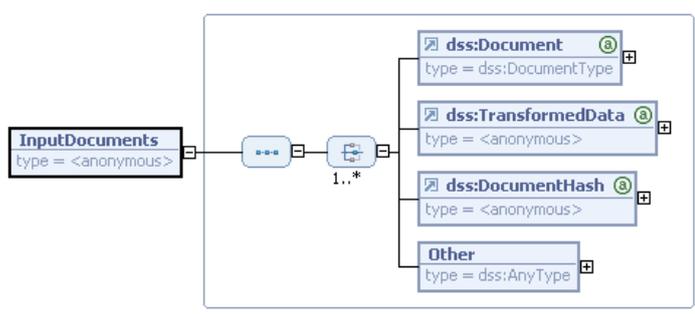
L'estructura bàsica dels missatges utilitzats per a fer peticions a la plataforma és la següent:

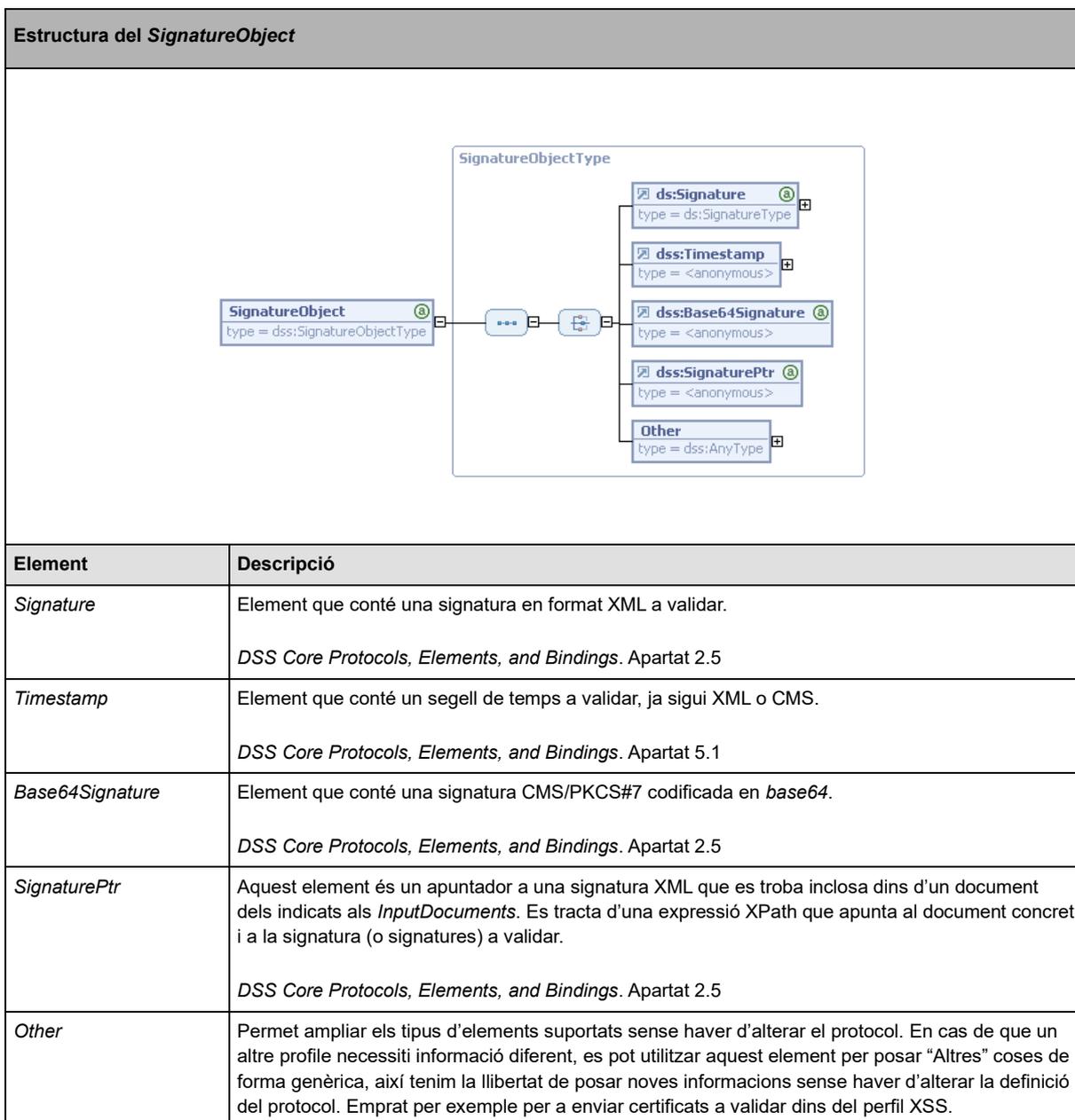


Estructura d'OptionalInputs



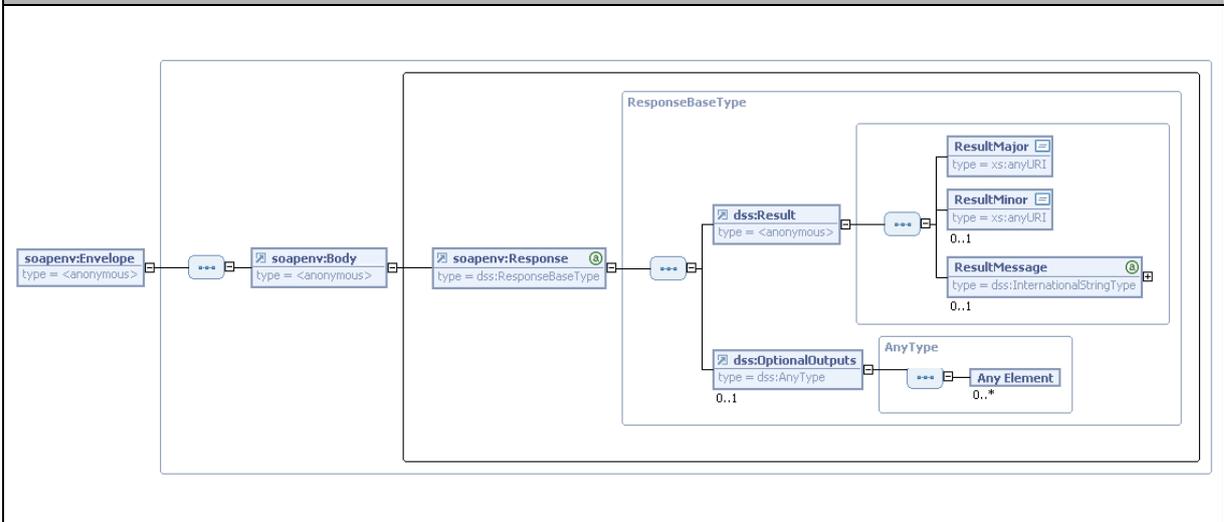
Element	Descripció
<i>OptionalInputs</i>	<p>Element que conté el conjunt de <i>OptionalInputs</i> que permetrà configurar l'execució de l'operació al servidor.</p> <p>Alguns dels <i>OptionalInputs</i> visibles a l'esquema adjuntat, s'exposen en aquest mateix document a l'apartat 5, separats per funcionalitat.</p> <p><i>DSS Core Protocols, Elements, and Bindings</i>. Apartat 2.4</p>

Estructura d' <i>InputDocuments</i>	
	
Element	Descripció
<i>Document</i>	<p>Aquest element contindrà un document a validar.</p> <p>Aquest document pot portar la signatura dins seu (signatura <i>attached enveloped</i>), o portar la signatura en el mateix missatge per separat (signatura <i>detached</i>) per a casos de validacions, o bé anar sol en cas d'estampació de segells de temps o creació de signatura.</p> <p><i>DSS Core Protocols, Elements, and Bindings</i>. Apartat 2.4</p>
<i>TransformedData</i>	<p>Aquest element conté un document sobre el qual s'ha efectuat algun tipus de transformació per part del client abans d'enviar-lo al servidor. Aquestes transformacions poden ser qualsevol de les estàndards definides com ara <i>c14n</i>, <i>c14nexcl</i>, <i>base64</i>... o bé alguna definida <i>adhoc</i>, però que haurà d'estar suportada pel servidor.</p> <p><i>DSS Core Protocols, Elements, and Bindings</i>. Apartat 2.4</p>
<i>DocumentHash</i>	<p>En aquest tipus d'elements trobem dades a les quals el client ja ha aplicat un resum criptogràfic amb la finalitat que el document no viatgi al servidor, ja sigui per causes de mida o privacitat del mateix.</p> <p><i>DSS Core Protocols, Elements, and Bindings</i>. Apartat 2.4</p>
<i>Other</i>	<p>Permet ampliar els tipus de documents suportats sense haver d'alterar el protocol. En cas de que un altre profile necessiti informació diferent, es pot utilitzar aquest element per posar "Altres" coses de forma genèrica, així tenim la llibertat de posar noves informacions sense haver d'alterar la definició del protocol.</p>



I les respostes de la plataforma PSIS, tenen la següent estructura:

Estructura del missatge de resposta



Element	Descripció								
<i>Result</i>	<p>Conté el resultat de la operació demanada pel client i vindrà informat sempre per a qualsevol operació. Els detalls sobre els diferents codis es poden trobar a l'apartat 5.</p> <p><i>DSS Core Protocols, Elements, and Bindings. Apartat 2.6</i></p> <table border="1"> <thead> <tr> <th>Element</th> <th>Descripció</th> </tr> </thead> <tbody> <tr> <td><i>ResultMajor</i></td> <td>Resultat de l'operació sense aportar detalls. És a dir, notifica si tot ha anat bé o hi ha hagut algun error, però no proporciona cap més informació.</td> </tr> <tr> <td><i>ResultMinor</i></td> <td>Resultat de l'operació o la causa de l'error, segons el cas.</td> </tr> <tr> <td><i>ResultMessage</i></td> <td>Opcionalment informa del resultat de forma textual.</td> </tr> </tbody> </table>	Element	Descripció	<i>ResultMajor</i>	Resultat de l'operació sense aportar detalls. És a dir, notifica si tot ha anat bé o hi ha hagut algun error, però no proporciona cap més informació.	<i>ResultMinor</i>	Resultat de l'operació o la causa de l'error, segons el cas.	<i>ResultMessage</i>	Opcionalment informa del resultat de forma textual.
Element	Descripció								
<i>ResultMajor</i>	Resultat de l'operació sense aportar detalls. És a dir, notifica si tot ha anat bé o hi ha hagut algun error, però no proporciona cap més informació.								
<i>ResultMinor</i>	Resultat de l'operació o la causa de l'error, segons el cas.								
<i>ResultMessage</i>	Opcionalment informa del resultat de forma textual.								
<i>OptionalOutputs</i>	<p>Informació generada pel processament dels elements <i>OptionalInputs</i> sol·licitats en la petició realitzada pel client. Tot i que aquest cas és l'habitual, el servidor pot decidir afegir a la resposta <i>OptionalOutputs</i> inclosos a la seva política de servei, tot i que el client no els hagi sol·licitat.</p> <p><i>DSS Core Protocols, Elements, and Bindings. Apartat 2.9</i></p>								

5. Funcionalitats

De totes les funcionalitats que permet la plataforma PSIS, aquest document es centra en les següents:

- Validació de certificats
- Validació de signatures en format PKCS#7 / CMS i XML
- Validació i completat de signatures XAdES / CAdES
- Validació i completat de documents PDF signats
- Creació i validació de segells de temps

Es descriu la missatgeria que intervé a les comunicacions entre els clients i el servidor de la plataforma PSIS per tal d'executar les funcionalitats esmentades.

Per a cada funcionalitat es detalla el missatge a enviar des del client (missatge d'entrada) i el missatge de resposta que generarà la plataforma PSIS un cop processada la sol·licitud (missatge de sortida). Per a cada missatge s'inclouran breus explicacions dels paràmetres i elements que es fan servir en cada cas, a més d'incloure un detall amb els paràmetres opcionals que es poden afegir.

Adicionalment s'inclou el procés de desenvolupament amb els llenguatges de programació Java, .NET (C#) i Visual Basic 6, per a poder arribar a construir el missatge d'entrada que s'acabarà enviant a la plataforma PSIS.

NOTA: Els exemples que s'han documentat únicament fan una funció de suport de les explicacions donades per a cada funcionalitat i les seves dades no son útils ja que s'han formatat per tal de ser més aclaridores.

NOTA: Totes les descripcions d'estructures / elements que formen part de la missatgeria DSS contenen el nom del document a on es pot trobar el detall de la descripció juntament amb possibles comentaris particulars de la plataforma PSIS.

5.1. Validació de certificats

Aquesta funcionalitat permet validar certificats X509, així com l'extracció d'informació dels certificats fent servir funcionalitats definides al perfil XSS.

Endpoints

- Entorn d'integració:
<https://psis-pre.aoc.cat/psis/catcert-test/dss>
- Entorn d'explotació:
<https://psis.aoc.cat/psis/catcert/dss>

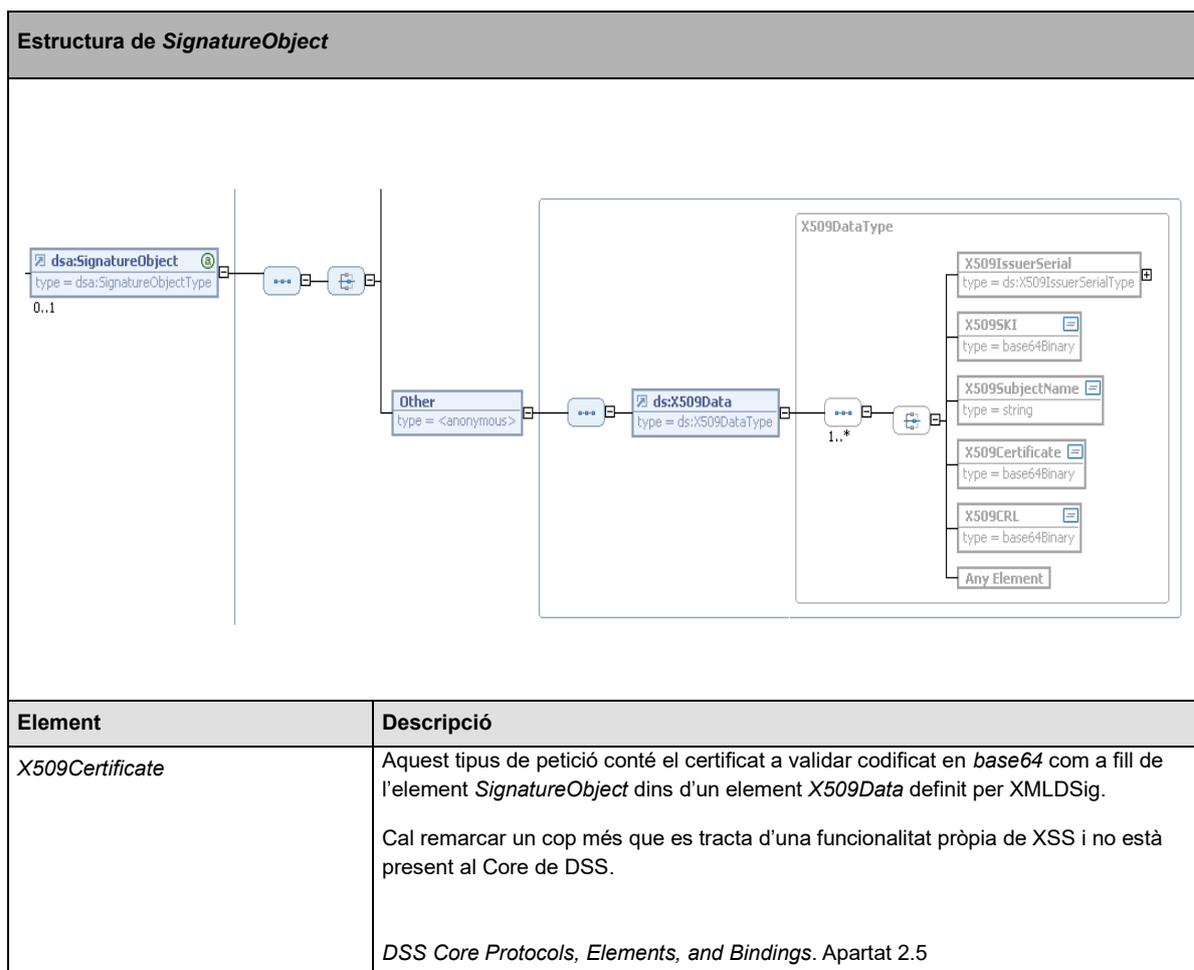
En el següent exemple, es descriu la missatgeria necessària per a poder sol·licitar al servidor la validació d'un certificat, així com d'altres funcionalitats addicionals a la mateixa:

Missatge d'entrada

Validació de certificat X509
<pre> <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"> <soapenv:Body> <dss:VerifyRequest Profile="urn:oasis:names:tc:dss:1.0:profiles:XSS" xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema" xmlns:xd="http://www.w3.org/2000/09/xmldsig#" xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"> <dss:OptionalInputs> <dss:ReturnProcessingDetails/> <xss:ReturnX509CertificateInfo> <xss:AttributeDesignator Name="urn:oasis:names:tc:dss:1.0:profiles:XSS:certificateAttributes:Version"/> <xss:AttributeDesignator Name="urn:oasis:names:tc:dss:1.0:profiles:XSS:certificateAttributes:SerialNumber"/> </xss:ReturnX509CertificateInfo> </dss:OptionalInputs> <dss:SignatureObject> <dss:Other> <xd:X509Data> <xd:X509Certificate> MIIHxTCCBq2gAwIBAgIQOiZLLU8OHRFCG0+XhWb/ ... 72e19BjFD6ELTFu018J0qjwM/m8ZlvGnkNvgN2paGWE3WALgZdhQDh6dWb2IYvECbMw6qjJAigi3Ii7GlhsX660x0Y 28TCBwGxkAxhwsMYv01At2YHlSXlYpxv1cnVI+a3dLECaRRER1Q8C16YuPGaA0CdryPlCCZkBKwAhMOuPFdxhV/Hj 9bLyUjgUQ=</xd:X509Certificate> </xd:X509Data> </dss:Other> </dss:SignatureObject> </dss:VerifyRequest> </soapenv:Body> </soapenv:Envelope> </pre>

Figura 4 Missatge de validació d'un certificat X509

El missatge d'entrada segueix l'estructura bàsica plantejada pel perfil XSS de l'estàndard DSS, aportant una sèrie de *OptionalInputs* (que comentem amb detall posteriorment) dins d'una *VerifyRequest*. El camp *SignatureObject* conté, en aquest cas, el certificat d'entitat final X509 a validar.



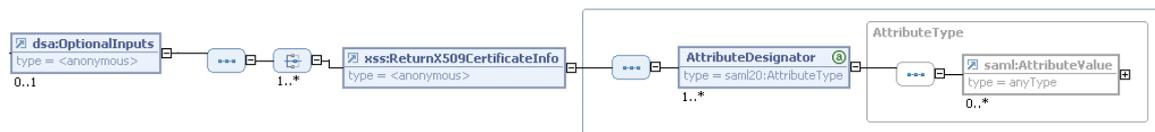
Dins d'aquest tipus de petició, el servidor permet realitzar operacions addicionals relacionades amb la pròpia validació i que s'invoquen mitjançant la inclusió d'una sèrie d'*OptionalInputs* que ara es detallen.

Estructura de ReturnProcessingDetails



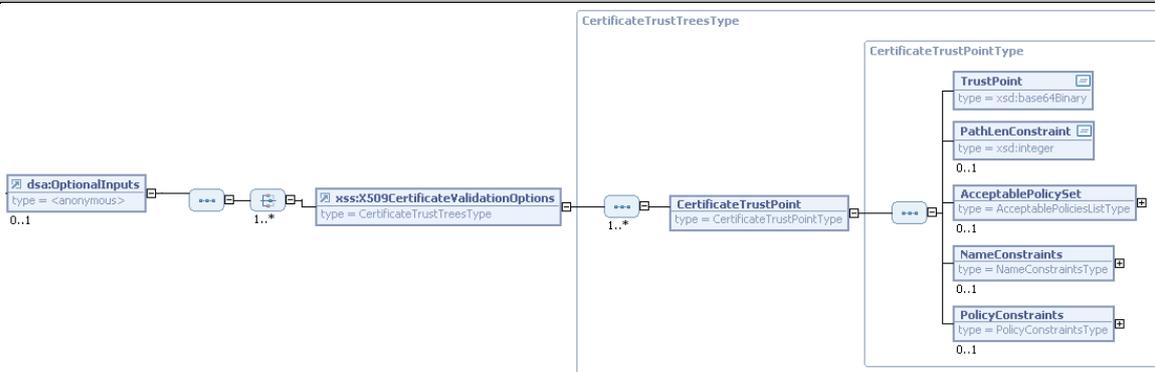
Element	Descripció
ReturnProcessingDetails	Sol·licitud de consulta per part de client d'informació detallada sobre el procés de validació. Així, l'usuari demana al servidor que doni detalls dels diferents passos que s'han dut a terme durant el procés de validació i que justifiquen el resultat retornat. DSS Core Protocols, Elements, and Bindings. Apartat 4.6.4

Estructura de ReturnX509CertificateInfo



Element	Descripció
ReturnX509CertificateInfo	Sol·licitud de consulta d'un atribut del certificat. Permet extreure informació del certificat proporcionat pel client. Es poden consultar 1 o N atributs en una mateixa consulta. Als annexes hi ha informació de tots els atributs de consulta disponibles. XSS Profile of the OASIS DSS. Apartat 3.1.5

Estructura de X509CertificateValidationOptions



Element	Descripció
<i>CertificateTrustPoint</i>	<p>Permet configurar amb molta precisió detalls de com el servidor realitzarà la validació del certificat. D'aquesta manera, es pot configurar les arrels de confiança per a la validació, la longitud del path de certificació i les restriccions de noms i polítiques de les CA's involucrades en el procés de validació.</p> <p>XSS Profile of the OASIS DSS. Apartat 5.1.4</p>

Estructura de <i>ReturnSignedResponse</i>	
Element	Descripció
<i>ReturnSignedResponse</i>	<p>Demana al servidor que retorni la resposta signada.</p> <p>XSS Profile of the OASIS DSS. Apartat 3.1.2</p>

Missatge de sortida

Reposta de la validació d'un certificat X509
<pre> <?xml version="1.0" encoding="UTF-8"?> <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"> <soapenv:Body> <dss:VerifyResponse Profile="urn:oasis:names:tc:dss:1.0:profiles:XSS" xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"> <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:certific ate:Definitive</dss:ResultMinor> </dss:Result> <dss:OptionalOutputs> <dss:ProcessingDetails> <dss:ValidDetail Type="urn:oasis:names:tc:dss:1.0:detail:ValidityInterval"> <dss:Message xml:lang="en">The signing key is inside its static validity interval.</dss:Message> </dss:ValidDetail> <dss:ValidDetail Type="urn:oasis:names:tc:dss:1.0:detail:IssuerTrust"> <dss:Message xml:lang="en">The issuer of the given key is trusted.</dss:Message> </dss:ValidDetail> <dss:ValidDetail Type="urn:oasis:names:tc:dss:1.0:detail:RevocationStatus"> </pre>

```

                                <dss:Message xml:lang="en">The signing key is
not revoked.</dss:Message>
                                </dss:ValidDetail>
                                </dss:ProcessingDetails>
                                <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
xmlns:urn1="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:integer">3</urn1:AttributeValue>
                                </urn:Attribute>
                                <urn:Attribute
Name="urn:oasis:names:tc:dss:1.0:profiles:XSS:certificateAttributes:SerialNumber">
                                <urn1:AttributeValue
xmlns:urn1="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:integer"
>77294064046332314987328417165725401088</urn1:AttributeValue>
                                </urn:Attribute>
                                </urn:X509CertificateInfo>
                                </dss:OptionalOutputs>
                                </dss:VerifyResponse>
                                </soapenv:Body>
</soapenv:Envelope>

```

Figura 5 Missatge resposta d'una validació d'un certificat X509

El missatge de sortida segueix l'estructura bàsica plantejada per l'estàndard DSS.

Els elements continguts a la resposta de la validació de certificat són:

- **Result**

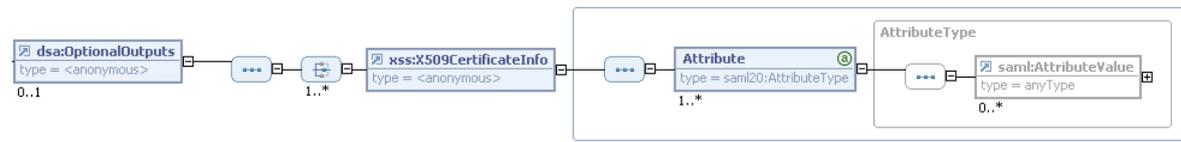
Estructura de dades amb el resultat del procés de validació. Com segueix el format DSS conté un major i un minor. Ambdós es troben detallats a l'annex corresponent i a la secció relativa als resultats de validació de certificats del perfil XSS.

- **OptionalOutputs**

Estructura de dades que contindrà la informació sol·licitada pel client als elements introduïts dins de l'estructura <OptionalInputs>.

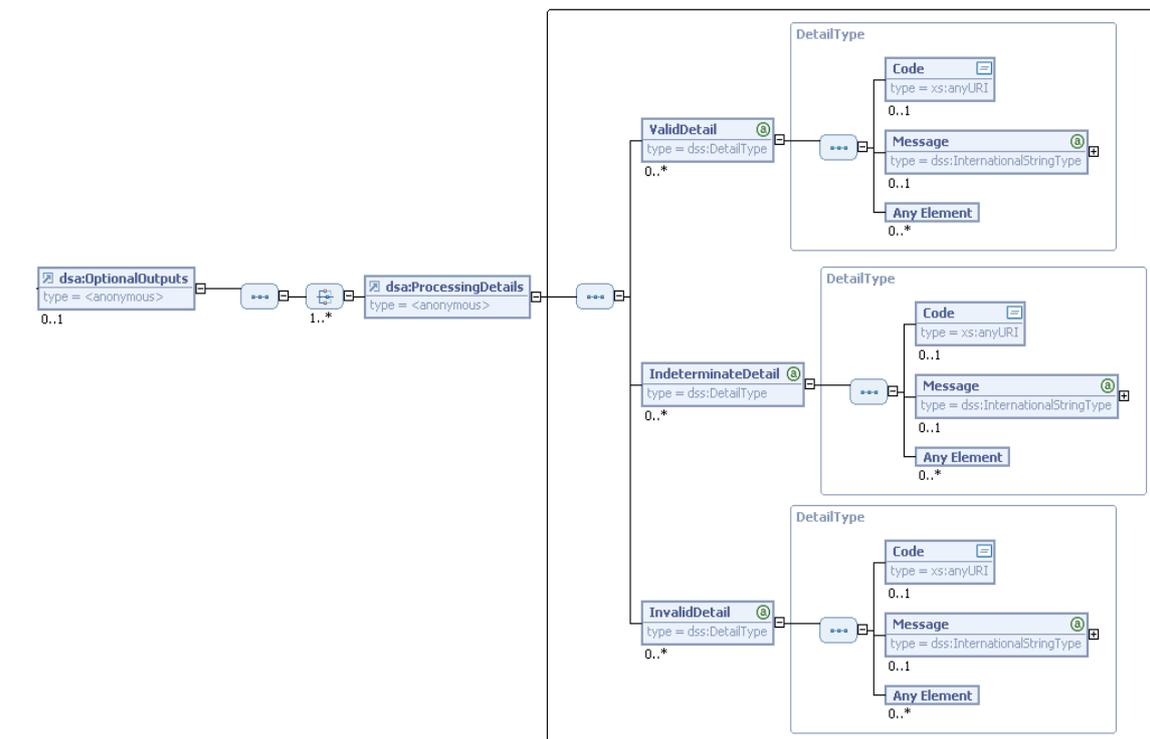
Es podran rebre els elements:

Estructura de *X509CertificateInfo*

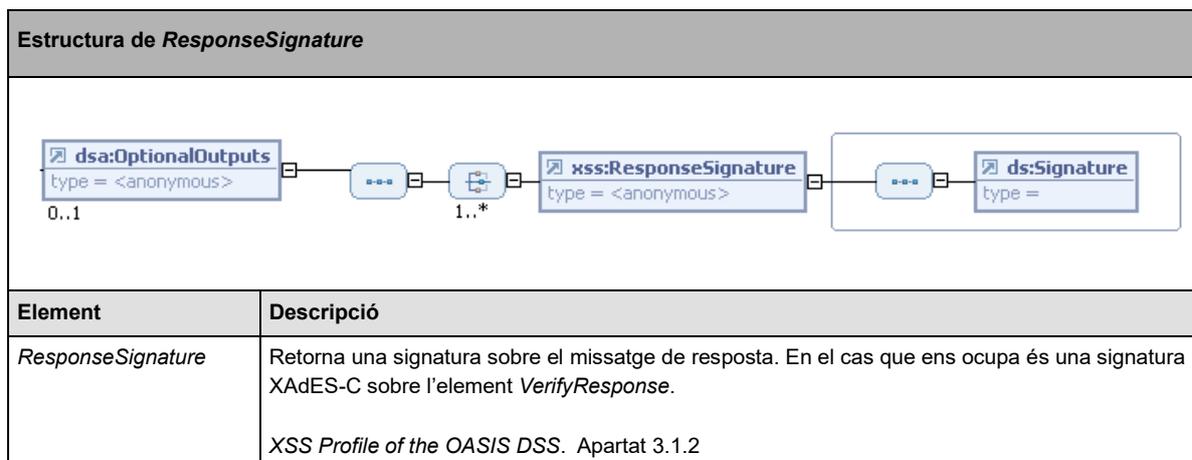


Element	Descripció
<i>X509CertificateInfo</i>	<p>Resposta amb informació dels atributs del certificat sol·licitats en la petició de validació.</p> <p>Es poden rebre 1 o N atributs en una mateixa consulta. En els annexes hi ha informació de tots els atributs de consulta disponibles.</p> <p>Resposta obtinguda per l'enviament de la sol·licitud <i>ReturnX509CertificateInfo</i>.</p> <p><i>XSS Profile of the OASIS DSS</i>. Apartat 3.1.5</p>

Estructura de *ProcessingDetails*



Element	Descripció
<i>ProcessingDetails</i>	<p>Informació detallada del procés de validació.</p> <p>Resposta obtinguda per l'enviament de la sol·licitud <i>ReturnProcessingDetails</i>.</p> <p><i>DSS Core Protocols, Elements and Bindings</i>. Apartat 4.6.4</p>



5.2. Validació de signatures en format PKCS#7 / CMS i XML

Aquesta funcionalitat permet la validació de signatures simples, aquelles que no són enteses en terminologia PKI com a signatures complexes.

Dins el que considerem com a signatures simples, es pot fer una primera classificació en signatures PCKS#7 / CMS (*Cryptographic Message Syntax*) i signatures XML o XMLDSig.

CMS és una ampliació del format PCKS#7, per la qual cosa quan es faci referència a PCKS#7 podem assumir que es tracta del format CMS.

Ambdós sistemes defineixen dues modalitats per a signatures: *Detached* i *Attached*.

El format *Detached* significa que el contingut signat no és present dins de la signatura i ha de ser transmès per altres vies. Així doncs, és el mètode més simple, donat que la signatura únicament conté el resum criptogràfic (*digest*) del contingut signat i no el contingut íntegre.

El format *Attached* implica que el contingut signat es troba dins de la signatura. Ara bé, en el cas XMLDSig trobem dues modalitats: *Enveloping* i *Enveloped*. En el primer cas, les dades signades es troben com a referència dins la signatura, mentre que en el segon cas la signatura forma part del document (com a nus XML), la qual cosa implica que els algorismes de càlcul de signatura han d'ignorar el valor del camp de signatura en els càlculs sobre el document.

Així doncs, els clients hauran de construir diferents missatges depenent de la tipologia de la signatura que vulguin validar. Els detalls de les diferents tipologies, així com els elements DSS que es fan servir en els mateixes, estan detallats a DSS, realitzant-se en aquest document una breu menció aclarativa.

Endpoints

- Entorn d'integració:
<https://psis-pre.aoc.cat/psis/catcert-test/dss>
- Entorn d'explotació:
<https://psis.aoc.cat/psis/catcert/dss>

En els següents exemples es descriu la missatgeria:

Missatge d'entrada

Missatge per a la validació d'una signatura **CMS attached**. En aquest cas, no existeix cap document, donat que el document signat va dins de la signatura i només proveïm d'un *SignatureObject* que conté una signatura binària codificada en *Base64*.

```
Validació de signatura CMS attached

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <!-- DSS message validating a correct CMS -->
    <!-- Result: Valid -->
    <dss:VerifyRequest xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
      <dss:OptionalInputs>
        <dss:ReturnProcessingDetails/>
      </dss:OptionalInputs>
      <dss:SignatureObject>
        <dss:Base64Signature Type="urn:ietf:rfc:3369">
          .../66L1XkDrd81Nk7OFR6jdu5YL2g1oUQXBBRtCohbH5kTAS25CtBYFHYfN/Md6gzkdwX1+54gGHYH/mHq
          b8My+nAH/oOfbINBncnG0i5RfsvBuLymrh1YnUiEo01zd5VNSgC1QBfH6k3BOM5YC69znLmD0a8XsY3etywad8ylUA
          AAAAAAA</dss:Base64Signature>
        </dss:SignatureObject>
      </dss:VerifyRequest>
    </soapenv:Body>
  </soapenv:Envelope>
```

Figura 6 Missatge de validació de signatura CMS attached

Missatge per a la validació d'una signatura **CMS detached**. En aquest supòsit, existeix un document que proveïm a *InputDocuments*, i la signatura la proveïm dins un *SignatureObject* que conté dita signatura binària codificada en *Base64*. El document adjuntat en aquest cas pot ser el document en sí codificat en *Base64* o bé el seu resum criptogràfic, tal i com disposa DSS.

Validació de signatura CMS detached

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <!-- DSS message validating a correct CMS -->
    <!-- Result: Valid -->
    <dss:VerifyRequest xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
      <dss:OptionalInputs>
        <dss:ReturnProcessingDetails/>
      </dss:OptionalInputs>
      <dss:InputDocuments>
        <dss:Document>
          <dss:Base64Data>YWFhYWFhYWFh</dss:Base64Data>
        </dss:Document>
      </dss:InputDocuments>
      <dss:SignatureObject>
        <dss:Base64Signature Type="urn:ietf:rfc:3369">
          .../66L1XkDrd81Nk7OFR6jdu5YL2g1oUQXBBRtCohbH5kTAS25CtBYFHYfN/Md6gzkdwX1+54gGHYH/mHq
          b8My+nAH/oOfbINBncnG0i5RfsvBuLymrhlYnUiEo01zd5VNSgC1QBfH6k3BOM5YC69znLmD0a8XsY3etywaD8ylUA
          AAAAAAA </dss:Base64Signature>
        </dss:SignatureObject>
      </dss:VerifyRequest>
    </soapenv:Body>
  </soapenv:Envelope>
```

Figura 7 Missatge de validació de signatura CMS detached

Missatge per a la validació d'una signatura **XML attached enveloping**, en la que, com es pot veure, el contingut a signar ha estat inclòs en el node amb *Id*="Object" de la mateixa. La signatura es proveeix dins del *SignatureObject* com a una signatura XMLDSig.

Validació de signatura XML attached enveloping

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <dss:VerifyRequest Profile="urn:oasis:names:tc:dss:1.0:profiles:XSS"
      xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
      <dss:OptionalInputs>
        <dss:ReturnProcessingDetails/>
      </dss:OptionalInputs>
      <dss:SignatureObject>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
            <ds:CanonicalizationMethod
              Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
            <ds:SignatureMethod
              Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#Object">
              <ds:Transforms>
                <ds:Transform
                  Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/><ds:Transform
                  Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/></ds:Transforms>
```

```

                                <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><ds:DigestValue>
8sEMF3ipDgNdjPoShP51Hbgly4k </ds:DigestValue>
                                </ds:Reference>
                                </ds:SignedInfo>
                                <ds:SignatureValue> a/kmv5..... </ds:SignatureValue>
                                <ds:KeyInfo>
                                <ds:KeyValue>
                                <ds:RSAKeyValue>
                                <ds:Modulus> uY17h.....
</ds:Modulus>
                                <ds:Exponent>AQAB</ds:Exponent>
                                </ds:RSAKeyValue>
                                </ds:KeyValue>
                                <ds:X509Data>
                                <ds:X509Certificate> MIH...
</ds:X509Certificate>
                                </ds:X509Data>
                                </ds:KeyInfo>
                                <ds:Object Id="Object">
                                <a><b>.....</b></a>
                                </ds:Object>
                                </ds:Signature>
                                </dss:SignatureObject>
                                </dss:VerifyRequest>
                                </soapenv:Body>
</soapenv:Envelope>

```

Figura 8 Missatge de validació de signatura XML attached enveloping

Missatge per a la validació d'una signatura **XML attached enveloped**, on la signatura està continguda dins del document signat.

Adicionalment, es pot proveir dins del *SignatureObject* un punter o **SignaturePtr** a la signatura que es troba dins del document, especificant l'identificador del document. Per a més detalls sobre aquest tema, es pot consultar l'apartat sobre el *SignaturePtr* del document *DSS Core*.

Validació de signatura XML attached enveloped

```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <urn:VerifyRequest
      Profile="urn:oasis:names:tc:dss:1.0:profiles:XSS"
      xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"
      xmlns:urn="urn:oasis:names:tc:dss:1.0:core:schema"
      xmlns:xsp="http://uri.etsi.org/2038/v1.1.1#"
      xmlns:xd="http://www.w3.org/2000/09/xmldsig#"
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
      <urn:OptionalInputs>
        <urn:ReturnProcessingDetails/>
      </urn:OptionalInputs>
      <urn:InputDocuments>
        <urn:Document ID="doc" RefURI="">

```

```

<urn:InlineXML><a><b><ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="id-1795ea06-d2ec-4dd0-8b67-
05f9e47fa6de">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"></ds:CanonicalizationMethod>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"></ds:SignatureMethod>
<ds:Reference URI="">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
<ds:DigestValue>630+0/BNGDxKudkxe5SUmEjFRmE=</ds:DigestValue>
</ds:Reference>
<ds:Reference Type="http://uri.etsi.org/01903/v1.2.2#SignedProperties" URI="#id-92759a28-
aff4-4567-96f2-9d534d156592">
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
<ds:DigestValue>QTpnCN3iXDOXa6pw6jyOALtgFYg=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
TnUs37pGeU43rONYqW9LgtEcmLvDH//ALUpCJpVlDyEy5uFRgoMV5UK6xg99dNCYEvK9Rf3Ho9R0
017prbL6xwWsPnW7iO1GPDkxWGFSS2J6+hdQLRVoDulIluX5Lw/09Fb0LtyUVhdAyBFjaWWzHTvV
MQQfgvtQQavwqJbQ9cM=
</ds:SignatureValue>
<ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIIHfjCCBmagAwIBAgIQJHlaK1NuFEBD0L+
...QfTY/vJJkcyKxDNug6h0WRMA8A33sR3frMChUUPwF3pWB7YX8yLejdC6681rUkTHkPMvDi0rmaeK0BX/t7+nIi
tdYZZ+Jz1NRctE=</ds:X509Certificate></ds:X509Data><ds:KeyValue><ds:RSAKeyValue><ds:Modulus
>AK4+XKbPxINVvVyYall60uLvrZHJS0mdjkbRRsSdc8W0XbjSnx3BUsRv8H4I68GXHD2SNuc2HjFRGCnK2pInVi95
VDEfACTkuTF8iyVpplAk3GqaN34wBCUC1Nu93ALlmNd0VDUQ8ZUhb1K7MJ/LU47YNhs8sJRGHct4yk/m0YZ</ds:Mo
dulus><ds:Exponent>AQAB</ds:Exponent></ds:RSAKeyValue></ds:KeyValue><ds:KeyInfo><ds:Objec
t><xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.2.2#" Target="#id-
1795ea06-d2ec-4dd0-8b67-05f9e47fa6de"><xades:SignedProperties Id="id-92759a28-aff4-4567-
96f2-
9d534d156592"><xades:SignedSignatureProperties><xades:SigningCertificate><xades:Cert><xade
s:CertDigest><ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod><ds:DigestValue>/O+sU
Urdp+pwvhlslJkCOC2zlnw=</ds:DigestValue></xades:CertDigest><xades:IssuerSerial><ds:X509Iss
uerName>CN=EC-SAFP,OU=Secretaria d'Administració i Funció Pública,OU=Vegeu
https://www.catcert.net/verCIC-2 (c)03,OU=Serveis Publics de Certificació ECV-
2,L=Passatge de la Concepció 11 08008 Barcelona,O=Agència Catalana de Certificació (NIF Q-
0801176-
I),C=ES</ds:X509IssuerName><ds:X509SerialNumber>48482304617635335619431060243083832167</ds
:X509SerialNumber></xades:IssuerSerial></xades:Cert></xades:SigningCertificate></xades:Sig
nedSignatureProperties></xades:SignedProperties></xades:QualifyingProperties></ds:Objec
t></ds:Signature></b></a></urn:InlineXML>
</urn:Document>
</urn:InputDocuments>
<urn:SignatureObject>
<urn:SignaturePtr WhichDocument="doc"/>
</urn:SignatureObject>
</urn:VerifyRequest>
</soapenv:Body>
</soapenv:Envelope>

```

Figura 9 Missatge de validació de signatura XML attached enveloped

Missatge per a la validació d'una signatura **XML detached**, on cal proveir tant la signatura com els documents signats de forma separada. La signatura es proveeix dins de l'element *SignatureObject*, com en el cas enveloping, mentre que el document es proveeix dins de l'element *InputDocuments*.

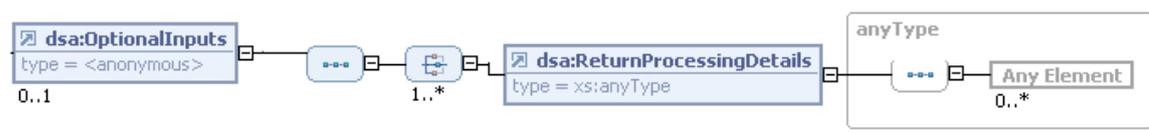
```

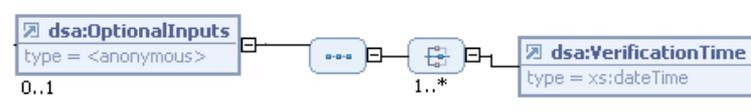
Validació de signatura XML detached
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <dss:VerifyRequest Profile="urn:oasis:names:tc:dss:1.0:profiles:XSS"
      xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
      <dss:OptionalInputs>
        <dss:ReturnProcessingDetails/>
      </dss:OptionalInputs>
      <dss:InputDocuments>
        <dss:Document ID="doc" RefURI="mydoc.catcert.net">
          <dss:InlineXML><a><b>.....</b></a></dss:InlineXML>
        </dss:Document>
      </dss:InputDocuments>
      <dss:SignatureObject>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
            <ds:CanonicalizationMethod
              Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
            <ds:SignatureMethod
              Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="mydoc.catcert.net">
              <ds:Transforms>
                <ds:Transform
                  Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                <ds:Transform
                  Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
              </ds:Transforms>
            <ds:DigestMethod
              Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>
              8sEMF3ipDgNdjPoShP51Hbgly4k </ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue> a/kmv5..... </ds:SignatureValue>
          <ds:KeyInfo>
            <ds:KeyValue>
              <ds:RSAKeyValue>
                <ds:Modulus> uY17h.....
              </ds:Modulus>
                <ds:Exponent>AQAB</ds:Exponent>
              </ds:RSAKeyValue>
            </ds:KeyValue>
            <ds:X509Data>
              <ds:X509Certificate> MIH...
            </ds:X509Certificate>
          </ds:KeyInfo>
        </ds:Signature>
      </dss:SignatureObject>
    </dss:VerifyRequest>
  </soapenv:Body>
</soapenv:Envelope>

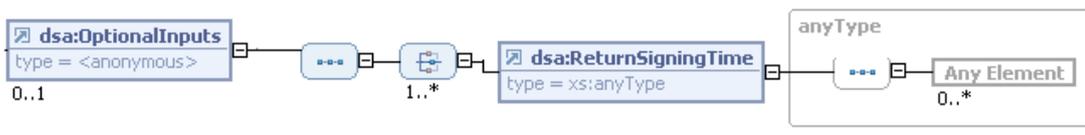
```

Figura 10 Missatge de validació de signatura XML detached

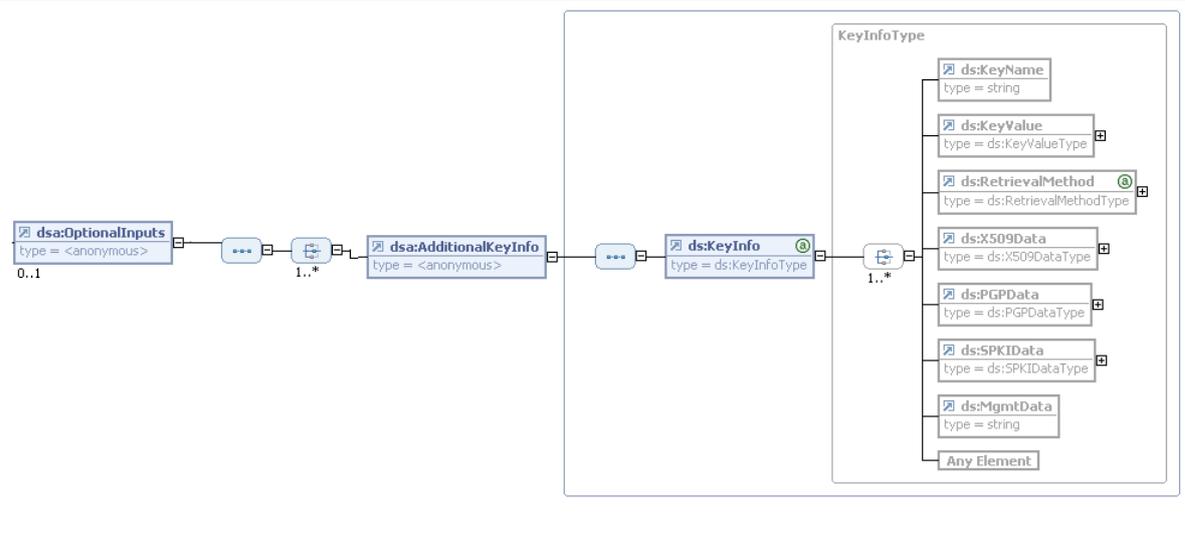
A més, de manera idèntica a la resta de peticions basades en DSS conté una sèrie de *OptionalInputs* que procedim a detallar:

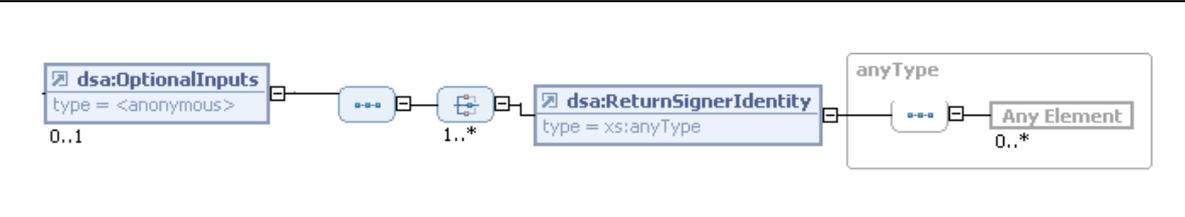
Estructura de <i>ReturnProcessingDetails</i>	
	
Element	Descripció
<i>ReturnProcessingDetails</i>	<p>Molt similar al seu homònim ja tractat amb anterioritat a la validació de certificats, però en aquest cas proporciona detalls sobre la validació de la signatura en sí, a més dels referits a l'estat del certificat amb el qual es va realitzar la signatura.</p> <p><i>DSS Core Protocols, Elements and Bindings. Apartat 4.6.4</i></p>

Estructura de <i>VerificationTime</i>	
	
Element	Descripció
<i>VerificationTime</i>	<p>Proporciona un instant de temps al·legat per a la validació de la signatura. Si no es proporciona cap, l'instant de validació per a aquest tipus de signatures serà l'actual.</p> <p><i>DSS Core Protocols, Elements and Bindings. Apartat 4.6.2</i></p>

Estructura de <i>ReturnSigningTime</i>	
	
Element	Descripció
<i>ReturnSigningTime</i>	<p>Demana al servidor que retorni la data en la qual es va dur a terme la signatura, si és possible determinar-la a partir de la mateixa.</p>

	<p>La utilització d'aquest element generarà la creació de l'element <i>SigningTime</i> dins de l'estructura <i>OptionalOutputs</i>.</p> <p><i>DSS Core Protocols, Elements and Bindings. Apartat 4.6.5</i></p>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Estructura de <i>AdditionalKeyInfo</i>	
	
Element	Descripció
<i>AdditionalKeyInfo</i>	<p>Proporciona al servidor informació addicional útil en el procés de validació com ara CA's intermitjies o CRL's necessàries per tal de poder validar la signatura.</p> <p><i>DSS Core Protocols, Elements and Bindings. Apartat 4.6.3</i></p>

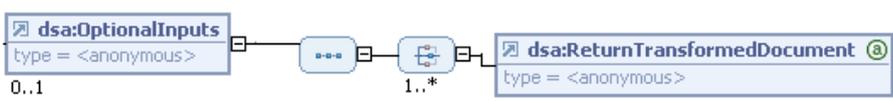
Estructura de <i>ReturnSignerIdentity</i>	
	
Element	Descripció
<i>ReturnSignerIdentity</i>	<p>Demana al servidor que retorni la identitat del creador de la signatura.</p> <p>La utilització d'aquest element generarà la creació de l'element <i>SignerIdentity</i> dins de l'estructura <i>OptionalOutputs</i>.</p> <p><i>DSS Core Protocols, Elements and Bindings. Apartat 4.6.6</i></p>

Estructura de <i>ReturnSignatureInfo</i>	
Element	Descripció
<i>ReturnSignatureInfo</i>	<p>Sol·licitud de consulta d'atributs de la signatura o del seu certificat.</p> <p>La utilització d'aquest element passa per crear, per cada atribut, un nou element fill de tipus <i>AttributeDesignator</i> que contindrà un atribut amb el nom de "Name" i que agafarà el nom de l'atribut a consultar.</p> <p>Es poden demanar 1 o N atributs en una mateixa consulta. En els annexes hi ha informació de tots els atributs de consulta disponibles.</p> <p>XSS Profile of the OASIS DSS. Apartat 3.1.4</p>

Estructura de <i>ReturnSignedResponse</i>	
Element	Descripció
<i>ReturnSignedResponse</i>	<p>Demana al servidor que retorni la resposta signada.</p> <p>XSS Profile of the OASIS DSS. Apartat 3.1.2</p>

Estructura de <i>RequireQualifiedCertificate</i>	
Element	Descripció
<i>RequireQualifiedCertificate</i>	<p>Indica al servidor que verifiqui que el certificat que es farà servir per a verificar la signatura és un certificat correcte (d'acord amb la normativa de <i>EC Directive On Electronic Signatures</i>).</p> <p>La utilització d'aquest element no genera cap sortida dins de l'estructura <i>OptionalOutputs</i>.</p> <p>XSS Profile of the OASIS DSS. Apartat 5.1.6</p>

També podem trobar OptionalInputs exclusius per a signatures del tipus XML.

Estructura de <i>ReturnTransformedDocument</i>	
	
Element	Descripció
<i>ReturnTransformedDocument</i>	<p>Indica al servidor que ha de retornar en la resposta el document transformat sota una referència particular.</p> <p>La utilització d'aquest element generarà la creació de l'element <i>TransformedDocument</i> dins de l'estructura <i>OptionalOutputs</i>.</p> <p><i>DSS Core Protocols, Elements, and Bindings</i>. Apartat 4.6.8</p>

Estructura de <i>VerifyManifests</i>	
	
Element	Descripció
<i>VerifyManifests</i>	<p>Indica al servidor que ha de verificar els "Manifest" de la signatura.</p> <p>La utilització d'aquest element generarà la creació de l'element <i>VerifyManifestResults</i> dins de l'estructura <i>OptionalOutputs</i>.</p> <p>La implementació actual de la plataforma PSIS no dona suport a aquest element.</p> <p><i>DSS Core Protocols, Elements, and Bindings</i>. Apartat 4.6.1</p>

Missatge de sortida

Missatge de sortida per a una validació de signatura

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <dss:VerifyResponse Profile="urn:oasis:names:tc:dss:1.0:core:schema">
```

```

        xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
        <dss:Result>
            <dss:ResultMajor>
urn:oasis:names:tc:dss:1.0:resultmajor:Success </dss:ResultMajor>
            <dss:ResultMinor>
                urn:oasis:names:tc:dss:1.0:resultminor:valid:signature:onAllDocuments
            </dss:ResultMinor>
        </dss:Result>
        <dss:OptionalOutputs>
            <dss:ProcessingDetails>
                <dss:ValidDetail
Type="urn:oasis:names:tc:dss:1.0:detail:Signature">
                    <dss:Message xml:lang="en"> The signature is
valid. </dss:Message>
                    </dss:ValidDetail>
                </dss:ProcessingDetails>
            </dss:OptionalOutputs>
        </dss:VerifyResponse>
    </soapenv:Body>
</soapenv:Envelope>

```

Figura 11 Missatge de sortida per a una validació de signatura

El missatge de sortida segueix l'estructura bàsica plantejada per l'estàndard DSS.

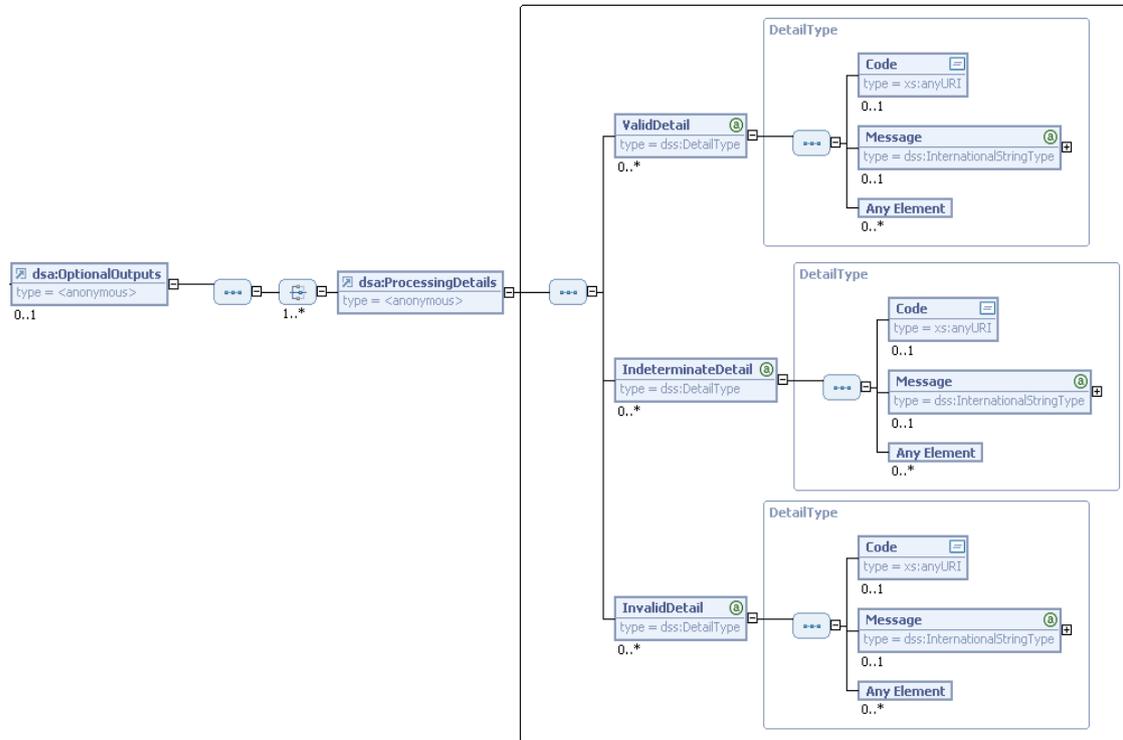
Els elements més importants continguts a la resposta d'una validació de signatura són:

- *Result*

Estructura de dades amb el resultat del procés de validació seguint l'estructura definida a DSS.
- *OptionalOutputs*

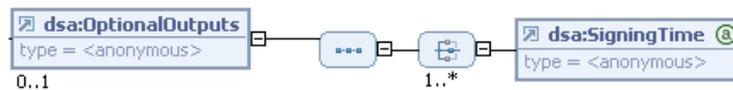
Estructura de dades que contindrà la informació sol·licitada pel client amb els elements introduïts dins de l'estructura *OptionalInputs*.

Estructura de *ProcessingDetails*



Element	Descripció
<i>ProcessingDetails</i>	<p>Informació detallada del procés de validació.</p> <p>Resposta obtinguda per l'enviament de la sol·licitud <i>ReturnProcessingDetails</i>.</p> <p><i>DSS Core Protocols, Elements, and Bindings</i>. Apartat 4.6.4</p>

Estructura de *SigningTime*



Element	Descripció
<i>SigningTime</i>	<p>Retorna el temps al·legat de signatura si aquest es troba present a la mateixa.</p> <p><i>DSS Core Protocols, Elements, and Bindings</i>. Apartat 4.6.5</p>

Estructura de <i>SignerIdentity</i>	
Element	Descripció
<i>SignerIdentity</i>	<p>Retorna la identitat del creador de la signatura.</p> <p><i>DSS Core Protocols, Elements, and Bindings. Apartat 4.6.6</i></p>

Estructura de <i>SignatureInfo</i>	
Element	Descripció
<i>SignatureInfo</i>	<p>Retorna la informació extreta de la signatura o del seu certificat a partir del demanat a l'<i>OptionalInput ReturnSignatureInfo</i></p> <p><i>XSS Profile of the OASIS DSS. Apartat 3.1.4</i></p>

Estructura de <i>ResponseSignature</i>	
Element	Descripció
<i>ResponseSignature</i>	<p>Retorna una signatura sobre el missatge de resposta. En el cas que ens ocupa és una signatura XAdES-C sobre la <i>VerifyResponse</i></p> <p><i>XSS Profile of the OASIS DSS. Apartat 3.1.2</i></p>

OptionalOutputs exclusius per a signatures XML:

Estructura de <i>TransformedDocument</i>	
Element	Descripció
<i>TransformedDocument</i>	<p>Retorna el document apuntat per la referència indicada per l'<i>OptionalInput</i>.</p> <p>El document transformat és el resultat d'aplicar totes les transformacions indicades a la signatura sobre el mateix.</p> <p><i>DSS Core Protocols, Elements, and Bindings. Apartat 4.6.8</i></p>

Estructura de <i>VerifyManifestResults</i>	
Element	Descripció
<i>ManifestResult</i>	<p>Retorna el resultat de verificar els elements <i>Manifest</i> presents a la signatura XML.</p> <p>La implementació actual de la plataforma PSIS no pot generar aquesta sortida perquè no dóna suport a la seva petició.</p> <p><i>DSS Core Protocols, Elements, and Bindings. Apartat 4.6.1</i></p>

5.3. Validació de signatures XAdES

Les signatures avançades estan dotades d'informació addicional i més robustesa enfront les signatures simples. XAdES i CAdES són els formats avançats de les signatures XMLDSig i CMS respectivament.

Aquestes signatures poden arribar a contenir informació de referències al certificat del signant, referències a la cadena de certificació i a la informació de revocació de la mateixa, o fins i tot aquesta informació en sí. A banda d'això, la signatura i la seva informació estan protegides per segells de temps per dotar a la signatura d'instant de creació certificat, vigència durant el temps i protecció enfront de la majoria d'atacs criptogràfics fins i tot contra les CA's emissores dels certificats implicats.

Per a més informació sobre aquests tipus de signatura, es poden consultar els documents ETSI TS 101 903 V1.3.2 de *XML Advanced Electronic Signatures (XAdES)* i ETSI TS 101 733 de *CMS Advanced Electronic Signatures (CAdES)*.

En aquest apartat s'estudiarà la validació de signatures XAdES. El format dels missatges de petició és el mateix que l'utilitzat per a les signatures XML i tots els aspectes relatius a la tipologia de la signatura respecte als elements signats és idèntica. Només trobem diferència en que les signatures XAdES disposen de *OptionalInputs/Outputs* no disponibles per a les signatures XMLDSig.

En el cas de les signatures CAdES, el format dels missatges de petició és el mateix que l'utilitzat per a les signatures CMS. Els *OptionalInputs/Outputs* que apliquen a les signatures CAdES són els mateixos que els de les signatures XAdES.

Endpoints

- Entorn d'integració:
<https://psis-pre.aoc.cat/psis/catcert-test/dss>
- Entorn d'explotació:
<https://psis.aoc.cat/psis/catcert/dss>

Missatge d'entrada

En aquest missatge mostrem una petició de validació d'una signatura *XAdES attached enveloped*. Podem observar que el missatge es idèntic al cas XMLDSig i només varia la forma de la signatura en sí.

Validació d'una signature XAdES enveloped

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <urn:VerifyRequest Profile="urn:oasis:names:tc:dss:1.0:profiles:XSS"
      xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"
      xmlns:urn="urn:oasis:names:tc:dss:1.0:core:schema"
      xmlns:xsp="http://uri.etsi.org/2038/v1.1.1#"
      xmlns:xd="http://www.w3.org/2000/09/xmldsig#"
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
      <urn:OptionalInputs>
        <urn:ReturnProcessingDetails/>
      </urn:OptionalInputs>
      <urn:InputDocuments>
        <urn:Document ID="docId" RefURI="">
          <urn:InlineXML><doc>
            <title>Proves</title>
            <body>Document de proves</body>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature">
              <ds:SignedInfo Id="SignedInfo">
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"></ds:CanonicalizationMethod>
                <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>
                <ds:Reference Id="SignedDataObject-enveloped" URI="">
                  <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"></ds:Transform>
                    <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"></ds:Transform>
                  </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
                <ds:DigestValue>/yjKqIr/J4PjFbNY5eNNgpBOVeY=</ds:DigestValue>
              </ds:Reference>
                <ds:Reference Id="SignedProperties-Reference"
                  Type="http://uri.etsi.org/01903/v1.2.2#SignedProperties" URI="#SignedProperties">
                  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
                  <ds:DigestValue>vk5AnJsa6M86VWgswL4HFyWzUU4=</ds:DigestValue>
                </ds:Reference>
              </ds:SignedInfo>
              <ds:SignatureValue Id="DocumentSignatureValue">
                dCg1R3xq+tx9uZOz0i4HJUUFcyxjzD8A8lmsTjg/i5YW/EFfUHvL9Tc/pYJQpebc8j3h5r1lgbOMa
                mHf7a4FO8aP/wckWT6TPikcvapnHQWSgLI8C3hB4rH0CwdfKPtTALPWLb39vxxMkbEwXHB1wf3XW
                VAEU2UfbRHS2S6fPIjCaGmP68sWUqRMEq19D00AtAyXx5K+KpVb287A1fUV7B18W51W4CCsQcyUr
                zclJpyhyphk0pQYmtfLaj1n2x+t/u//ZWhOcTZljkJbgBgh9SiOz5FqzJDKS0k+umO2Emt8tVvmwZ
                oz56rBX8Kv21o+tZFPLOwcdCcyZ9qS0ZCz/lkA==
              </ds:SignatureValue>
              <ds:KeyInfo Id="KeyInfo">
                <ds:X509Data>
                  <ds:X509Certificate>
                    MIIFLjCCBLSgAwIBAgIUdx.....
                  </ds:X509Certificate>
                </ds:X509Data>
                <ds:KeyValue>
                  <ds:RSAKeyValue>
                    <ds:Modulus>
                      1tAfAPcZdx7SKD3Y1kl+eQQNd/OxqCLFtm/uMsEaSpvsua3Ym4xK+gD1X4ksYB7kF9htgzcjFEip
                      okDJ+14Bbo6/A6Fy4YGN26eEkiidtc0FXt9q5EAv1k4Icbepoc6Q011T1D31ZCg7WJQOnXQtrsJq
                      /dj783WBa029691UPyLLI6KJrIaF3LbdyfEakaZKteORR5Tb0U0rjJ+C5azJmCNFN3J4Stj0gj7
                    </ds:Modulus>
                  </ds:RSAKeyValue>
                </ds:KeyValue>
              </ds:KeyInfo>
            </ds:Signature>
          </ds:Document>
        </urn:Document>
      </urn:InputDocuments>
    </urn:VerifyRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

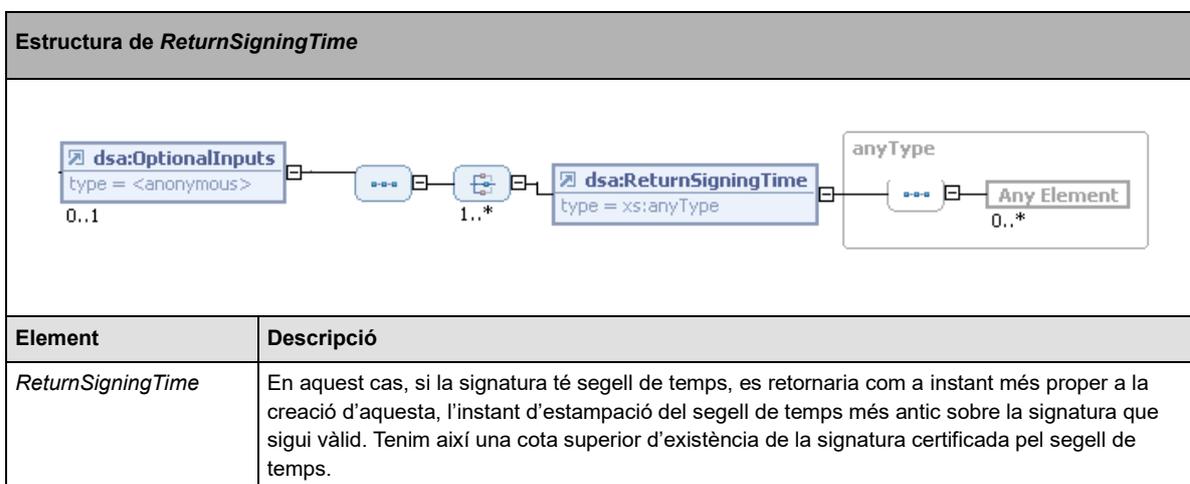
```

U26g9eMvEbnYntFokrShKlEMhc7a/95rT17WiB4F9Nj0MFple6AynhWJEH5nbj0iSsOKhalsDpGZ
2hZ9bcqSgnfTgYg43tG6tROp3P13xX//XgFC9w==
</ds:Modulus>
<ds:Exponent>AQAB</ds:Exponent>
</ds:RSAKeyValue>
</ds:KeyValue>
</ds:KeyInfo>
<ds:Object><xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.2.2#"
Id="QualifyingProperties" Target="#Signature"><xades:SignedProperties
Id="SignedProperties"><xades:SignedSignatureProperties><xades:SigningTime>2024-07-
17T11:11:15.018Z</xades:SigningTime><xades:SigningCertificate><xades:Cert><xades:CertDiges
t><ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod><ds:DigestValue>G1L+w
IA7TS+mwD9iuYUWnq7EBOk=</ds:DigestValue></xades:CertDigest><xades:IssuerSerial><ds:X509Iss
uerName>CN=SubCA SECTOR PUBLIC Q (G3)
A.1,2.5.4.97=#0c0f56415445532d513038303131373541,O=CONSORCI ADMINISTRACIO OBERTA DE
CATALUNYA,C=ES</ds:X509IssuerName><ds:X509SerialNumber>67984833968105534721351953193171481
0309069415732</ds:X509SerialNumber></xades:IssuerSerial></xades:Cert></xades:SigningCertif
icate></xades:SignedSignatureProperties><xades:SignedDataObjectProperties></xades:SignedDa
taObjectProperties></xades:SignedProperties></xades:QualifyingProperties></ds:Object>
</ds:Signature></doc></urn:InlineXML>
</urn:Document>
</urn:InputDocuments>
<urn:SignatureObject>
<urn:SignaturePtr WhichDocument="docId"/>
</urn:SignatureObject>
</urn:VerifyRequest>
</soapenv:Body>
</soapenv:Envelope>

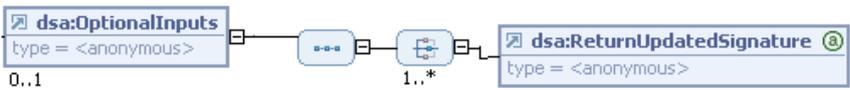
```

Figura 12 Missatge de validació d'una signature XAdES

Tanmateix, alguns dels *OptionalInputs* ja mencionats per a les signatures simples canvien lleugerament el seu significat. Detallarem els *OptionalInputs/Outputs* nous, així com el seu nou significat:



	<p>Si la signatura no té segell de temps, aleshores aquest cas es idèntic al cas simple, i es retornarà instant de temps al·legat dins d'aquesta.</p> <p><i>DSS Core Protocols, Elements, and Bindings. Apartat 4.6.5</i></p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Estructura de <i>ReturnUpdatedSignature</i>	
	
Element	Descripció
<i>ReturnUpdatedSignature</i>	<p>Demana al servidor que retorni la signatura actualitzada a la forma especificada. Hi ha tot un seguit de formes (com ara les definides a XAdES) i aquestes identifiquen una sèrie d'atributs que ha de contenir una signatura per tal de complir amb una forma concreta. El servidor intentarà afegir els atributs no presents a la signatura completant-la fins a complir amb la forma especificada.</p> <p>Els atributs poden ser, per exemple, referències a les CA's del camí de certificació, el path en sí, referències a informació de revocació (CRL/OCSP) o la informació de revocació en sí, així com els diferents tipus de <i>timestamps</i> definits per XAdES.</p> <p><i>DSS Core Protocols, Elements, and Bindings. Apartat 4.6.7</i></p>

Missatge de sortida

Resposta a una validació d'una signatura XAdES
<pre><?xml version="1.0" encoding="UTF-8"?> <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"><soapenv:Body><dss:VerifyResponse Profile="urn:oasis:names:tc:dss:1.0:profiles:XSS" xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"><dss:Result><dss:ResultMajor>urn:oasis: names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor><dss:ResultMinor>urn:oasis:names:tc: dss:1.0:resultminor:valid:signature:onAllDocuments</dss:ResultMinor></dss:Result><dss:Opti onalOutputs><dss:DocumentWithSignature><dss:Document ID="docId"><dss:InlineXML><doc> <title>Proves</title> <body>Document de proves</body> <ds:Signature Id="Signature" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> <ds:SignedInfo Id="SignedInfo"> <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/> <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/> <ds:Reference Id="SignedDataObject-enveloped" URI=""> <ds:Transforms> <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/> <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/> </ds:Transforms> <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/></pre>

```
<ds:DigestValue>/yjKqIr/J4PjFbNY5eNNgpBOVeY=</ds:DigestValue>
</ds:Reference>
<ds:Reference Id="SignedProperties-Reference"
Type="http://uri.etsi.org/01903/v1.2.2#SignedProperties" URI="#SignedProperties">
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>vk5AnJSa6M86VWgswL4HFyWzUU4=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue Id="DocumentSignatureValue">
dCg1R3xq+tx9uZ0z0i4HJUUFcyxjzD8A8lmsTjg/i5YW/EFfUHVl9Tc/pYJQpebc8j3h5r1gbOMA
mHf7a4FO8aP/wckWT6TPikcvapnHQWSGLI8C3hB4rH0CwdfKPtAlPWL39vxxMkbEwXHB1Wf3XW
VAEU2UfbRHS2S6fPIjCaGmP68sWUqRMEql9D00AtAyXx5K+KpVb287A1fUV7B18W51W4CCsQcyUr
zclJpyhyPk0pQYMTfLajln2x+t/u//ZWhOcTZlGkJbgBgh9SiOz5FqzJDKS0k+umO2Emt8tVvmwZ
oz56rBX8Kv21o+tZFPLOwcdCcyZ9qS0ZCz/lkA==
</ds:SignatureValue>
<ds:KeyInfo Id="KeyInfo">
<ds:X509Data>
<ds:X509Certificate>
MIIFLjCCBLsgAwIBAgIUdxV0MscI9JhFuYsSDHmIA9qpTQwCgYIKoZIzj0EAwMwYUxuCzAJBgNV
BAYTAkVTMTMwMQYDVQQKDCpDT05TT1JDSSBBRE1JTk1TVFJBQ01PIE9CRVJUQSBERSDQVRBTFVO
WUEXGDAWBGnVBGEMD1ZBVEVTLVEwODAxMTC1QTEhNCUGAlUEAwweU3ViQ0EgU0VDVE9SIFBvQkxj
QyBRlChMykQs4xMB4XDTIOMDMYMDU0MTk1OFoXDTI4MDMYMDU0MTk1N1owgagxCzAJBgNVBAYT
AkVTR8wHQYDVQKDBZPcmNhbm10emFjacOzIGRlIHByb3ZzMRgWFGYDVQRhDA9WQVRFUy1RMDAw
MDAwMEoxIjAgBgNVBAsMGUNlcnRpZmljYXQgZOKAmWFwG1jYWNpw7MxEjAQBGNVBAUTCVEMDAW
MDAwSjEmMCQGA1UEAwdu21zdGvtYSBvIGFwG1jYWNpw7MgZGUGchJvdmEwgGEMDA0GCSGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDw0B8A9zN3HtIoPdJWSX55BA1387GoIsW2b+4ywRpKm+y5rdib
jEr6APVfiSxgHuQX2G2DNYMUSKmiQMn6XgFujr8DoXLhgY3bp4SSJ21zQVe32rkQC9WWTghxt6mh
zpDTWVOUPfVkdTylA6ddC2uwmr92PvzdYfo7b3r3VQ/IssjoomshoXctt3J8RqRpkq145FH1NvR
Q6uMn4L1rMkMI0U3cNhK2PSCPtTbqD14y8Rudie0WiStKEqUQwdztr/3mtPXtaIHgX02OgwWmV7
oDKeFYkQfmduPSJKw4qFrWwOkZnaFn1typKcd90BiDjeObq1E6nc+XfFf/9eAUL3AgMBAAGjggIQ
MIICDDAMBGNVHRMBAf8EAJAAMB8GA1UdIwQYMBAAFB3+KWURvz9XZYk719R4YTSbd1PmMGkGCCsG
AQUFBwEBBF0wWzA4BggrBgEFBQcwoAoYsaHR0cDovL2Vvc2NkLmFvYy5jYXQvZGVzY2FycmVnYS9j
YXN1Y11hMS5jcnQwHwYIKwYBBQUHMAIGE2h0dHA6Ly9vY3NwLmFvYy5jYXQvYQYDVDR0GBHYwdDBN
BgwrBgEEAfV4AQMCWwEwVzArBggrBgEFBQcCARYfaHR0cHM6Ly9lcHNjZC5hb2MuY2F0L3JlZ3Vs
YWNpbzAoBggrBgEFBQcCAjAcDBpDZXJ0aWZpY2F0IGTigJ1hcGxpY2FjacOzLjAJBgGCEAIvsQAEB
MB4GA1UdJQQXMBUGCCsGAQUFBwMCAgkqhkiG9y8BAQUwagYIKwYBBQUHAQMEYjBcMAGBGAjkyB
ATALBgYEA15GAQMCAQ8wEwYGBACORgEGMAkGBwQAJkyBBgIwLgYGBACORgEFMCQwIhYcaHR0cHM6
Ly9lcHNjZC5hb2MuY2F0L3Bkc191bhMCZW4wNgYDVDR0fBC8wLTAroCmgJ4YlaHR0cDovL2Vvc2Nk
LmFvYy5jYXQvY3JsL2Nhc3ViLWExLmNybDAdBgNVHQ4EFgQUf4EEqGaM2aThoY8q3ug2g3H9DK8w
DgYDVDR0PAQH/BAQDAgXgMAoGCCqGSM49BAMDA2gAMGUCMQCKdQXmAgAKQwE3zKmbmLUaBx7S9/
IvN6T5HcwqRJsYRLDbcmGsn0kVD3DtWfL8CMF+fc8gt3ZByC+cXjEmQTMzVc3VvF1Ng9o4GodC
1Xu+6fXfU31yKa+uo8dWx3CgBw==
</ds:X509Certificate>
</ds:X509Data>
<ds:KeyValue>
<ds:RSAKeyValue>
<ds:Modulus>
1tAfAPczdx7SKD3Y1kl+eQQNd/OxqCLFtm/uMsEaSpvsua3Ym4xK+gD1X4ksYB7kF9htgzcjFEip
okDJ+14Bbo6/A6Fy4YGN26eEkidtc0FXt9q5EAav1k4Icbepoc6Q011T1D31ZCg7WJQOnXQtrsJq
/dj783WBaO29691UPyLLI6KJrIaF3LbdyfEakaZKteORR5Tb0UOrjJ+C5azJmCNFN3J4Stj0gj7
U26g9eMvEbnYntFokrShK1EMHc7a/95rT17WiB4F9Nj0MFple6AynhWJEH5bnj0iSsOKhalsDpGZ
2hZ9bcqSgnfTgYg43tG6tRop3P13xX//XgFC9w==
</ds:Modulus>
<ds:Exponent>AQAB</ds:Exponent>
</ds:RSAKeyValue>
</ds:KeyValue>
</ds:KeyInfo>
<ds:Object><xades:QualifyingProperties Id="QualifyingProperties" Target="#Signature"
xmlns:xades="http://uri.etsi.org/01903/v1.2.2#"><xades:SignedProperties
Id="SignedProperties"><xades:SignedSignatureProperties><xades:SigningTime>2024-07-
```



```

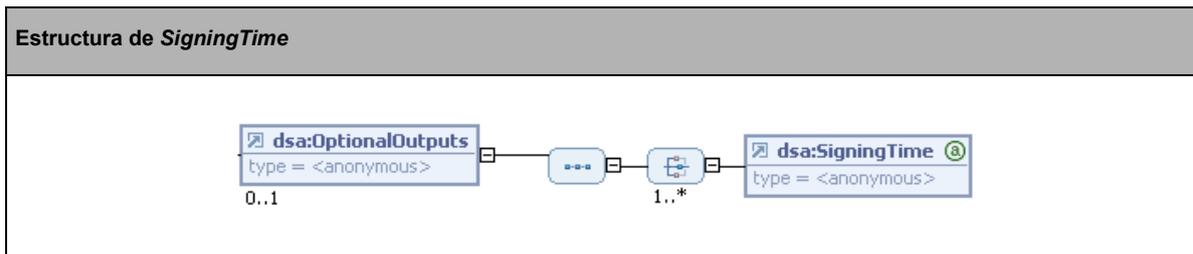
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><ds:DigestValue>lsvizjpsVurJn9SIgeu50
MNH7c=</ds:DigestValue></xades:CertDigest><xades:IssuerSerial><ds:X509IssuerName>CN=CA
CONSORCI AOC (G3) ROOT-A,2.5.4.97=#0c0f56415445532d513038303131373541,O=CONSORCI
ADMINISTRACIO OBERTA DE
CATALUNYA,C=ES</ds:X509IssuerName><ds:X509SerialNumber>11933380261995576280039581641610225
2218</ds:X509SerialNumber></xades:IssuerSerial></xades:Cert></xades:CertRefs></xades:Compl
eteCertificateRefs><xades:CompleteRevocationRefs Id="id-40dae46f-69f1-4657-b4d0-
c18dff28561"><xades:CRLRefs><xades:CRLRef><xades:DigestAlgAndValue><ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><ds:DigestValue>uK3lM5Q0cSVX5EAuJTN1l
krzI4=</ds:DigestValue></xades:DigestAlgAndValue><xades:CRLIdentifier><xades:Issuer>CN=Sub
CA SECTOR PUBLIC Q (G3) A.1,2.5.4.97=#0c0f56415445532d513038303131373541,O=CONSORCI
ADMINISTRACIO OBERTA DE CATALUNYA,C=ES</xades:Issuer><xades:IssueTime>2024-07-
17T11:07:29.000Z</xades:IssueTime><xades:Number>121</xades:Number></xades:CRLIdentifier></
xades:CRLRef><xades:CRLRef><xades:DigestAlgAndValue><ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><ds:DigestValue>7+Cf86ENmsLvnzg66CN6ap
03CAk=</ds:DigestValue></xades:DigestAlgAndValue><xades:CRLIdentifier><xades:Issuer>CN=CA
CONSORCI AOC (G3) ROOT-A,2.5.4.97=#0c0f56415445532d513038303131373541,O=CONSORCI
ADMINISTRACIO OBERTA DE CATALUNYA,C=ES</xades:Issuer><xades:IssueTime>2024-03-
21T12:02:59.000Z</xades:IssueTime><xades:Number>6</xades:Number></xades:CRLIdentifier></xa
des:CRLRef></xades:CRLRefs></xades:CompleteRevocationRefs></xades:UnsignedSignaturePropert
ies></xades:UnsignedProperties></xades:QualifyingProperties></ds:Object>
</ds:Signature></doc></dss:InlineXML></dss:Document></dss:DocumentWithSignature><dss:Updat
edSignature Type="urn:oasis:names:tc:dss:1.0:profiles:XAdES:forms:ES-
C"><dss:SignatureObject><dss:SignaturePtr
WhichDocument="docId"/></dss:SignatureObject></dss:UpdatedSignature></dss:OptionalOutputs>
</dss:VerifyResponse></soapenv:Body></soapenv:Envelope>
  
```

Figura 13 Missatge de resposta a una validació d'una signature XAdES

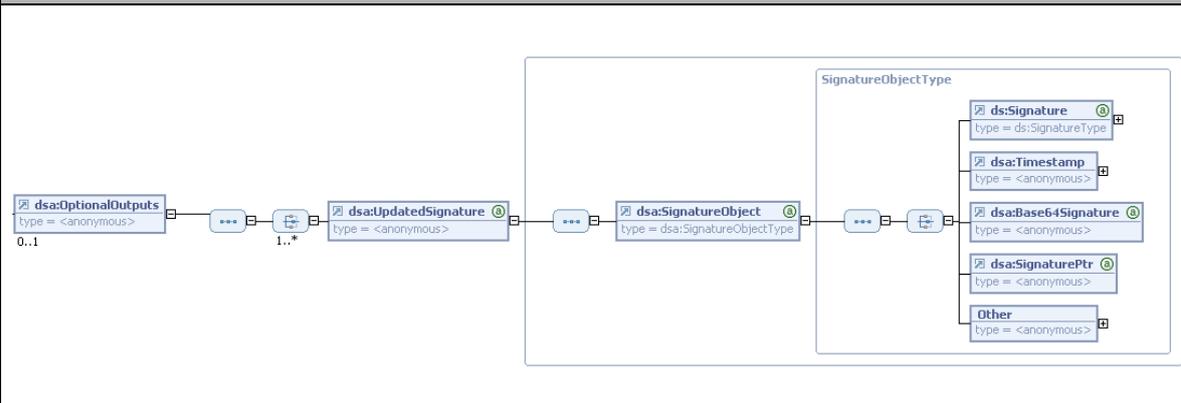
El missatge de sortida segueix l'estructura bàsica plantejada per l'estàndard DSS.

Els elements més importants continguts a la resposta d'una validació de signatura XAdES són:

- **Result**
 Estructura de dades amb el resultat del procés de validació. Indica el resultat de la validació com la resta de les respostes basades en DSS.
- **OptionalOutputs**
 Estructura de dades que contindrà la informació sol·licitada pel client als elements introduïts dins de l'estructura *OptionalInputs*.



Element	Descripció
<i>SigningTime</i>	Retorna el temps de signatura. El procés d'obtenció està detallat a l' <i>OptionalInput</i> corresponent. <i>DSS Core Protocols, Elements, and Bindings</i> . Apartat 4.6.5

Estructura de <i>UpdatedSignature</i>	
	
Element	Descripció
<i>UpdatedSignature</i>	Retorna la signatura actualitzada a la forma demanada (en cas que no la complís) així com la URI corresponent a la forma més propera a la signatura retornada que pugui determinar el servidor. <i>DSS Core Protocols, Elements, and Bindings</i> . Apartat 4.6.7

5.4. Validació de documents PDF signats

La validació de documents PDF signats és pràcticament igual que la validació d'una signatura qualsevol, però amb alguns canvis com l'endpoint que s'invoca, o atributs específics, etc...

- L'endpoint on s'envia la petició és diferent. Si les peticions de validació de certificats o signatures s'envien a l'endpoint acabat en "dss", en aquest cas s'han d'enviar a l'endpoint acabat en "dsspdf".
- Les peticions han de tenir el perfil (*profile*) següent:
urn:OASIS:names:tc:dss:1.0:profiles:DSS_PDF
- Cal indicar el mimetype del document que s'adjunta a la VerifyRequest, en aquest cas amb el valor de "application/pdf".

Endpoints

- Entorn d'integració:
<https://psis-pre.aoc.cat/psis/catcert-test/dsspdf>
- Entorn d'explotació:
<https://psis.aoc.cat/psis/catcert/dsspdf>

Missatge d'entrada

Un possible missatge d'entrada podria ser el següent (on el contingut complet del document PDF, la signatura del qual es vol validar, s'ha eliminat per a major claredat):

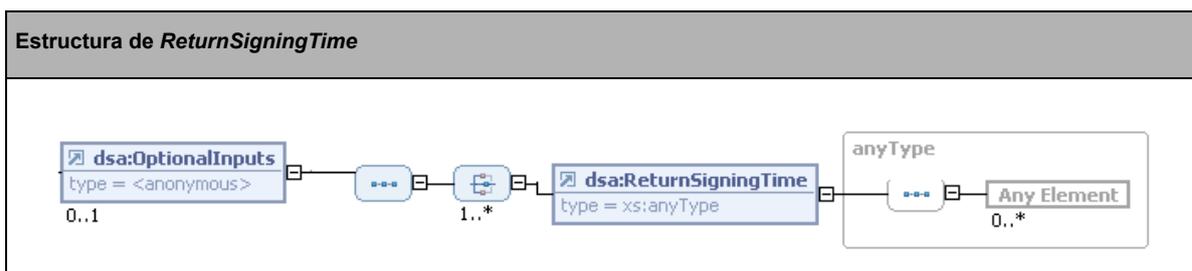
```

Validació d'un document PDF

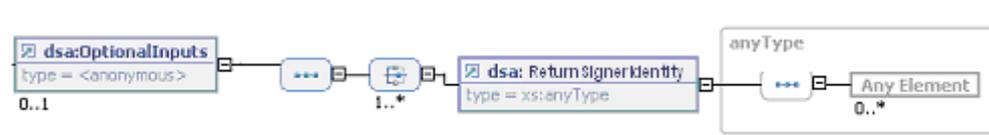
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <dss:VerifyRequest Profile="urn:oasis:names:tc:dss:1.0:profiles:DSS_PDF"
  xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
  xmlns:pdf="urn:oasis:names:tc:dss:1.0:profiles:DSS_PDF">
      <dss:OptionalInputs>
        <dss:ReturnSigningTime/>
        <dss:ReturnSignerIdentity/>
        <pdf:ReturnSignatureReason/>
      </dss:OptionalInputs>
      <dss:InputDocuments>
        <dss:Document>
          <dss:Base64Data MimeType="application/pdf">JVBER...</dss:Base64Data>
        </dss:Document>
      </dss:InputDocuments>
    </dss:VerifyRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
  
```

Figura 14 Missatge de validació d'un document PDF

OptionalInputs que es poden sol·licitar en una petició de validació d'un PDF signat:



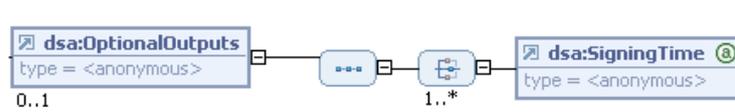
Element	Descripció
<i>ReturnSigningTime</i>	Demana al servidor que retorni l'instant de creació de la signatura.

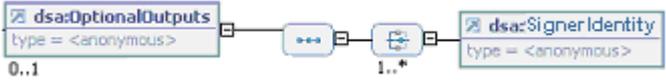
Estructura de <i>ReturnSignerIdentity</i>	
	
Element	Descripció
<i>ReturnSignerIdentity</i>	Demana al servidor que retorni la identitat del signant present a la signatura.

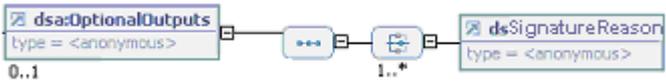
Estructura de <i>ReturnSignatureReason</i>	
	
Element	Descripció
<i>ReturnSignatureReason</i>	Demana al servidor que retorni la raó que va definir per a la creació de la signatura el seu creador.

Missatge de sortida

El format del missatge de sortida segueix els mateixos criteris que la resta de validació de signatura.

Estructura de <i>SigningTime</i>	
	
Element	Descripció
<i>SigningTime</i>	Retorna el temps de creació de la signatura sobre el document. El procés d'obtenció està detallat a l' <i>OptionalInput</i> corresponent.

Estructura de <i>SignerIdentity</i>	
	
Element	Descripció
<i>SignerIdentity</i>	Retorna la identitat del signant.

Estructura de <i>SignatureReason</i>	
	
Element	Descripció
<i>SignatureReason</i>	Retorna la raó de la signatura que el seu creador va especificar quan la va crear.

5.5. Creació de segells de temps

Un segell de temps és una evidència electrònica mitjançant la qual podem assegurar sense possibilitat de repudiació que una dada existia en un moment de temps determinat. Els segells de temps són creats per unes autoritats especials anomenades TSA (*TimeStamp Authorities*).

Les TSA són entitats en els rellotges de les quals (o sistemes de mesura del temps) es diposita confiança. La TSA de PSIS està sincronitzada amb el servidor de temps NTP del Real Observatorio de la Armada (ROA), que marca l'hora oficial a Espanya. ROA té com a missió principal el manteniment de la unitat bàsica de Temps a Espanya així com el manteniment i la difusió oficial de l'escala "Temps Universal Coordinat" (UTC (ROA)), considerada amb caràcter general com la base de l'hora legal a tot el territori nacional (R. D. 23 octubre 1992, núm. 1308/1992).

Actualment la TSA publica els serveis de segell de temps de les formes següents:

- Notació abstracta ASN.1, així es compleix amb les especificacions de la IETF RFC3161, utilitzant sintaxi de peticions i respostes en notació abstracta ASN.1 codificat en DER.
- Web Service dissenyats per facilitar la integració amb les aplicacions, fent servir l'especificació de missatges XML-SOAP.

A continuació es detalla el procés per obtenir un segell de temps (aquest procés pot realitzar-se mitjançant el client subministrat):

1. El client vol generar un segell de temps per a un document que posseeix.
2. Es genera el hash del document a la màquina del client, mitjançant un dels algorismes permesos per la plataforma.
3. S'envia una petició de creació de segell de temps que contindrà el hash del document. L'estructura de la petició serà diferent segons el protocol que es faci servir: Web-Service (DSS) o TCP (RFC3161).
4. PSIS generarà el segell de temps amb el hash, la data i l'hora (obtinguda gràcies a un client NTP sincronitzat ROA), i la signatura electrònica de la TSA.
5. S'envia el segell de temps al client.

5.5.1. Creació de segell de temps mitjançant protocol TCP

L'endpoint on s'envia la petició és diferent. Si les peticions de validació de certificats o signatures s'envien a l'endpoint acabat en "dss", en aquest cas s'han d'enviar a l'endpoint acabat en "tsp".

No és objectiu del present document detallar la manera com es crea un missatge ASN.1 de sol·licitud de segell de temps. El protocol de segellat de temps, en els quals es basa la plataforma, es troben especificats al següent RFC:

RFC 3161 "Internet X.509 Public Key Infrastructure Time Stamp Protocols", estàndard definit per Internet Engineering Task Force (IETF) per al protocol Time Stamp.

Endpoints

- Entorn d'integració:
<https://psis-pre.aoc.cat/psis/catcert-test/tsp>
- Entorn d'explotació:
<https://psis.aoc.cat/psis/catcert/tsp>

5.5.2. Creació de segell de temps amb missatgeria DSS

Existeix un perfil de DSS anomenat *Timestamp Profile* que amplia el core del DSS per fer possible la creació i validació de segells de temps.

PSIS suporta ambdues maneres de procedir amb el tractament de segells de temps (creació i validació) i per tal de poder accedir a la plataforma PSIS en aquest perfil el client només ha d'afegir l'atribut **Profile**="urn:OASIS:names:tc:dss:1.0:profiles:timestamping" a la **VerifyRequest** en cas de validacions o a la **SignRequest** en cas de peticions.

A grans trets, el procés per a obtenir un segell de temps consisteix en generar el resum digital (*digest* o *hash*) del document a segellar per a transmetre'l a la TSA desitjada. La TSA, quan rep el missatge a segellar, genera una marca de temps (*timestamp*) la qual afegeix al hash rebut i el signa digitalment amb la seva clau privada.

Endpoints

- Entorn d'integració:
<https://psis-pre.aoc.cat/psis/catcert-test/dss>
- Entorn d'explotació:
<https://psis.aoc.cat/psis/catcert/dss>

En el següent exemple es descriu la missatgeria:

Missatge d'entrada

En aquest tipus de missatge estem demanant al servidor que ens retorni un segell de temps sobre el document proporcionat. Podem demanar diferents tipus de segells de temps (CMS o XML) sobre diferents tipus de components. Això vol dir que els continguts a segellar poden ser un *digest*, dades en *Base64* o XML, però no tots són compatibles amb tots.

A continuació podem veure una taula on es detalla les compatibilitats amb tots els tipus.

Taula comparativa	
Tipus de segell de temps	Tipus de contingut a segellar compatible
CMS	Digest
XML	Digest, Base64, XML

Figura 15 Taula de compatibilitat entre formats de segells de temps i els continguts a estampar

Normalment els segells de temps CMS es fan servir per a dades binàries en *Base64* o digerides mentre que els XML poden segellar qualsevol tipus de contingut.

Aquest primer missatge demana la creació d'un segell de temps XML sobre el contingut proporcionat ja digerit pel client.

Creació d'un segell de temps en format XML

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <dss:SignRequest
      RequestID="I9e54e5e59e9724683b2379f846ec0f98"
      xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
      Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping">
      <dss:OptionalInputs>
        <dss:SignatureType>
oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken </dss:SignatureType>
      </dss:OptionalInputs>
      <dss:InputDocuments>
        <dss:DocumentHash ID="Doc1">
          <ds:DigestMethod
            Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
            xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
          <ds:DigestValue
            xmlns:ds="http://www.w3.org/2000/09/xmldsig#">2jmj715rSw0yVb/vlWAYkK/YBwk=</ds:DigestValue
          >
        </dss:DocumentHash>
      </dss:InputDocuments>
    </dss:SignRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Figura 16 Missatge de creació d'un segell de temps en format XML

En el següent exemple es pot comprovar com es pot demanar la creació d'un segell de temps CMS sobre un contingut ja digerit pel client.

Creació d'un segell de temps en format CMS

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <dss:SignRequest
      RequestID="I9e54e5e59e9724683b2379f846ec0f98"
      xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
      Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping">
      <dss:OptionalInputs>
        <dss:SignatureType>urn:ietf:rfc:3161</dss:SignatureType>
      </dss:OptionalInputs>
      <dss:InputDocuments>
        <dss:DocumentHash ID="Doc1">
          <ds:DigestMethod
            Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
            xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
          <ds:DigestValue
            xmlns:ds="http://www.w3.org/2000/09/xmldsig#">2jmj715rSw0yVb/vlWAYkK/YBwk=</ds:DigestValue
          >
        </dss:DocumentHash>
      </dss:InputDocuments>
    </dss:SignRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

```

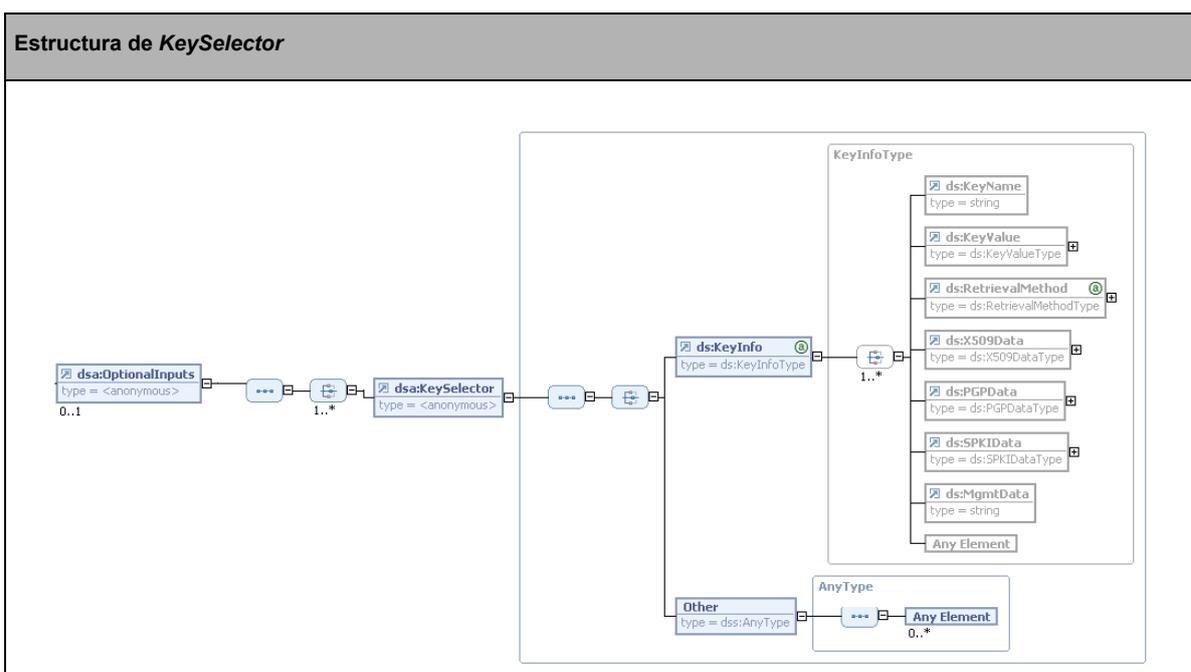
</dss:InputDocuments>
  </dss:SignRequest>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Figura 17 Missatge de creació d'un segell de temps en format CMS

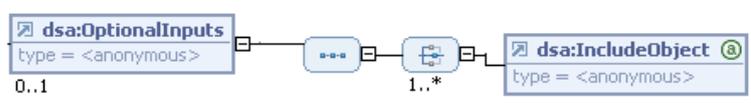
En el cas de creació de segells de temps, els *OptionalInputs* prenen un paper clau i són determinants per a la correcta creació dels segells.

Estructura de <i>SignatureType</i>	
Element	Descripció
<i>SignatureType</i>	Determina el tipus de segell de temps a generar pel servidor. <i>DSS Core Protocols, Elements, and Bindings. Apartat 3.5.1</i>
Tipus de segells de temps disponibles	Valor
<i>Timestamp</i> (CMS)	urn:ietf:rfc:3161
<i>Timestamp</i> (XMLDSig)	oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken



Element	Descripció
<i>KeyInfo</i>	<p>Determina la clau que ha de fer servir el servidor per a crear el segell de temps ja que el certificat proporcionat indica al servidor quina és la identitat que ha d'assumir a l'hora de signar el segell.</p> <p>La implementació actual de la plataforma PSIS no dona suport a aquest element.</p> <p><i>XSS Profile of the OASIS DSS. Apartat 4.13</i></p>

Aquest *OptionalInput* només aplica al cas XML:

Estructura de <i>IncludeObject</i>	
	
Element	Descripció
<i>IncludeObject</i>	<p>Demana al servidor que quan creï el segell de temps inclogui el contingut signat dins del propi segell, creant segells de temps <i>enveloping</i>.</p> <p><i>DSS Core Protocols, Elements, and Bindings. Apartat 3.5.6</i></p>

Missatge de sortida

El missatge de sortida ens retorna, a banda d'un codi que ens informa de si la petició s'ha processat de manera correcta o no (veure codis de retorn DSS per a més informació), un *SignatureObject* idèntic al present a les peticions de validació però que conté el segell de temps generat.

Aquí trobarem un element *Signature* si el segell és XML i un *timestamp* codificat en *Base64* en cas de que sigui CMS.

Resposta de creació d'un segell de temps XML

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <dss:SignResponse Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping"
      RequestID="I9e54e5e59e9724683b2379f846ec0f98"
      xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
      <dss:Result>
<dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>
        <dss:ResultMessage xml:lang="en">Signature created</dss:ResultMessage>
      </dss:Result>
    </dss:SignResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

```

<dss:OptionalOutputs/>
<dss:SignatureObject>
  <dss:Timestamp>
    <ds:Signature Id="id-35628298-7ff4-4b3d-99f2-a90b66852f5e"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo Id="id-edf7e577-0201-4d47-aced-5345661e474a">
        <ds:CanonicalizationMethod
          Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
        <ds:SignatureMethod
          Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference Id="id-6b24e8c2-8b5a-4378-85f4-ae1b7c66e723">
          <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>2jmj715rSw0yVb/vlWAYkK/YBwk=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#TSTInfo-id-a58ac98d-106e-41fb-af7a-
4be4779d5a02" Id="id-172ca137-8939-4af6-8636-13a9961832af"
Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken">
          <ds:Transforms>
            <ds:Transform
              Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </ds:Transforms>
          <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>Bfg4btfaYTpHH+WF8476LIq90/o=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>
Rju4P8zGqsQw8Yn0HjAnFYt+uVkhUTXe/yzpL4z6YTS3A3mYv4SKmsBLmvt0HGwvRHR3STMiQC2o
qdf5e/KrEDIkF4CG/+PUTJp4M7766mRMR5yrBg7x157F8SNeEbwBQsqnblcrF3poW5JcW0ayS2uf
zXS+vU/zZD+kseX3ag0=</ds:SignatureValue>
      <ds:KeyInfo>
        <ds:X509Data>
<ds:X509Certificate>MIIHIDCCBgigAwIBAgIQbg5vDBUDLv1ELR24xDVsZzANBgk
.../BAQDAgeAMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMIMEB0GA1UdDgQWBQBp0Ii85EbkB/+WT2f5cqRUu8oo3F4REK
59hnPbxLaVZ/8zDp2afqKOGOAd9e8TCKY3Nx7tOijnd+jnEIYe/BTisMTXqx8+o0eYoI9uFX/imQmms569KsPXGnVd
byuys5LE6iCfeeOOVwz9ruKeDwX6f+MQw9mkTguh7vFebCNpyfxIzjbDHXKy1NOeVdd1UYs2tgPhOqHBHXZLepU8aR
Zx3ixKF7TQaipnQc4PLrKUqPrPkQCMtN73b1RrOtfcd09C8ZtLIwVELd9vbYAp9n0TvdxbWvHSHvFfkFWjq8HRUD+
ptXHDZaWBxmuUQ==</ds:X509Certificate>
        </ds:X509Data>
        <ds:KeyValue>
          <ds:RSAKeyValue>
<ds:Modulus>ALMdRzdnoHg90PT4ukAz6VpNL+qDcfoJE7R+1N08SdlvqeFarXqkYze36dJ3J2ypXHf+vKWF5HsEYy
jfsCkPRyil6CWYoQOfyhycVr1X3gAmsFSlQmiIZsrbuE3cXR+4I2ZIxGlvqbpSVRp0Nmfo90W5s4OofWbbemGSldpK
pA8v</ds:Modulus>
          <ds:Exponent>AQAB</ds:Exponent>
          </ds:RSAKeyValue>
        </ds:KeyValue>
      </ds:KeyInfo>
      <ds:Object Id="TSTInfo-id-a58ac98d-106e-41fb-af7a-4be4779d5a02"
MimeType="application/xml">
        <dss:TstInfo>
<dss:SerialNumber>487517772120598484027575696654783309170220764526</dss:SerialNumber>
        <dss:CreationTime>2006-08-
08T09:29:11.515Z</dss:CreationTime>
        <dss:Policy>urn:oid:0.4.0.2023.1.1</dss:Policy>
        <dss:ErrorBound>PT1S</dss:ErrorBound>
        <dss:Ordered>true</dss:Ordered>
        <dss:TSA

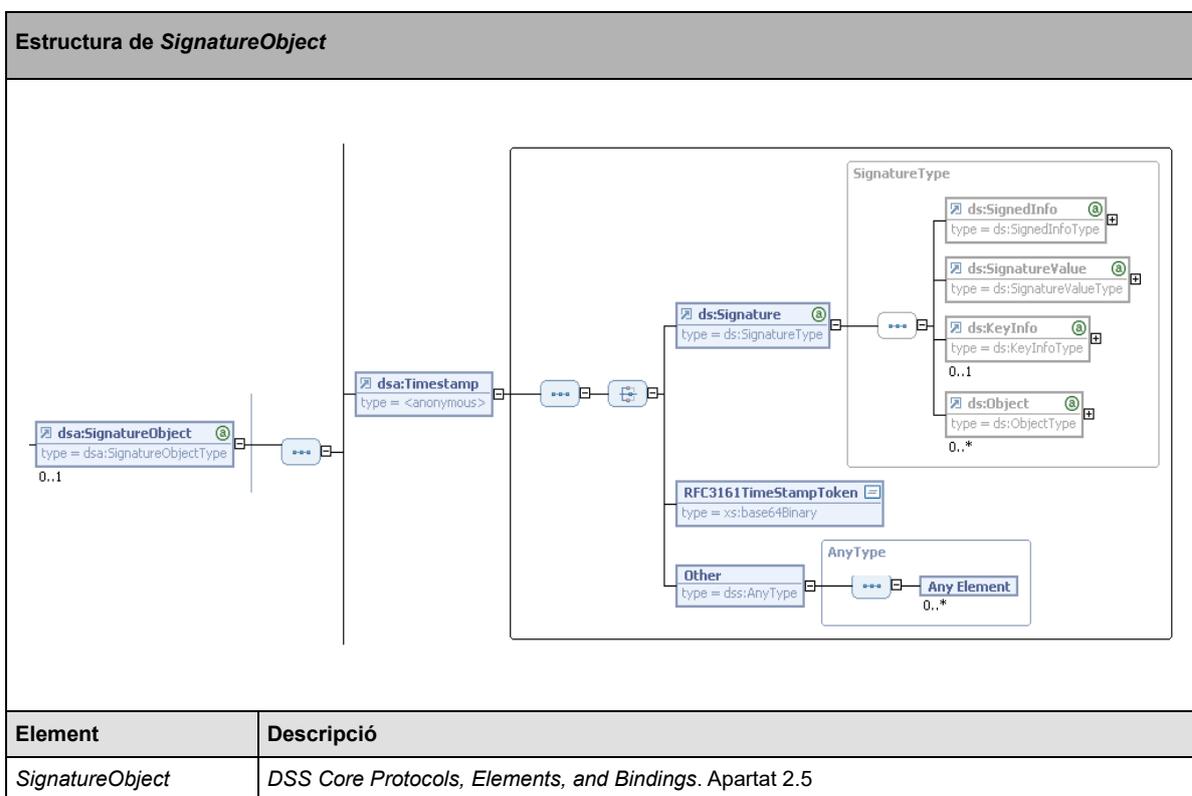
```

```

format:X509SubjectName"
Format="urn:oasis:names:tc:SAML:1.1:nameid-
Entitats de
>CN=Servei de segellat de temps de PSIS,OU=Jerarquia
Certificacio Catalanes,OU=Vegeu
https://www.catcert.net/verCIT-1
(c)05,OU=Serveis Publics de Certificacio CIT-
1,O=Agencia
Catalana de Certificacio (NIF Q-0801176-
I),C=ES</dss:TSA>
</dss:TstInfo>
</ds:Object>
</ds:Signature>
</dss:Timestamp>
</dss:SignatureObject>
</dss:SignResponse>
</soapenv:Body>
</soapenv:Envelope>
  
```

Figura 18 Missatge de resposta de creació d'un segell de temps

Així els segells de temps resultants aniran dins de l'estructura *SignatureObject* següent.



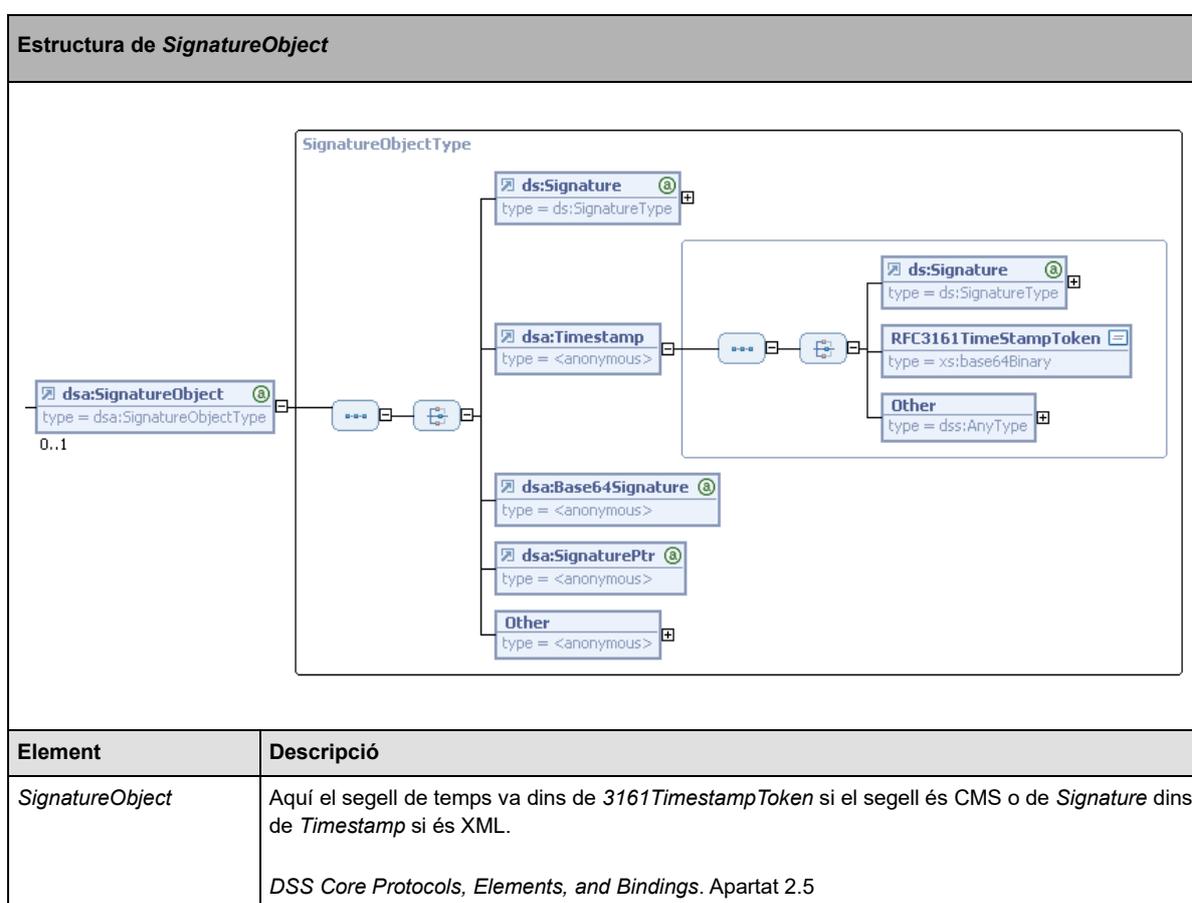
5.5.3. Validació de segells de temps amb missatgeria DSS

Aquesta funcionalitat permet fer la validació d'un segell de temps. És molt similar a la validació de signatures (donat que un segell de temps no és més que una signatura amb constància de l'instant temporal) i la seva missatgeria és gairebé idèntica.

Endpoints

- Entorn d'integració:
<https://psis-pre.aoc.cat/psis/catcert-test/dss>
- Entorn d'exploració:
<https://psis.aoc.cat/psis/catcert/dss>

L'únic aspecte en el qual mostren discrepàncies importants és que el segell de temps va dins de l'element *Timestamp* del *SignatureObject* i no dins del *SignatureObject* en sí. D'aquesta manera indiquem que la signatura que estem validant és un segell de temps.



En el següent exemple es descriu la missatgeria:

Missatge d'entrada

Aquí mostrem un exemple de validació de segell de temps XML.

Validació d'un segell de temps en format XML

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <dss:VerifyRequest Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping"
      xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
      <dss:InputDocuments>
        <dss:DocumentHash ID="Doc1">
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
            xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
          <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
            >2jmj715rSw0yVb/vlWAYkK/YBwk=</ds:DigestValue>
        </dss:DocumentHash>
      </dss:InputDocuments>
      <dss:SignatureObject>
        <dss:Timestamp>
          <ds:Signature Id="id-43d445db-c7b8-474b-8671-59cfd1f1d4b6"
            xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:SignedInfo Id="id-1481a051-8df1-43ce-b5f3-2651a485b60d">
              <ds:CanonicalizationMethod
                Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
              <ds:SignatureMethod
                Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
              <ds:Reference URI="#TSTInfo-id-53785d35-b3d4-4053-b8e4-
015420b7a652"
                Id="id-9be94625-1874-4e12-8a4e-66644e54bc31"
                Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken">
                <ds:Transforms>
                  <ds:Transform
                    Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
                </ds:Transforms>
                <ds:DigestMethod
                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>Ra+HCOC2g2ET1aPTEqSt9fa2FrY=</ds:DigestValue>
              </ds:Reference>
              <ds:Reference Id="id-edac93f9-1a1d-48e5-a464-8c81b2abb090">
                <ds:DigestMethod
                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>2jmj715rSw0yVb/vlWAYkK/YBwk=</ds:DigestValue>
              </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>
              ccb5951HswznoFYkXwwjc4RZ2ozXuVng0gg3ABSixat3yEsxG4oGzbRAeZnE+xeurYnD9RRv1rTE
              edAawGn8YQskeUY74ONeyGMdOXMV1fc8n7sSJdThLWEINQtXg/nAkSxTALSINqW/BW9OGbmRyXN+
              +RA115ef1x6sJHqFtPE=</ds:SignatureValue>
            <ds:KeyInfo>
              <ds:X509Data>
```

```

<ds:X509Certificate>MIIHIDCCBgigAwIBAgIQbg5vDBUDLv1ELR24xDVsZzANBgkqhkiG9w0BAQUFADCB8zELMA
kGAlUEBhMCRVMxOzA5BgNVBAoTMkFnZW5jaWEgQ2F0YWxhbmEgZGUgQ2VydGlmaWNhY21vICChOSUYgUS0wODAxMTc2
LUkpMSgwJgYDVQQLEx9TZXJ2ZWlziFB1Ymxp...+dO9C8ZtLIwVEld9vbYAp9n0TvdxbWrHSHvFfkFWjq8HRUD+ptX
HDZaWBxmuUQ==</ds:X509Certificate>
      </ds:X509Data>
      <ds:KeyValue>
        <ds:RSAKeyValue>
<ds:Modulus>ALMdRzdnoHg90PT4ukAz6VpNL+qDcfOjE7R+1NO8SdlvqeFarXqkYze36dJ3J2ypXHf+vKWF5HsEYy
jfsCkPRyil6CWYoqOfyhycVr1X3gAmsFSlQmiIZsrbuE3cXR+4I2ZIxGlvqbpSVRp0Nmfo90W5s4OofWbbemGSldpK
pA8v</ds:Modulus>
          <ds:Exponent>AQAB</ds:Exponent>
        </ds:RSAKeyValue>
      </ds:KeyValue>
    </ds:KeyInfo>
    <ds:Object Id="TSTInfo-id-53785d35-b3d4-4053-b8e4-015420b7a652"
      MimeType="application/xml">
      <dss:TstInfo
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
<dss:SerialNumber>70640059021933358515457823778492235485949471232</dss:SerialNumber>
      <dss:CreationTime>2006-04-
12T11:51:36.977Z</dss:CreationTime>
      <dss:Policy>urn:oid:9.9.9.9</dss:Policy>
      <dss:ErrorBound>PT1S</dss:ErrorBound>
      <dss:Ordered>true</dss:Ordered>
      <dss:TSA
          Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName"
          >CN=Servei de segellat de temps de PSIS,OU=Jerarquia
Entitats de
          Certificacio Catalanes,OU=Vegeu
https://www.catcert.net/verCIT-1
          (c)05,OU=Serveis Publics de Certificacio CIT-
1,O=Agencia
          Catalana de Certificacio (NIF Q-0801176-
I),C=ES</dss:TSA>
        </dss:TstInfo>
      </ds:Object>
    </ds:Signature>
  </dss:Timestamp>
</dss:SignatureObject>
</dss:VerifyRequest>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Figura 19 Missatge de validació d'un segell de temps en format XML

El següent és un exemple de validació de segell de temps CMS:

Validació d'un segell de temps en format CMS

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>

```

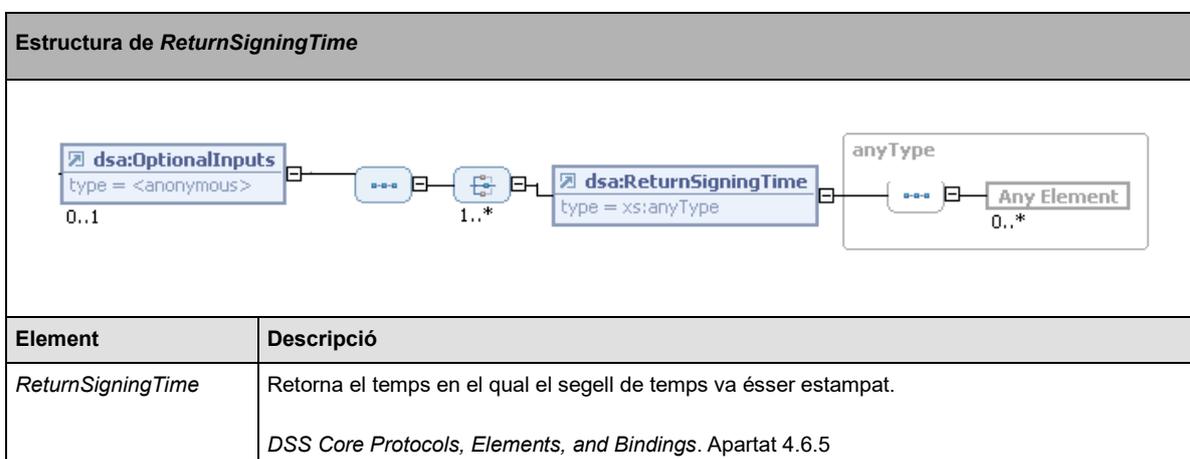
```

<dss:VerifyRequest Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
  <dss:OptionalInputs>
    <dss:ReturnProcessingDetails/>
  </dss:OptionalInputs>
  <dss:InputDocuments>
    <dss:DocumentHash ID="Doc1">
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmlsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmlsig#"/>
      <ds:DigestValue
xmlns:ds="http://www.w3.org/2000/09/xmlsig#">2jmmj715rSw0yVb/v1WAYkK/YBwk=</ds:DigestValue
>
    </dss:DocumentHash>
  </dss:InputDocuments>
  <dss:SignatureObject><dss:Timestamp><dss:RFC3161TimeStampToken>MIAGCSqGSib3DQEHAqCAMIACAQM
xCzAJBgUrdGMCgGUAMIAGCyqGSib3DQEJEAEEOIAEggGHMIIBgwIBAQQYEgnEJCTAhMAkGBSsOAwIaBQAEEFN05o+5ea
0sNMLW/75VgGJCv2AcJAhQ2aw5KFUwGIemIkQPiS+xpPNQlhRgPMjAwNjA0MTIxMTUzMjZaMAkCAQGAQAQGBAQBaf+
...
+Q9b10Be20Hlp46QxiQ3s+5R+eWNZqCjtRWdwdqa9ITmbOie0sNall1E9hrQtTXr4kgmHG55w+ULDTqoK0mW07ABLU
MUEwLtSrVpzRmAAAAA</dss:RFC3161TimeStampToken></dss:Timestamp></dss:SignatureObject>
</dss:VerifyRequest>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Figura 20 Missatge de validació d'un segell de temps en format CMS

Els *OptionalInputs/Outputs* són els mateixos que a les validacions de signatura. Només s'inclouen els que canvien el seu significat.



Missatge de sortida

El missatge de sortida es idèntic al retornat pel servidor en el cas de validacions de signatures, així que les mateixes consideracions sobre *Result* i *OptionalOutputs* son vàlides.

Resposta d'una validació d'un segell de temps

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <dss:VerifyResponse Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping"
      xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
      <dss:Result>
<dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>
<dss:ResultMinor>urn:oasis:names:tc:dss:1.0:resultminor:valid:signature:onAllDocuments</ds
s:ResultMinor>
        </dss:Result>
        <dss:OptionalOutputs/>
      </dss:VerifyResponse>
    </soapenv:Body>
  </soapenv:Envelope>
```

Figura 21 Missatge de resposta d'una validació d'un segell de temps

6. Codis de resposta

Codis de resposta de PSIS.

6.1. 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.

6.1.1. ResultMajor

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

Els possibles valors que pot prendre són:

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

6.1.2. ResultMinor

Aporta informació sobre el resultat de la operació.

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

6.1.2.1. 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
<i>NotAuthorized</i>	Error	El client no està autoritzat a realitzar la operació especificada.
<i>NotSupported</i>	Error	No es suporta o reconeix la petició sol·licitada pel client.
<i>InvalidSignatureObject</i>	Error	El contingut de l'element <i>SignatureObject</i> de la petició no és correcte.
<i>InvalidOptionalInput</i>	Error	L' <i>OptionalInput</i> especificat no està suportat pel perfil de la petició o pel servidor.
<i>XMLDocumentNotValid</i>	Error	No es pot validar el document contra el seu esquema.
<i>NotParseableXMLDocument</i>	Error	No es pot <i>parsejar</i> el document com a un XML vàlid.
<i>XPathEvaluationError</i>	Error	El resultat d'avaluar l'expressió XPath indicada és erroni.
<i>InvalidCertificateAttribute</i>	Error	S'ha demanat un atribut inexistent per a ésser extret del certificat.
<i>invalid:InvalidHashLength</i>	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
<i>InternalServerError</i>	Error	S'ha produït un error intern en el servidor.

6.1.2.2. 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
<i>Definitive</i>	Vàlid	El certificat d'entitat final enviat a validar es vàlid.
<i>Temporal</i>	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
<i>OnHold</i>	Invàlid	El certificat d'entitat final enviat a validar està en estat suspès.
<i>Revoked</i>	Invàlid	El certificat d'entitat final enviat a validar està revocat.
<i>Expired</i>	Invàlid	El certificat d'entitat final enviat a validar ha expirat.
<i>NotYetValid</i>	Invàlid	El certificat d'entitat final enviat a validar encara no ha començat el seu període de validesa.
<i>CertificatePolicyNotSupported</i>	Invàlid	El certificat enviat està estampat seguint una política de certificació no suportada pel servidor.
<i>QualifiedCertificateRequired</i>	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
<i>CertificateNotEE</i>	Error	El certificat enviat a validar no és un certificat d'entitat final.
<i>Status_NoCertificatePathFound</i>	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.
<i>PathValidationFails</i>	Error	No s'ha pogut validar la cadena de certificats del certificat d'entitat final a validar.
<i>RevocationStatusInfoNotFound</i>	Error	El servidor no pot trobar la informació de revocació d'algun dels certificats de la cadena.
<i>UntrustedRevocationStatusInfo</i>	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.
<i>BadCertificateFormat</i>	Error	El certificat a validar no està codificat correctament.
<i>BadCertificateSignature</i>	Error	La signatura que protegeix el certificat no és vàlida.

6.1.2.3. 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
<i>OnAllDocuments</i>	Vàlid	Signatura o segell de temps vàlids.
<i>onTransformedDocuments</i>	Vàlid	Signatura o segell de temps vàlids sobre documents enviats amb transformacions no especificades pel client.

<i>notAllDocumentsReferenced</i>	Vàlid	Signatura o segell de temps vàlids sobre algun dels documents enviats pel client, però no tots els documents adjunts dins dels <i>InputDocuments</i> estan referenciats per la signatura.
<i>allNecessaryIdentifiersNotPresent</i>	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 <i>Id</i> , etc...)

urn:oasis:names:tc:dss:1.0:resultminor:invalid:[valor]		
Valor	Tipus	Descripció
<i>referencedDocumentNotPresent</i>	Invàlid	La petició de validació no conté algun dels documents referenciats per la signatura.
<i>signatureNotPresent</i>	Invàlid	El document PDF enviat a validar no conté cap signatura.
<i>incorrectSignature</i>	Invàlid	La signatura no és correcta, ja sigui perquè s'ha generat incorrectament, o perquè ha sigut modificada.
<i>indeterminateKey</i>	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.
<i>untrustedKey</i>	Invàlid	El servidor no considera que el certificat de la signatura sigui vàlid. Això vol dir que està revocat o <i>suspès</i> .

urn:oasis:names:tc:dss:1.0:resultminor:[valor]		
Valor	Tipus	Descripció
<i>ValidMultiSignatures</i>	Vàlid	Totes les signatures són vàlides.
<i>InvalidMultiSignature</i>	Invàlid	Alguna o totes les signatures són invàlides.
<i>CannotDeterminePDUValidity</i>	Error	Impossible determinar la validesa de la PDU.
<i>InvalidTransformURI</i>	Error	L'URI de transformada especificada no és vàlida o no està suportada.
<i>CannotPerformTransform</i>	Error	El servidor no pot dur a terme la transformació.
<i>InvalidSignatureCheckDetails</i>	Error	La signatura és invàlida. Consultar els detalls de validació per determinar les causes.
<i>inappropriate:signature</i>	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.
<i>indetermined:checkOptionalOutput</i>	Error	El client haurà de verificar la resposta obtinguda en l'element <i>ProcessingDetails</i> per a determinar l'error.
<i>InvalidDocumentProvided</i>	Error	El document proporcionat no és vàlid.

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

6.1.2.4. Creació de signatures i segells de temps

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

6.1.3. 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.

6.1.3.1. 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

6.1.3.2. 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: <i>{missatge excepció}</i>
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: <i>{missatge excepció}</i>

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

7. Requisits previs

Tot seguit es descriuen els requisits necessaris per a desenvolupar un client de la plataforma PSIS.

7.1. Comunicacions

Cal una connexió a Internet configurada a l'ordinador on es faci el desenvolupament, per tal de poder:

- Obtenir arxius de compilació WSDL i XSD.
- Obtenir llibreries per al desenvolupament.
- Compilar el client a partir del WSDL.
- Executar el servei de la plataforma PSIS des del client.

Cal verificar que la connexió amb la plataforma PSIS es troba disponible (garantia de que el servei està funcionant i no hi ha incidències). Per a verificar l'accés, només s'han d'introduir les adreces que s'indiquen tot seguit al navegador i verificar la resposta del servidor:

- Entorn d'integració (o preproducció):
 - <https://psis-pre.aoc.cat/psis/catcert-test/dss>
 - <https://psis-pre.aoc.cat/psis/catcert-test/dsspdf>
 - <https://psis-pre.aoc.cat/psis/catcert-test/tsp>
- Entorn d'explotació (o producció):
 - <https://psis.aoc.cat/psis/catcert/dss>
 - <https://psis.catcert.net/psis/catcert/dsspdf>
 - <https://psis.aoc.cat/psis/catcert/tsp>

Si la connexió és satisfactòria, apareixerà un missatge semblant a la figura següent:

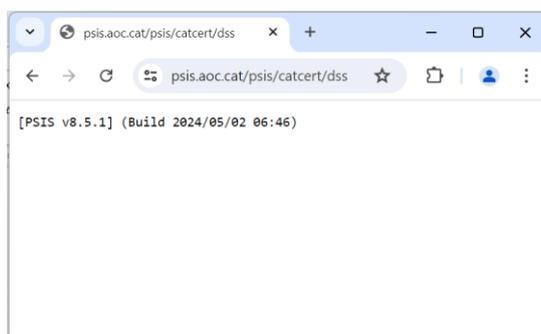


Figura 22 Captura de pantalla amb una connexió correcta a la plataforma PSIS

La plataforma PSIS es troba disponible només sota connexió segura (SSL). Això fa que s'hagin de configurar els certificats SSL a l'ordinador client per tal de poder tenir connexió un cop haguem creat el client de la plataforma.

7.2. Software

Abans de posar-se a desenvolupar el seu client, ha de conèixer quins són els requisits de *software* necessaris per al llenguatge de programació que utilitzarà.

A la taula següent es detallen aquests requisits i més endavant podrà veure algun exemple d'ús.

Tecnologia	Software necessari	Descripció / documentació / descàrrega
Java	JDK v1.5 o superior	Paquet bàsic de desenvolupament Java. <ul style="list-style-type: none"> http://java.sun.com/javase/downloads/index.jsp
	<i>Ant 1.6.2</i> (Si s'utilitza Eclipse, no és necessari descarregar-ho).	Llibreria per a la creació de <i>scripts</i> fent ús d'arxius de tipus XML. <ul style="list-style-type: none"> http://ant.apache.org/manual/install.html http://ant.apache.org/bindownload.cgi
	<i>XFire 1.2.6</i>	<i>Framework</i> per a la connexió i configuració de serveis web. <ul style="list-style-type: none"> http://repository.codehaus.org/org/codehaus/xfire/xfire-distribution/1.2.6/xfire-distribution-1.2.6.zip
C# (.NET)	<i>Microsoft (R) .NET Framework 1.1.4322.573</i> o superior (Per a poder compilar és necessari l'SDK)	Paquet bàsic per a desenvolupar i utilitzar aplicacions .NET. <ul style="list-style-type: none"> http://msdn.microsoft.com/netframework/downloads/updates/default.aspx
Visual Basic 6	<i>Microsoft Visual Basic 6 + Service Pack 6</i>	Paquet bàsic per a desenvolupar i utilitzar aplicacions Visual Basic 6. Els desenvolupaments es poden distribuir mitjançant instal·lables que copien a l'ordinador de l'usuari totes les llibreries i arxius necessaris per a la seva execució.

7.3. WSDL

Els serveis que ofereix la plataforma PSIS s'han desenvolupat facilitant l'ús d'una definició coneguda tècnicament amb el nom WSDL (*Web Service Definition Language*).

WSDL defineix tots els mètodes, interfícies i elements necessaris per a que el programador desenvolupi el codi del seu client d'una forma autònoma i gairebé automàtica si s'utilitzen eines de compilació de WSDL.

Es pot descarregar l'arxiu WSDL de la plataforma PSIS des de les següents URLs:

- Integració:
 - o <https://psis-pre.aoc.cat/wsd/dss-pre.wsd>
- Producció:
 - o <http://psis.aoc.cat/wsd/dss.wsd>

8. Creació del client

A continuació, es detallarà el procés de creació del client de la plataforma PSIS en els següents llenguatges de programació:

- Java
- .NET (C#)
- Visual Basic 6

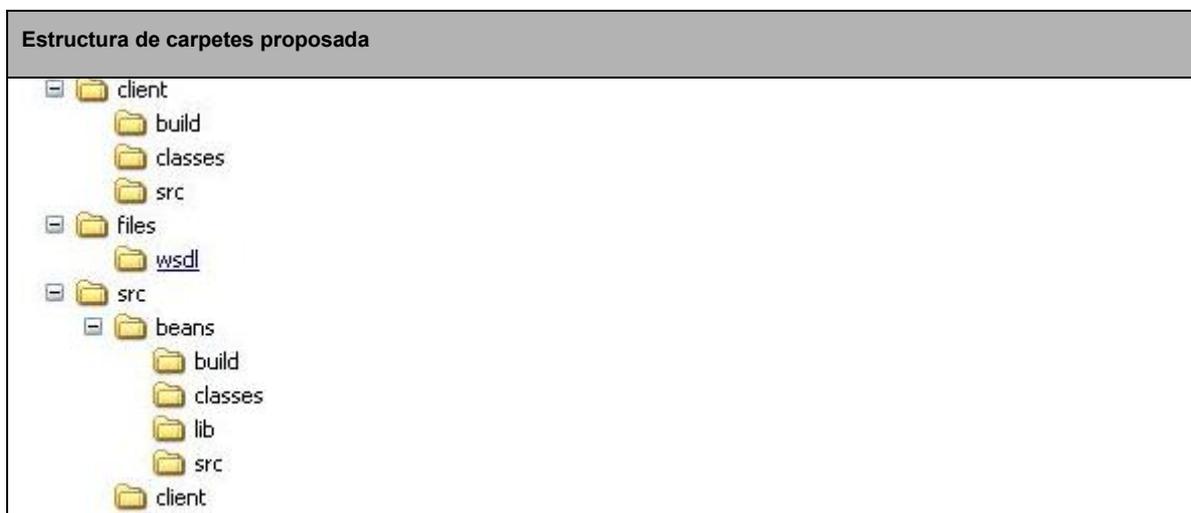
8.1. Java

Pautes a seguir per a la creació del client Java.

1. Preparació

Per a facilitar el procés de creació del client ens ajudarem de les eines que proporciona *Ant* (eina per realitzar tasques automàtiques i repetitives normalment durant la fase de compilació i generació de codi font).

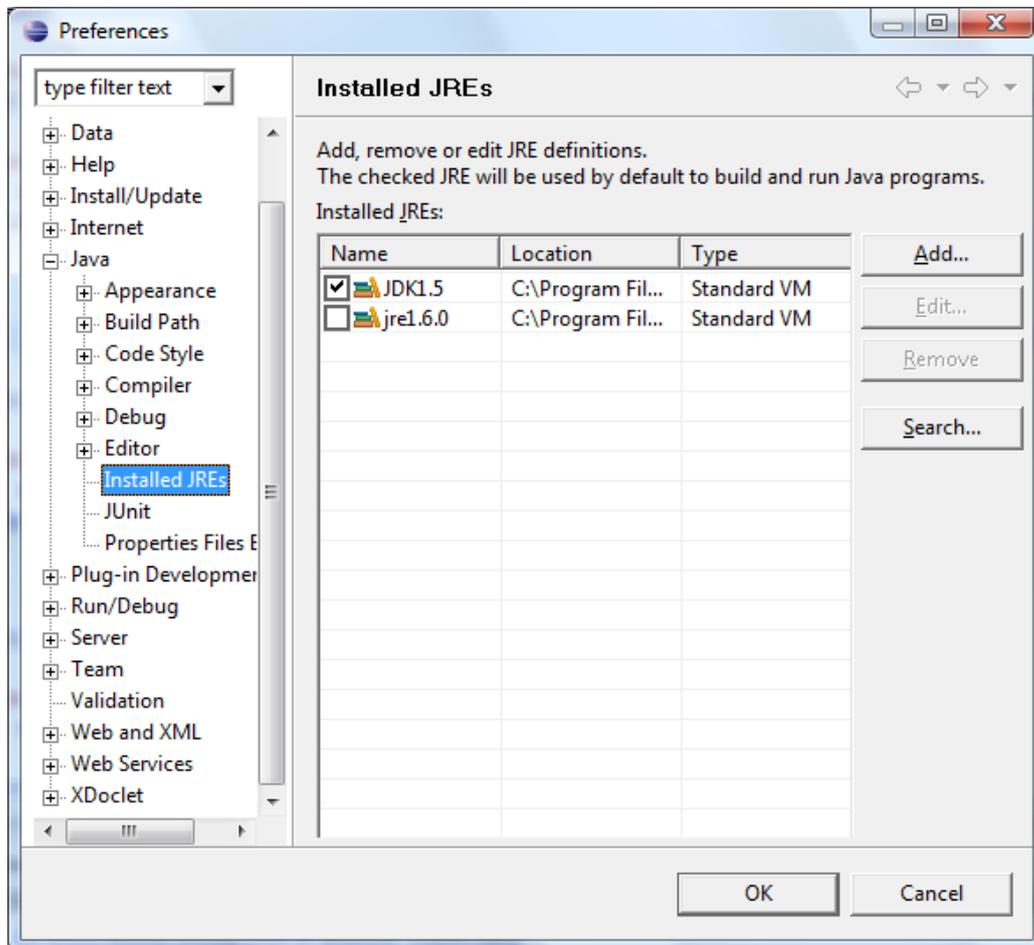
Per a configurar *Ant* proposem una estructura de carpetes, que caldrà adaptar si per necessitats del client es vol modificar.



Realitzar les següents accions:

- Copiar les llibreries contingudes dins del directori /lib del paquet Xfire (XFire 1.2.6) al directori src/beans/lib.
- Ubicar el fitxer xfire-all-1.2.6.jar, també del paquet Xfire, al directori src/beans/lib.

- Ubicar el fitxer dss.wsdl (extret de la URL indicada al punt 6.4) al director files/wsd
- Selecció del compilador de JDK (*javac.exe*) en lloc del JRE.



- Si es treballa amb Eclipse, cal que verifiquem que tenim la versió correcta de JDK afegida a les preferències. S'hi pot accedir a través del menú superior: Window > Preferences.
- Dins la finestra que s'obre, s'accedeix a Java > Installed JREs, i tenint en compte que s'hagi instal·lat prèviament el JDK 1.5, només cal que l'afegim si no hi és present. Add...

2. Generació

Es procedeix a la generació de les llibreries que utilitzarà el client per construir missatges de petició a PSIS i processar les respostes.

En primer lloc, s'ha de crear el següent arxiu d'Ant, que anomenarem **build-libs.xml**, i que s'ubicarà sota el directori arrel del projecte:

build-libs.xml

```
<project name="PSIS_LIBS" default="default" basedir=".">

  <!-- Definició de les carpetes per a poder generar els beans amb XmlBeans -->
  <property name="beans.dir" value="${basedir}/src/beans" />
  <property name="beans.lib" value="${beans.dir}/lib" />
  <property name="beans.src" value="${beans.dir}/src" />
  <property name="beans.classes" value="${beans.dir}/classes" />
  <property name="beans.build" value="${beans.dir}/build" />

  <!-- Definició de les carpetes per a poder generar el client amb Xfire -->
  <property name="client.dir" value="${basedir}/src/client" />

  <!-- Definició de l'arxiu WSDL -->
  <property name="wsdl.location" value="${basedir}/files/wsdl/dss.wsdl" />

  <!-- Definició de llibreries necessaries per a compilar els beans -->
  <path id="xmlbeans.classpath">
    <fileset dir="${beans.lib}">
      <include name="xbean-2.2.0.jar" />
      <include name="jsr173_api_1.0.jar" />
    </fileset>
  </path>
  <!-- Definició de llibreries necessaries per a compilar el wsdl -->
  <path id="wsdlgenerator.classpath">
    <fileset dir="${beans.lib}">
      <include name="*.jar" />
    </fileset>
    <fileset dir="${beans.build}">
      <include name="*.jar" />
    </fileset>
  </path>
  <!-- Definició del compilador de XMLBeans -->
  <taskdef name="scomp" classname="org.apache.xmlbeans.impl.tool.XMLBean"
classpathref="xmlbeans.classpath">
  </taskdef>

  <!-- Definició del compilador de XFire -->
  <taskdef name="wsngen" classname="org.codehaus.xfire.gen.WsGenTask"
classpathref="wsdlgenerator.classpath" />

  <!-- Tasca de compilació dels beans -->
  <target name="build-beans">
    <scomp schema="${wsdl.location}" destfile="${beans.build}/psis-beans.jar"
download="true" classpathref="xmlbeans.classpath" classgendir="${beans.classes}"
srcgendir="${beans.src}" />
  </target>

  <!-- Tasca de compilació del wsdl -->
  <target name="compile-wsdl">
    <wsngen outputDirectory="${client.dir}/src" wsdl="${wsdl.location}" overwrite="true"
binding="xmlbeans" />
  </target>
  <!-- Tasca global -->
  <target name="default" depends="build-beans,compile-wsdl" />
</project>
```

Figura 23 Contingut del fitxer ant per generar el client Java de PSIS fent servir el fitxer WSDL

Nota

Aquest fitxer està subjecte a les versions de XMLBeans i Xfire a utilitzar. En tot cas, reviseu que coincideixin amb les vostres en el punt...

```
<path id="xmlbeans.classpath">
  <fileset dir="${beans.lib}">
    <include name="xbean-2.2.0.jar" />
    <include name="jsr173_api_1.0.jar" />
  </fileset>
</path>
```

o adapteu el fitxer.

Com es pot veure, en aquest arxiu està descrit l'arbre de directoris proposat anteriorment. En el cas de que es vulgui utilitzar una estructura diferent, també s'haurà de modificar aquest document amb les noves carpetes. Cal comprovar també que les versions de les llibreries utilitzades coincideixen amb les descrites al build-libs.xml.

Un cop creat l'arxiu anterior, es procedirà a la seva execució mitjançant *Ant*. Aquesta execució té de dues tasques principals que s'han de realitzar en un ordre concret (en el cas d'utilitzar Eclipse, la compilació del build-libs.xml mitjançant Ant inclou les dues tasques, realitzades automàticament de forma consecutiva: target name="default").

La primera tasca (**build-beans**) que cal fer ens permetrà generar les classes Java que posteriorment ens ajudaran a construir els missatges d'enviament i recepció de la plataforma PSIS. Per a executar-la, escriurem la següent comanda:

Sentència

```
ant -buildfile build-libs.xml build-beans
```

I obtindrem aquest resultat:

Log de sortida per pantalla

```
Buildfile: build-libs.xml
```

```
build-beans:
```

```
[scomp] Time to build schema type system: 1.632 seconds
[scomp] Time to generate code: 2.033 seconds
[scomp] Compiling 496 source files to D:\PSIS\src\beans\classes
[scomp] Note: * uses or overrides a deprecated API.
[scomp] Note: Recompile with -Xlint:deprecation for details.
[scomp] Time to compile code: 10.856 seconds
[scomp] Building jar: D:\PSIS\src\beans\build\psis-beans.jar
```

```
BUILD SUCCESSFUL
```

```
Total time: 49 seconds
```

Observarem que, com a resultat, obtenim el fitxer **psis-beans.jar** sota el directori `src/beans/build/`. Aquest paquet conforma tot el gruix de classes que permet al client interactuar amb PSIS, i s'ha d'afegir al `classpath` del projecte..

La segona tasca (**compile-wsdl**) genera les classes Java que implementen el client de la plataforma PSIS. Per a fer-ho escriurem la següent comanda:

Sentència

```
ant -buildfile build-libs.xml compile-wsdl
```

I obtindrem aquest resultat:

Log de sortida per pantalla

```
Buildfile: build-libs.xml
```

```
compile-wsdl:
```

```
[wsgen] log4j:WARN No appenders could be found for logger  
(org.codehaus.xfire.gen.Wsdl11Generator).
```

```
[wsgen] log4j:WARN Please initialize the log4j system properly.
```

```
[wsgen] Retrieving schema at 'http://www.w3.org/TR/2002/REC-xmlldsig-core-  
20020212/xmlldsig-core-schema.xsd', relative to 'file:/D:/PSIS/files/wsdl/dss.wsdl'.
```

```
[wsgen] Retrieving schema at 'http://www.w3.org/TR/xmlldsig-core/xmlldsig-core-  
schema.xsd', relative to 'file:/D:/PSIS/files/wsdl/dss.wsdl'.
```

```
[wsgen] Retrieving schema at 'http://www.w3.org/2001/xml.xsd', relative to  
'file:/D:/PSIS/files/wsdl/dss.wsdl'.
```

```
[wsgen] Retrieving schema at 'http://docs.oasis-open.org/security/saml/v2.0/saml-schema-  
assertion-2.0.xsd', relative to 'file:/D:/PSIS/files/wsdl/dss.wsdl'.
```

```
[wsgen] Retrieving schema at 'http://www.w3.org/TR/2002/REC-xmlldsig-core-  
20020212/xmlldsig-core-schema.xsd', relative to 'http://docs.oasis-
```

```
open.org/security/saml/v2.0/saml-schema-assertion-2.0.xsd'.
```

```
[wsgen] Retrieving schema at 'http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-  
schema.xsd', relative to 'http://docs.oasis-open.org/security/saml/v2.0/saml-schema-  
assertion-2.0.xsd'.
```

```
[wsgen] Retrieving schema at 'http://www.w3.org/TR/2002/REC-xmlldsig-core-  
20020212/xmlldsig-core-schema.xsd', relative to 'http://www.w3.org/TR/2002/REC-xmlenc-core-  
20021210/xenc-schema.xsd'.
```

```
[wsgen] Retrieving schema at 'http://www.w3.org/2001/xml.xsd', relative to  
'file:/D:/PSIS/files/wsdl/dss.wsdl'.
```

```
[wsgen] Retrieving schema at 'http://www.oasis-  
open.org/committees/download.php/3408/oasis-sstc-saml-schema-protocol-1.1.xsd', relative to  
'file:/D:/PSIS/files/wsdl/dss.wsdl'.
```

```
[wsgen] Retrieving schema at 'http://www.w3.org/TR/xmlldsig-core/xmlldsig-core-  
schema.xsd', relative to 'http://www.oasis-open.org/committees/download.php/3408/oasis-sstc-  
saml-schema-protocol-1.1.xsd'.
```

```
[wsgen] Retrieving schema at 'http://www.w3.org/TR/xmlldsig-core/xmlldsig-core-  
schema.xsd', relative to 'file:/D:/PSIS/files/wsdl/dss.wsdl'.
```

```
[wsgen] oasis\names\tc\dss\1_0\core\wsdl\SOAPport.java
```

```
[wsgen] oasis\names\tc\dss\1_0\core\wsdl\digitalSignatureServiceClient.java
```

```
[wsgen] oasis\names\tc\dss\1_0\core\wsdl\digitalSignatureServiceImpl.java
```

```
BUILD SUCCESSFUL
```

```
Total time: 22 seconds
```

El resultat és un nou paquet que conforma el client de la plataforma PSIS amb les següents classes:

Packet	Classe	Descripció
oasis.names.tc.dss._1_0.core.wsd.	digitalSignatureServiceClient	Factoria de clients de la plataforma PSIS
	digitalSignatureServiceImpl	Implementació de la interfície SOAPPort
	SOAPport	Interfície de definició de mètodes de la plataforma PSIS

4. Compilació

Per a facilitar l'ús del client, s'empaquetarà el codi font del client dintre d'un arxiu JAR que posteriorment s'inclourà en el del *classpath* del nostre projecte Java. El resultat serà un fitxer **psis-client.jar**, ubicat sota *src/client/build*.

Per a fer-ho, configurarem l'arxiu *Ant* següent, anomenat **build-client.xml**, ubicat sota el directori arrel.

build-client.xml

```
<project name="PSIS_CLIENT" default="default" basedir=". ">

  <!-- Definició de les carpetes per poder generar els beans amb XmlBeans -->
  <property name="beans.dir" value="${basedir}/src/beans" />
  <property name="beans.lib" value="${beans.dir}/lib" />
  <property name="beans.build" value="${beans.dir}/build" />

  <!-- Definició de directoris per poder generar el client amb Xfire -->
  <property name="client.dir" value="${basedir}/src/client" />
  <property name="client.lib" value="${client.dir}/lib" />
  <property name="client.src" value="${client.dir}/src" />
  <property name="client.classes" value="${client.dir}/classes" />
  <property name="client.build" value="${client.dir}/build" />

  <!-- Definició de llibreries necessaries per compilar el client -->
  <path id="client.classpath">
    <fileset dir="${beans.lib}">
      <include name="*.jar" />
    </fileset>
    <fileset dir="${beans.build}">
      <include name="*.jar" />
    </fileset>
  </path>

  <!-- Tasca de compilació del client -->
  <target name="build-client">
    <mkdir dir="${client.classes}" />
    <mkdir dir="${client.build}" />
  </target>
</project>
```

```

<javac srcdir="${client.dir}/src" destdir="${client.dir}/classes"
includes="**/*.java" classpathref="client.classpath" failonerror="true" debug="true"
source="1.5" />
  <jar destfile="${client.build}/psis-client.jar" basedir="${client.dir}/classes" />
</target>

<!-- Tasca global -->
<target name="default" depends="build-client" />

</project>

```

Figura 24 Contingut del fitxer ant per compilar el client Java generat a partir del fitxer WSDL

I executarem la següent comanda:

Sentència

```
ant -buildfile build-client.xml build-client
```

Obtenint aquest resultat:

Log de sortida per pantalla

```

Buildfile: build-client.xml

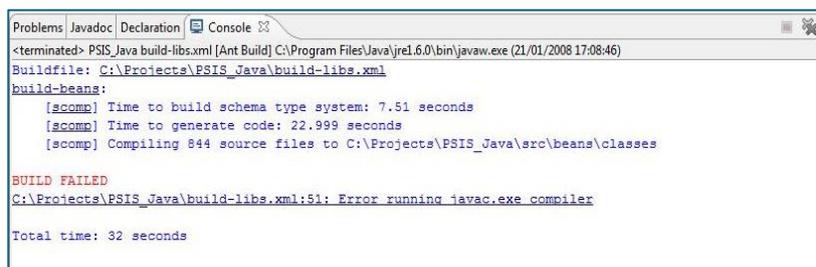
build-client:
  [javac] Compiling 3 source files to D:\PSIS\src\client\classes
  [javac] Note:
D:\PSIS\src\client\src\wsdl\core\_0\_1\dss\tc\names\oasis\digitalSignatureServiceClient.java
uses unchecked or unsafe operations.
  [javac] Note: Recompile with -Xlint:unchecked for details.
  [jar] Building jar: D:\PSIS\src\client\build\psis-client.jar

BUILD SUCCESSFUL
Total time: 2 seconds

```

Recordar que s'ha d'afegir aquest paquet al *classpath* del projecte.

Si no tenim seleccionada o instal·lada correctament la versió del JRE (JDK 1.5 o superior), l'Eclipse ens llençarà un error d'aquest tipus:



```

Problems Javadoc Declaration Console
<terminated> PSIS_Java build-libs.xml [Ant Build] C:\Program Files\Java\jre1.6.0\bin\javaw.exe (21/01/2008 17:08:46)
Buildfile: C:\Projects\PSIS_Java\build-libs.xml
build-beans:
  [scomp] Time to build schema type system: 7.51 seconds
  [scomp] Time to generate code: 22.999 seconds
  [scomp] Compiling 844 source files to C:\Projects\PSIS_Java\src\beans\classes

BUILD FAILED
C:\Projects\PSIS_Java\build-libs.xml:51: Error running javac.exe compiler

Total time: 32 seconds

```

5. Utilització

El següent exemple de codi fa una connexió a la plataforma PSIS i envia un missatge de validació buit, per comprovar la correcta integració.

Exemple de creació de la connexió amb la plataforma PSIS

```
public static void main(String args[]) throws Exception {

    // Inicialització del client
    digitalSignatureServiceClient proxy = new digitalSignatureServiceClient();

    // Indicar el servidor
    SOAPport port = proxy.getdssPortSoap("http://psisbeta.catcert.net/psis/catcert-
test/dss");

    // Composició del missatge
    VerifyRequestDocument requestDocument1 = VerifyRequestDocument.Factory.newInstance();

    // Codi de composició del missatge
    ...

    // Execució del servei per verificar
    VerifyResponseDocument responseDocument1 = port.verify(requestDocument1);

    // Codi de processat de la resposta
    ...

}
```

Figura 25 Exemple de creació de la connexió amb la plataforma PSIS en Java

Al paquet d'integradors es proporciona un joc de proves més extens, per testejar les funcionalitats bàsiques de PSIS.

Caldrà canviar el package de les classes java d'acord a l'estructura muntada segons cada implementació.

8.2. .NET (C#)

Pautes a seguir per a la creació del client .NET (C#).

1. Generació

Per a poder generar totes les classes necessàries per a fer la connexió a la plataforma PSIS s'ha d'executar la següent instrucció que generarà el codi font del client en llenguatge C#: La utilitat wsdl.exe només es compatible amb el fitxer WSDL de PSIS en la seva versió

inclosa al framework .net 1.1. Per a *clients integrant fent servir .net 2.0 el fitxer WSDL s'ha de compilar fent servir .net 1.1* i el fitxer generat si que es pot compilar fent servir .net 2.0 .

Sentència

```
wSDL /language:cs
      /namespace:net.catcert.psis
      /out:PSISClient.cs http://psisbeta.catcert.net/wSDL/dss-pre.wSDL
```

NOTA

El procés de generació dels stubs fent servir l'eina wsd.exe genera una sèrie de WARNINGS durant el procés. Aquests són totalment normals i derivats de la natura de certs dels missatges involucrats en el procés de prestació de servei de PSIS. Si no apareix cap ERROR i només apareixen WARNINGS el procés es pot considerar totalment correcte.

NOTA

S'ha indicat en el procés de generació dels stubs es fa servir la referència al servidor psisbeta. Es pot generar el client directament des de l'entorn de producció indicant la URL <http://psis.catcert.net/wSDL/dss.wSDL> i mantenint la resta de paràmetres.

NOTA

La generació del client a partir del WSDL proporcionat obliga a realitzar alguns canvis posteriors. Existeix la possibilitat d'obtenir directament el fitxer PSISClient.cs que s'inclou dins del paquet d'integració.

3. Compilació

Un cop es té el codi font generat, cal fer-ne la compilació. Aquesta compilació s'utilitzarà per a crear la llibreria (DLL) que posteriorment farem servir des d'un nou projecte de C# (.NET) o VB6.

El procés de compilació varia en funció de la màquina virtual de .NET que es tingui instal·lada a l'ordinador.

.NET SDK 1.1

```
sn -k PSISClient.snk
csc /out:PSISClient.netmodule /target:module *.cs
al /out:PSISClient.dll PSISClient.netmodule /keyFile:PSISClient.snk
```

.NET SDK 2.0

```
sn      -k PSISClient.snk
csc     /out:PSISClient.dll /t:library *.cs /keyfile:PSISClient.snk
```

NOTA

Al directori on es realitzin aquestes operacions han d'ubicar-se previament PSISClient.cs obtingut prèviament, i el Utils.cs proporcionat amb el paquet d'integració.

4. Utilització

El següent exemple de codi fa la connexió a la plataforma PSIS i envia un missatge buit. Posteriorment es veuran exemples per a poder compondre els missatges que s'enviaran.

Exemple de creació de la connexió amb la plataforma PSIS

```
private void main()
{
    // Inicialització del client
    digitalSignatureService proxy = new digitalSignatureService();

    // Indicar el servidor
    proxy.Url = http://psisbeta.catcert.net/catcert-test/dss;

    VerifyRequest requestDocument1 = new VerifyRequest();

    // Codi de composició del missatge
    ...

    // Execució del servei per a verificar
    VerifyResponse responseDocument1 = proxy.verify (requestDocument1);

    // Codi de processament de la resposta
    ...
}
```

Figura 26 Exemple de creació de la connexió amb la plataforma PSIS en .net

8.3. Visual Basic 6

El desenvolupament d'un client en Visual Basic 6 pot ser costós degut al poc suport que es disposa per a aquest llenguatge d'operacions amb *web services*. Per a facilitar el

desenvolupament, farem servir un objecte de .NET dins de Visual Basic 6 a mode de referència.

Per tant, els usuaris de Visual Basic han de seguir primer els passos de generació del client fent ús del .NET explicats en l'apartat previ.

Aquí detallarem com s'ha de registrar i desregistrar (en cas d'error) la llibreria generada en .NET i poder-ne fer ús des de Visual Basic 6.

NOTA

En el procés d'integració fent servir Visual Basic 6 s'han descrit cassos de mal funcionament dels clients generats. Aquests problemes venen derivats d'un estat inestable en el registre de sistema Windows on es desenvolupa la integració.
Es recomana fer ús d'eines de registre de Windows en cas de que aquests problemes es presentin.

1. Registre

En funció de la versió de .NET que es tingui instal·lada a l'ordinador on es faci el desenvolupament, cal fer el registre de la llibreria fent servir un procés diferent de registre per a cada cas.

Els passos recollits a continuació són per la compilació i registre de la DLL per fer servir en el VBasic en funció del .NET que s'hagi fet servir.

Aquest procés descrit registra la DLL que ha d'haver estat generada fent servir .net (amb casuístiques diferents per a llibreries compilades i generades amb .net 1.1, 2.0 o bé una combinació de les mateixes) i que es registra a Windows per tal de que els clients escrits en Visual Basic 6 en pugin fer ús.

La idea del procés és crear un embolcall en forma d'objecte COM sobre els objectes .net per tal de que Visual Basic 6 en pugui fer ús.

.NET SDK 1.1

Requisits:

La llibreria PSISClient.dll s'ha hagut de generar fent servir els passos descrits amb anterioritat en aquesta documentació.

Comanda:

```
regasm /tlb:PSISClient.tlb PSISClient.dll
gacutil /i PSISClient.dll
tlbexp PSISClient.dll
```

.NET SDK 2.0 (registre d'una llibreria generada amb .NET SDK 1.1)

Requisits:	La llibreria PSISClient.dll i l'arxiu PSISClient.netmodule s'han hagut de generar fent servir els passos descrits amb anterioritat en aquesta documentació.
Comanda:	regasm /tlb:PSISClient.tlb PSISClient.dll gacutil /i PSISClient.dll

2. Desregistrar

.NET SDK 1.1 o 2.0

Requisits:	La llibreria PSISClient.dll s'ha hagut d'instal·lar prèviament fent servir els passos indicats en els punts anteriors.
Comanda:	regasm /u PSISClient.dll

NOTA

S'adjunta el fitxer PSISClient.dll en el paquet d'integració, per si es volen obviar tots aquests passos.

3. Utilització

El següent exemple de codi fa la connexió a la plataforma PSIS i envia un missatge buit. Posteriorment es veuran exemples per a poder compondre els missatges que s'enviaran.

Exemple de creació de la connexió amb la plataforma PSIS

```
Private Sub main()

    ` Inicialització del client
    Dim proxy As New PSISClient.digitalSignatureService

    proxy.url="http://psisbeta.catcert.net/psis/catcert-test/dss"

    ` Composició del missatge
    Dim requestDocument1 As PSISClient.VerifyRequest
    Dim responseDocument1 As PSISClient.VerifyResponse
```

```

` Codi de composició del missatge
...

` Execució del servei per verificar
Set responseDocument1 = proxy.verify(requestDocument1)

` Codi de processat de la resposta
...

End Sub

```

Figura 27 Exemple de creació de la connexió amb la plataforma PSIS en .net

El següent exemple de codi realitza també la connexió a la plataforma PSIS i envia un missatge buit amb OptionalInputs, utilitzant la versió VB 9.0.

Exemple de creació de la connexió amb la plataforma PSIS amb VB 9.0

```

Private Sub main()
    'Utilitats
    Dim Utils As New net.catcert.psis.Utils
    Dim proxy As net.catcert.psis.digitalSignatureService

    proxy = New Net.catcert.psis.digitalSignatureService
    'Necessitem autenticació?
    ' proxy.Url = "https://psisbeta.catcert.net/psis/catcert-test/dss-secure" o bé
    ' proxy.Url = "https://psis.catcert.net/psis/catcert/dss"
    proxy.Url = "https://psisbeta.catcert.net/psis/catcert-test/dss-secure"

    'Indiquem un timeout de 20 segons'
    proxy.Timeout = "20000"

    Dim p12client As New X509Certificate2("psisauth.p12", "sIikZSmz")
    proxy.ClientCertificates.Add(p12client)

    'Composició del missatge
    'Preparant el SignatureOption

    'En funció de la codificació triem base64 o binari
    'certsObj(0) = Utils.Base64File(rutaFitxer)
    'certsObj(0) = Local.BinariFile(rutaFitxer)
    Dim certsObj(1)

    certsObj(0) = Local.BinariFile(rutaFitxer)

    Dim types(1) As Integer
    types(0) = Net.catcert.psis.ItemsChoiceType.X509Certificate

    Dim certificate As New Net.catcert.psis.X509DataType
    certificate.Items = certsObj
    certificate.ItemsElementName = types

    Dim other As New Net.catcert.psis.SignatureObjectTypeOther
    other.X509Data = certificate

```

```

Dim signatureType As New Net.catcert.psis.SignatureObjectType
signatureType.Item = other

'Anem a preparar els Optional Inputs
Dim OptInputsNew As New Net.catcert.psis.OptionalInputs

'Creació del missatge DSS
Dim requestDocument As New Net.catcert.psis.VerifyRequest
requestDocument.SignatureObject = signatureType
requestDocument.OptionalInputs = PreparaOptionals(OptInputsNew)
requestDocument.Profile = "urn:oasis:names:tc:dss:1.0:profiles:XSS"

'Visualització de la petició
Console.WriteLine(Utils.MessageToString(requestDocument))

'Execució del servei
Dim responseDocument As Net.catcert.psis.VerifyResponse
responseDocument = proxy.verify(requestDocument)

'Visualització de la resposta del primer optional output demanat
Presenta_Solucio(responseDocument)

End Sub

```

Figura 28 Exemple de creació de la connexió amb la plataforma PSIS en .net (VB 9.0)

9. Creació de la missatgeria

Exemples d'ús dels clients amb els tres llenguatges de programació que s'han utilitzat prèviament per a crear-los.

En aquests exemples s'utilitza un paquet anomenat *Utils* que no forma part del protocol dss ni hauria d'utilitzar-se com a punt de partida en un desenvolupament, però ens servirà d'ajuda per no repetir codis senzills en aquest document com poden ser llegir de disc.

Per tant quan es decideixi provar aquests exemples d'integració es pot optar per implementar aquestes senzilles funcions, o directament es poden demanar aquest codis per utilitzar-los en aquests exemples.

Els exemples desenvolupen les següents funcionalitats:

- Validació de certificats
- Validació de signatures en format PKCS#7 / CMS
- Validació signatures XMLDsig
- Validació signatures XAdES
- Validació de signatures PDF
- Creació de segells de temps
- Validació de segells de temps
- Validació de certificats amb autenticació de client SSL

9.1. Java

Validació de certificats

```
import java.util.Hashtable;

import org.apache.xmlbeans.XmlBase64Binary;
import org.apache.xmlbeans.XmlOptions;

import org.w3.x2000.x09.xmlldsig.X509DataDocument;
import org.w3.x2000.x09.xmlldsig.X509DataType;

import oasis.names.tc.dss._1_0.core.wsdl.SOApport;
import oasis.names.tc.dss._1_0.core.wsdl.digitalSignatureServiceClient;

import x0CoreSchema.oasisNamesTcDss1.SignatureObjectType;
import x0CoreSchema.oasisNamesTcDss1.VerifyRequestDocument;
import x0CoreSchema.oasisNamesTcDss1.VerifyResponseDocument;
import x0CoreSchema.oasisNamesTcDss1.OptionalInputsDocument.OptionalInputs;
```

```

import x0CoreSchema.oasisNamesTcDss1.SignatureObjectType.Other;
import x0CoreSchema.oasisNamesTcDss1.VerifyRequestDocument.VerifyRequest;

public class ValidacioCertificat {

    @SuppressWarnings("unchecked")
    public static void main(String args[]) throws Exception {

        // Inicialització del client
        digitalSignatureServiceClient proxy = new digitalSignatureServiceClient();
        SOAPport port = proxy.getdssPortSoap("http://psisbeta.catcert.net/psis/catcert-
test/dss");

        // Composició del missatge

        // Certificat que es verificarà
        byte[] certificate = Utils.readBase64File("certificate.dat");

        // Definició dels namespaces correctes
        Hashtable prefixes = new Hashtable();
        prefixes.put("urn:oasis:names:tc:dss:1.0:core:schema", "dss");
        prefixes.put("http://www.w3.org/2000/09/xmldsig#", "ds");

        XmlOptions options = new XmlOptions();
        options.setSaveSuggestedPrefixes(prefixes);

        // Creació del missatge DSS
        VerifyRequestDocument requestDocument =
VerifyRequestDocument.Factory.newInstance(options);

        VerifyRequest request = requestDocument.addNewVerifyRequest();
        request.setProfile("urn:oasis:names:tc:dss:1.0:profiles:XSS");

        // Creació de l'element amb el certificat a verificar
        SignatureObjectType signature = request.addNewSignatureObject();

        X509DataDocument x509doc = X509DataDocument.Factory.newInstance();
        X509DataType x509data = x509doc.addNewX509Data();

        XmlBase64Binary b64certificate = x509data.addNewX509Certificate();
        b64certificate.setByteArrayValue(certificate);

        Other any = signature.addNewOther();
        any.set(x509doc);

        signature.setOther(any);

        // Creació de l'element amb els paràmetres opcionals a consultar
        OptionalInputs optional = request.addNewOptionalInputs();
        optional.addNewReturnProcessingDetails();

        // Consulta de l'atribut X509 SubjectDN
        ReturnX509CertificateInfo info = optional.addNewReturnX509CertificateInfo();

        AttributeType SubjectDNcommonName = info.addNewAttributeDesignator();
        SubjectDNcommonName.setName("urn:oasis:names:tc:dss:1.0:profiles:XSS:certificateAttributes:S
ubjectDistinguishedName:commonName");

        // Execució del servei per verificar
        VerifyResponseDocument responseDocument = port.verify(requestDocument);
    }
}

```

```

// Visualització de la petició
System.out.println(requestDocument.xmlText(options));

// visualització de la resposta
System.out.println(responseDocument.xmlText(options));

}

}

```

Figura 29 Exemple en Java de validació de certificats

Validació de signatures PKCS#7 / CMS

```

import java.util.Hashtable;

import org.apache.xmlbeans.XmlOptions;

import oasis.names.tc.dss._1_0.core.wsdl.SOAPport;
import oasis.names.tc.dss._1_0.core.wsdl.digitalSignatureServiceClient;

import x0CoreSchema.oasisNamesTcDss1.DocumentType;
import x0CoreSchema.oasisNamesTcDss1.SignatureObjectType;
import x0CoreSchema.oasisNamesTcDss1.VerifyRequestDocument;
import x0CoreSchema.oasisNamesTcDss1.VerifyResponseDocument;
import x0CoreSchema.oasisNamesTcDss1.Base64DataDocument.Base64Data;
import x0CoreSchema.oasisNamesTcDss1.Base64SignatureDocument.Base64Signature;
import x0CoreSchema.oasisNamesTcDss1.InputDocumentsDocument.InputDocuments;
import x0CoreSchema.oasisNamesTcDss1.OptionalInputsDocument.OptionalInputs;
import x0CoreSchema.oasisNamesTcDss1.VerifyRequestDocument.VerifyRequest;

public class ValidacioSignaturaCMS {

    @SuppressWarnings("unchecked")
    public static void main(String args[]) throws Exception {

        // Inicialització del client
        digitalSignatureServiceClient proxy = new digitalSignatureServiceClient();
        SOAPport port = proxy.getdssPortSoap("http://psisbeta.catcert.net/psis/catcert-
test/dss");

        // Composició dle missatge de petició de validació de signatura PKCS#7/CMS
        // de tipus detached document amb el document complert

        // Signatura a verificar
        byte[] signature = Utils.readBase64File("cms-signature.dat");

        // Document en B64 que s'ha signat
        byte[] doc = Utils.readBase64File("cms-doc.dat");

        // Tipus de signatura
        String type = "urn:ietf:rfc:3852";

        // Definició dels namespaces correctes
        Hashtable prefixes = new Hashtable();

```

```

prefixes.put("urn:oasis:names:tc:dss:1.0:core:schema", "dss");
prefixes.put("http://www.w3.org/2000/09/xmldsig#", "ds");

XmlOptions options = new XmlOptions();
options.setSaveSuggestedPrefixes(prefixes);

// Creació del missatge DSS
VerifyRequestDocument requestDocument =
VerifyRequestDocument.Factory.newInstance(options);

VerifyRequest request = requestDocument.addNewVerifyRequest();

// Creació de l'element amb la signatura CMS a verificar
SignatureObjectType signatureType = request.addNewSignatureObject();

Base64Signature b64signature = Base64Signature.Factory.newInstance();
b64signature.setByteArrayValue(signature);
b64signature.setType(type);

signatureType.setBase64Signature(b64signature);

// Creació de l'element amb els documents a enviar
InputDocuments inpDocuments = request.addNewInputDocuments();

Base64Data b64data = Base64Data.Factory.newInstance();
b64data.setByteArrayValue(doc);

DocumentType document = inpDocuments.addNewDocument();
document.setBase64Data(b64data);

// Creació de l'element amb els paràmetres opcionals a consultar
OptionalInputs optional = request.addNewOptionalInputs();
optional.addNewReturnProcessingDetails();

// Execució del servei per verificar
VerifyResponseDocument responseDocument = port.verify(requestDocument);

// Visualització de la petició
System.out.println(requestDocument.xmlText(options));

// visualització de la resposta
System.out.println(responseDocument.xmlText(options));

}
}

```

Figura 30 Exemple en Java de validació de signatura CMS

Validació de signatures XMLDsig

```

import java.util.Hashtable;

import org.apache.xmlbeans.XmlOptions;

import oasis.names.tc.dss._1_0.core.wsdl.SOAPport;
import oasis.names.tc.dss._1_0.core.wsdl.digitalSignatureServiceClient;

```

```

import x0CoreSchema.oasisNamesTcDss1.SignatureObjectType;
import x0CoreSchema.oasisNamesTcDss1.VerifyRequestDocument;
import x0CoreSchema.oasisNamesTcDss1.VerifyResponseDocument;
import x0CoreSchema.oasisNamesTcDss1.OptionalInputsDocument.OptionalInputs;
import x0CoreSchema.oasisNamesTcDss1.VerifyRequestDocument.VerifyRequest;

public class ValidacioSignaturaXMLDsig {

    @SuppressWarnings("unchecked")
    public static void main(String args[]) throws Exception {

        // Inicialització del client
        digitalSignatureServiceClient proxy = new digitalSignatureServiceClient();
        SOAPPort port = proxy.getdssPortSoap("http://psisbeta.catcert.net/psis/catcert-
test/dss");

        // Composició del missatge

        // Validació d'una signatura xml enveloping
        String signature = Utils.readXmlFile("xmldsig-signature.dat");

        // Definició dels namespaces correctes
        Hashtable prefixes = new Hashtable();
        prefixes.put("urn:oasis:names:tc:dss:1.0:core:schema", "dss");
        prefixes.put("http://www.w3.org/2000/09/xmldsig#", "ds");

        XmlOptions options = new XmlOptions();
        options.setSaveSuggestedPrefixes(prefixes);

        // Creació del missatge DSS
        VerifyRequestDocument requestDocument =
VerifyRequestDocument.Factory.newInstance(options);

        VerifyRequest request = requestDocument.addNewVerifyRequest();

        // Creació de l'element amb la signatura XMLDsig
        SignatureObjectType signaturetype = SignatureObjectType.Factory.parse(signature,
options);

        request.setSignatureObject(signaturetype);

        // Creació de l'element amb els paràmetres opcionals a consultar
        OptionalInputs optInputs = OptionalInputs.Factory.newInstance(options);
        optInputs.addNewReturnProcessingDetails();

        request.setOptionalInputs(optInputs);

        // Execució del servei per verificar
        VerifyResponseDocument responseDocument = port.verify(requestDocument);

        // Visualització de la petició
        System.out.println(requestDocument.xmlText(options));

        // visualització de la resposta
        System.out.println(responseDocument.xmlText(options));
    }
}

```

Figura 31 Exemple en Java de validació de signatura XML

Validació de signatures XAdES

```

import java.util.Hashtable;
import org.apache.xmlbeans.XmlOptions;
import oasis.names.tc.dss._1_0.core.wsdل.SOAPport;
import oasis.names.tc.dss._1_0.core.wsdل.digitalSignatureServiceClient;
import x0CoreSchema.oasisNamesTcDss1.SignatureObjectType;
import x0CoreSchema.oasisNamesTcDss1.VerifyRequestDocument;
import x0CoreSchema.oasisNamesTcDss1.VerifyResponseDocument;
import x0CoreSchema.oasisNamesTcDss1.VerifyRequestDocument.VerifyRequest;

public class ValidacioSignaturaXAdES {

    @SuppressWarnings("unchecked")
    public static void main(String args[]) throws Exception {

        // Inicialització del client
        digitalSignatureServiceClient proxy = new digitalSignatureServiceClient();
        SOAPport port = proxy.getdssPortSoap("http://psisbeta.catcert.net/psis/catcert-
test/dss");

        // Composició del missatge

        // Validació d'una signatura xades enveloping
        String signature = Utils.readXmlFile("xades-signature.dat");

        // Definició dels namespaces correctes
        Hashtable prefixes = new Hashtable();
        prefixes.put("urn:oasis:names:tc:dss:1.0:core:schema", "dss");
        prefixes.put("http://www.w3.org/2000/09/xmldsig#", "ds");

        XmlOptions options = new XmlOptions();
        options.setSaveSuggestedPrefixes(prefixes);

        // Creació del missatge DSS
        VerifyRequestDocument requestDocument =
VerifyRequestDocument.Factory.newInstance(options);

        VerifyRequest request = requestDocument.addNewVerifyRequest();

        // Creació de l'element amb la signatura XAdES
        SignatureObjectType signaturetype = SignatureObjectType.Factory.parse(signature,
options);

        request.setSignatureObject(signaturetype);

        // Execució del servei per verificar
        VerifyResponseDocument responseDocument = port.verify(requestDocument);

        // Visualització de la petició
        System.out.println(requestDocument.xmlText(options));

        // visualització de la resposta
        System.out.println(responseDocument.xmlText(options));
    }
}

```

Figura 32 Exemple en Java de validació de signatura XAdES

Validació de documents PDF signats

```

import java.util.Hashtable;

import org.apache.xmlbeans.XmlOptions;

import oasis.names.tc.dss._1_0.core.wsdl.SOAPport;
import oasis.names.tc.dss._1_0.core.wsdl.digitalSignatureServiceClient;

import x0CoreSchema.oasisNamesTcDss1.DocumentType;
import x0CoreSchema.oasisNamesTcDss1.SignatureObjectType;
import x0CoreSchema.oasisNamesTcDss1.VerifyRequestDocument;
import x0CoreSchema.oasisNamesTcDss1.VerifyResponseDocument;
import x0CoreSchema.oasisNamesTcDss1.Base64DataDocument.Base64Data;
import x0CoreSchema.oasisNamesTcDss1.InputDocumentsDocument.InputDocuments;
import x0CoreSchema.oasisNamesTcDss1.OptionalInputsDocument.OptionalInputs;
import x0CoreSchema.oasisNamesTcDss1.VerifyRequestDocument.VerifyRequest;

public class ValidacioPDF {

    @SuppressWarnings("unchecked")
    public static void main(String args[]) throws Exception {

        //
        // !!! IMPORTANT !!!
        //
        // Inicialització del client (ATENCIÓ A LA URL: http://.../dsspdf)
        digitalSignatureServiceClient proxy = new digitalSignatureServiceClient();
        SOAPport port = proxy.getdssPortSoap("http://psisbeta.catcert.net/psis/catcert-
test/dsspdf");

        // Composició del missatge de petició de validació de signatura PDF

        // Document en B64 que s'ha signat
        byte[] doc = Uutils.readBase64File("doc.pdf");

        // Definició dels namespaces correctes
        Hashtable prefixes = new Hashtable();
        prefixes.put("urn:oasis:names:tc:dss:1.0:core:schema", "dss");
        prefixes.put("http://www.w3.org/2000/09/xmlsig#", "ds");

        XmlOptions options = new XmlOptions();
        options.setSaveSuggestedPrefixes(prefixes);

        // Creació del missatge DSS
        VerifyRequestDocument requestDocument =
VerifyRequestDocument.Factory.newInstance(options);

        VerifyRequest request = requestDocument.addNewVerifyRequest();

        //
        // !!! IMPORTANT !!!
        //
        // Activar el profile PDF
        request.setProfile("urn:oasis:names:tc:dss:1.0:profiles:DSS_PDF");

        // Creació de l'element amb els documents a enviar
        InputDocuments inpDocuments = request.addNewInputDocuments();
    
```

```

Base64Data b64data = Base64Data.Factory.newInstance();
b64data.setByteArrayValue(doc);

DocumentType document = inpDocuments.addNewDocument();
document.setBase64Data(b64data);

// Creació de l'element amb els paràmetres opcionals a consultar
OptionalInputs optional = request.addNewOptionalInputs();

// optional.addSignatureReason();

// Execució del servei per verificar
VerifyResponseDocument responseDocument = port.verify(requestDocument);

// Visualització de la petició
System.out.println(requestDocument.xmlText(options));

// visualització de la resposta
System.out.println(responseDocument.xmlText(options));

}
}

```

Figura 33 Exemple en Java de validació de documents PDF signats

Creació de segells de temps

```

import java.util.Hashtable;

import org.apache.xmlbeans.XmlAnyURI;
import org.apache.xmlbeans.XmlBase64Binary;
import org.apache.xmlbeans.XmlOptions;

import org.w3.x2000.x09.xmlldsig.DigestMethodType;
import org.w3.x2000.x09.xmlldsig.KeyInfoType;
import org.w3.x2000.x09.xmlldsig.X509DataType;

import oasis.names.tc.dss._1_0.core.wsdل.SOAPport;
import oasis.names.tc.dss._1_0.core.wsdل.digitalSignatureServiceClient;

import x0CoreSchema.oasisNamesTcDss1.SignRequestDocument;
import x0CoreSchema.oasisNamesTcDss1.SignResponseDocument;
import x0CoreSchema.oasisNamesTcDss1.DocumentHashDocument.DocumentHash;
import x0CoreSchema.oasisNamesTcDss1.IncludeObjectDocument.IncludeObject;
import x0CoreSchema.oasisNamesTcDss1.InputDocumentsDocument.InputDocuments;
import x0CoreSchema.oasisNamesTcDss1.KeySelectorDocument.KeySelector;
import x0CoreSchema.oasisNamesTcDss1.OptionalInputsDocument.OptionalInputs;
import x0CoreSchema.oasisNamesTcDss1.SignRequestDocument.SignRequest;

public class CreacioSegellDeTemps {

    @SuppressWarnings("unchecked")
    public static void main(String args[]) throws Exception {

```

```

// Inicialització del client
digitalSignatureServiceClient proxy = new digitalSignatureServiceClient();
SOAPport port = proxy.getdssPortSoap("http://psisbeta.catcert.net/psis/catcert-
test/dss");

// Composició del missatge

// Certificat amb què es generarà la signatura o timestamp
byte[] certificate = Utils.readBase64File("timestamp-certificate.dat");

// Digest
byte[] digest = Utils.readBase64File("timestamp-digest1.dat");

// Tipus de signatura disponibles
// TimeStamp amb signatura CMS/CADES:
//         urn:ietf:rfc:3161
// TimeStamp amb signatura XMLDsig:
//         oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken
// TimeStamp amb signatura XAdES:
//         oasis:names:tc:dss:1.0:core:schema:XAdESTimeStampToken
String type = "oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken";

// Definició dels namespaces correctes
Hashtable prefixes = new Hashtable();
prefixes.put("urn:oasis:names:tc:dss:1.0:core:schema", "dss");
prefixes.put("http://www.w3.org/2000/09/xmlsig#", "ds");

XmlOptions options = new XmlOptions();
options.setSaveSuggestedPrefixes(prefixes);

// Creació del missatge DSS
SignRequestDocument requestDocument = SignRequestDocument.Factory.newInstance(options);

SignRequest request = requestDocument.addNewSignRequest();
request.setProfile("urn:oasis:names:tc:dss:1.0:profiles:timestamping");

// Creació de l'element amb el document per a generar el timestamp
InputDocuments inpDocuments = InputDocuments.Factory.newInstance();

DocumentHash document = inpDocuments.addNewDocumentHash();
document.setID("Doc1");
document.setDigestValue(digest);

DigestMethodType digestMethod = document.addNewDigestMethod();
digestMethod.setAlgorithm("http://www.w3.org/2000/09/xmlsig#sha1");

request.setInputDocuments(inpDocuments);

// Creació de l'element amb els paràmetres opcionals necessaris per a
// generar el timestamp
OptionalInputs optional = request.addNewOptionalInputs();

KeySelector selector = optional.addNewKeySelector();

KeyInfoType key = selector.addNewKeyInfo();

X509DataType x509data = key.addNewX509Data();

// S'afegeix el certificat de TSA de CATCert en Base64
XmlBase64Binary b64certificate = x509data.addNewX509Certificate();

```

```

b64certificate.setByteArrayValue(certificate);

XmlAnyURI any = optional.addNewSignatureType();
any.setStringValue(type);

IncludeObject object = optional.addNewIncludeObject();
object.setObjId("Doc1");
object.setWhichDocument("Doc1");
object.setHasObjectTagsAndAttributesSet(false);
object.setCreateReference(true);

// Execució del servei per verificar
SignResponseDocument responseDocument = port.sign(requestDocument);

// Visualització de la petició
System.out.println(requestDocument.xmlText(options));

// visualització de la resposta
System.out.println(responseDocument.xmlText(options));

}
}

```

Figura 34 Exemple en Java de creació de segell de temps

Validació de segells de temps

```

import java.util.Hashtable;

import org.apache.xmlbeans.XmlOptions;

import org.w3.x2000.x09.xmlldsig.DigestMethodType;

import oasis.names.tc.dss._1_0.core.wsdl.SOAPport;
import oasis.names.tc.dss._1_0.core.wsdl.digitalSignatureServiceClient;

import x0CoreSchema.oasisNamesTcDss1.SignatureObjectType;
import x0CoreSchema.oasisNamesTcDss1.VerifyRequestDocument;
import x0CoreSchema.oasisNamesTcDss1.VerifyResponseDocument;
import x0CoreSchema.oasisNamesTcDss1.DocumentHashDocument.DocumentHash;
import x0CoreSchema.oasisNamesTcDss1.InputDocumentsDocument.InputDocuments;
import x0CoreSchema.oasisNamesTcDss1.OptionalInputsDocument.OptionalInputs;
import x0CoreSchema.oasisNamesTcDss1.VerifyRequestDocument.VerifyRequest;

public class ValidacioSegellDeTemps {

    @SuppressWarnings("unchecked")
    public static void main(String args[]) throws Exception {

        // Inicialització del client
        digitalSignatureServiceClient proxy = new digitalSignatureServiceClient();
        SOAPport port = proxy.getdssPortSoap("http://psisbeta.catcert.net/psis/catcert-
test/dss");

        // Composició del missatge

```

```

// Timestamp a verificar
String timestamp = Utils.readXmlFile("timestamp-xml.dat");

// Dades del digest
byte[] digest = Utils.readBase64File("timestamp-digest1.dat");

// Definició dels namespaces correctes
Hashtable prefixes = new Hashtable();
prefixes.put("urn:oasis:names:tc:dss:1.0:core:schema", "dss");
prefixes.put("http://www.w3.org/2000/09/xmldsig#", "ds");

XmlOptions options = new XmlOptions();
options.setSaveSuggestedPrefixes(prefixes);

// Creació del missatge DSS
VerifyRequestDocument requestDocument =
VerifyRequestDocument.Factory.newInstance(options);

VerifyRequest request = requestDocument.addNewVerifyRequest();
request.setProfile("urn:oasis:names:tc:dss:1.0:profiles:timestamping");

// Creació de l'element amb els segell de temps
SignatureObjectType signaturetype = SignatureObjectType.Factory.parse(timestamp,
options);

request.setSignatureObject(signaturetype);

// Creació de l'element amb un document
InputDocuments documents = request.addNewInputDocuments();

DocumentHash document = documents.addNewDocumentHash();
document.setID("Doc1");
document.setDigestValue(digest);

DigestMethodType method = document.addNewDigestMethod();
method.setAlgorithm("http://www.w3.org/2000/09/xmldsig#sha1");

// Creació de l'element amb els paràmetres opcionals a consultar
OptionalInputs optInputs = OptionalInputs.Factory.newInstance();
optInputs.addNewReturnProcessingDetails();

request.setOptionalInputs(optInputs);

// Execució del servei per verificar
VerifyResponseDocument responseDocument = port.verify(requestDocument);

// Visualització de la petició
System.out.println(requestDocument.xmlText(options));

// visualització de la resposta
System.out.println(responseDocument.xmlText(options));

}
}

```

Figura 35 Exemple en Java de validació de segell de temps

Validació de certificats amb autenticació SSL

```

import java.util.Hashtable;
import java.security.Security;
import org.apache.xmlbeans.XmlBase64Binary;
import org.apache.xmlbeans.XmlOptions;

import org.w3.x2000.x09.xmlldsig.X509DataDocument;
import org.w3.x2000.x09.xmlldsig.X509DataType;

import oasis.names.tc.dss._1_0.core.wsdl.SOAPport;
import oasis.names.tc.dss._1_0.core.wsdl.digitalSignatureServiceClient;

import x0CoreSchema.oasisNamesTcDss1.SignatureObjectType;
import x0CoreSchema.oasisNamesTcDss1.VerifyRequestDocument;
import x0CoreSchema.oasisNamesTcDss1.VerifyResponseDocument;
import x0CoreSchema.oasisNamesTcDss1.OptionalInputsDocument.OptionalInputs;
import x0CoreSchema.oasisNamesTcDss1.SignatureObjectType.Other;
import x0CoreSchema.oasisNamesTcDss1.VerifyRequestDocument.VerifyRequest;

public class ValidacioCertificat {

    @SuppressWarnings("unchecked")
    public static void main(String args[]) throws Exception {

        // Inicialització del client

        //configuració socket TSL

        //keystore del client

        System.setProperty("javax.net.ssl.keyStore","path_to_p12");
        System.setProperty("javax.net.ssl.keyStoreType","pkcs12");
        System.setProperty("javax.net.ssl.keyStorePassword", "password_p12");

        //trustore

        System.setProperty("javax.net.ssl.trustStore","path_to_cacerts");
        System.setProperty("javax.net.ssl.trustStoreType", "JKS");
        System.setProperty("javax.net.ssl.trustStorePassord", "changeit");

        System.setProperty("java.protocol.handler.pkgs","com.sun.net.ssl.internal.www.protocol");
        Security.addProvider(new com.sun.net.ssl.internal.ssl.Provider());

        digitalSignatureServiceClient proxy = new digitalSignatureServiceClient();
        SOAPport port = proxy.getdssPortSoap("http://psisbeta.catcert.net/psis/catcert-
test/dss");

        // Composició del missatge

        // Certificat que es verificarà
        byte[] certificate = Utils.readBase64File("certificate.dat");

        // Definició dels namespaces correctes
        Hashtable prefixes = new Hashtable();
        prefixes.put("urn:oasis:names:tc:dss:1.0:core:schema", "dss");
        prefixes.put("http://www.w3.org/2000/09/xmlldsig#", "ds");

        XmlOptions options = new XmlOptions();
    
```

```

options.setSaveSuggestedPrefixes(prefixes);

// Creació del missatge DSS
VerifyRequestDocument requestDocument =
VerifyRequestDocument.Factory.newInstance(options);

VerifyRequest request = requestDocument.addNewVerifyRequest();
request.setProfile("urn:oasis:names:tc:dss:1.0:profiles:XSS");

// Creació de l'element amb el certificat a verificar
SignatureObjectType signature = request.addNewSignatureObject();

X509DataDocument x509doc = X509DataDocument.Factory.newInstance();
X509DataType x509data = x509doc.addNewX509Data();

XmlBase64Binary b64certificate = x509data.addNewX509Certificate();
b64certificate.setByteArrayValue(certificate);

Other any = signature.addNewOther();
any.set(x509doc);

signature.setOther(any);

// Creació de l'element amb els paràmetres opcionals a consultar
OptionalInputs optional = request.addNewOptionalInputs();
optional.addNewReturnProcessingDetails();

// Consulta de l'atribut X509 SubjectDN
ReturnX509CertificateInfo info = optional.addNewReturnX509CertificateInfo();

AttributeType SubjectDNcommonName = info.addNewAttributeDesignator();
SubjectDNcommonName.setName("urn:oasis:names:tc:dss:1.0:profiles:XSS:certificateAttributes:SubjectDistinguishedName:commonName");

// Execució del servei per verificar
VerifyResponseDocument responseDocument = port.verify(requestDocument);

// Visualització de la petició
System.out.println(requestDocument.xmlText(options));

// visualització de la resposta
System.out.println(responseDocument.xmlText(options));

}

}

```

Figura 36 Exemple en Java de validació certificats amb autenticació SSL

9.2. .NET (C#)

Validació de certificats

```

using System;
using System.Web;

```

```

using net.catcert.psis;

public class ValidacioCertificat
{
    public ValidacioCertificat()
    {
    }

    static void Main()
    {
        // Utilitats
        Utils utils = new Utils();

        // Dades de prova
        byte[] certificate = utils.Base64File("c:/psis/certificate.dat");

        // Inicialització del client
        digitalSignatureService proxy = new digitalSignatureService();

        // Indicar l'adreça del servidor
        proxy.Url = "http://psisbeta.catcert.net/psis/catcert-test/dss";

        // Composició del missatge
        X509DataType x509DataType = new X509DataType();

        Object[] certificates = new Object[1];
        certificates[0] = certificate;

        ItemsChoiceType[] certificateType = new ItemsChoiceType[1];
        certificateType[0] = ItemsChoiceType.X509Certificate;

        x509DataType = new X509DataType();
        x509DataType.Items = certificates;
        x509DataType.ItemsElementName = certificateType;

        SignatureObjectTypeOther other = new SignatureObjectTypeOther();
        other.X509Data = x509DataType;

        SignatureObjectType signature = new SignatureObjectType();
        signature.Item = other;

        // Creació del missatge DSS
        VerifyRequest requestDocument = new VerifyRequest();
        requestDocument.SignatureObject = signature;

        // Execució del servei
        VerifyResponse responseDocument = proxy.verify (requestDocument);

        // Visualització de la petició
        Console.WriteLine(utils.MessageToString(requestDocument));

        // Visualització de la resposta
        Console.WriteLine(utils.MessageToString(responseDocument));
    }
}

```

Figura 37 Exemple en .net de validació de certificats

Validació de signatura PKCS#7 / CMS

```

using System;
using System.Web;
using net.catcert.psis;

public class ValidacioSignaturaCMS
{
    public ValidacioSignaturaCMS()
    {
    }

    static void Main()
    {
        // Utilitats
        Utils utils = new Utils();

        // Objectes temporals
        Object[] objects = null;
        ItemsChoiceType6[] types6 = null;

        // Inicialització del client
        digitalSignatureService proxy = new digitalSignatureService();

        // Indicar l'adreça del servidor
        proxy.Url = "http://psisbeta.catcert.net/psis/catcert-test/dss";

        // Composició del missatge

        // Dades de prova
        byte[] signature = utils.Base64File("c:/psis/cms-signature.dat");
        byte[] doc = utils.Base64File("c:/psis/cms-doc.dat");

        // Creació de l'element amb la signatura CMS a verificar
        Base64Signature b64signature = new Base64Signature();
        b64signature.Type = "urn:ietf:rfc:3852";
        b64signature.Value = signature;

        SignatureObjectType signatureType = new SignatureObjectType();
        signatureType.Item = b64signature;

        // Creació de l'element amb els documents a enviar
        Base64Data b64data = new Base64Data();
        b64data.Value = doc;

        DocumentType[] document = new DocumentType[1];
        document[0] = new DocumentType();
        document[0].Item = b64data;

        InputDocuments inpDocuments = new InputDocuments();
        inpDocuments.Items = document;

        // Creació de l'element amb els paràmetres opcionals a consultar
        OptionalInputs optInputs = new OptionalInputs();

        objects = new Object[1];
    }
}

```

```

objects[0] = new Object();

types6 = new ItemsChoiceType6[1];
types6[0] = ItemsChoiceType6.ReturnProcessingDetails;

optInputs.Items = objects;
optInputs.ItemsElementName = types6;

// Creació del missatge DSS
VerifyRequest requestDocument = new VerifyRequest();
requestDocument.SignatureObject = signatureType;
requestDocument.InputDocuments = inpDocuments;
requestDocument.OptionalInputs = optInputs;

// Execució del servei
VerifyResponse responseDocument = proxy.verify(requestDocument);

// Visualització de la petició
Console.WriteLine(utils.MessageToString(requestDocument));

// Visualització de la resposta
Console.WriteLine(utils.MessageToString(responseDocument));

}
}

```

Figura 38 Exemple en .net de validació de signatura CMS

Validació de signatura XMLDsig

```

using System;
using System.Web;
using net.catcert.psis;

public class ValidacioSignaturaXMLDsig
{
    public ValidacioSignaturaXMLDsig()
    {
    }

    static void Main()
    {
        // Utilitats
        Utils utils = new Utils();

        // Objectes temporals
        Object[] objects=null;
        ItemsChoiceType7[] types7 = null;

        // Inicialització del client
        digitalSignatureService proxy = new digitalSignatureService();

        // Indicar l'adreça del servidor
        proxy.Url = "http://psisbeta.catcert.net/psis/catcert-test/dss";
    }
}

```

```

// Composició del missatge

// Dades de prova
System.Xml.XmlElement signature = utils.XMLFile("c:/psis/xmldsig-signature.dat");

// Creació de l'element amb la signatura XMLDsig
SignatureObjectType signaturetype = new SignatureObjectType();
signaturetype.Any = signature;

// Creació de l'element amb els paràmetres opcionals a consultar
OptionalInputs optInputs = new OptionalInputs();

objects = new Object[1];
objects[0] = new Object();

types7 = new ItemsChoiceType7[1];
types7[0] = ItemsChoiceType7.ReturnProcessingDetails;

optInputs.Items = objects;
optInputs.ItemsElementName = types7;

// Creació del missatge DSS
VerifyRequest requestDocument = new VerifyRequest();
requestDocument.SignatureObject = signaturetype;
requestDocument.OptionalInputs = optInputs;

// Execució del servei per a verificar
VerifyResponse responseDocument = proxy.verify (requestDocument);

// Visualització de la petició
Console.WriteLine(utils.MessageToString(requestDocument));

// Visualització de la resposta
Console.WriteLine(utils.MessageToString(responseDocument));

}
}

```

Figura 39 Exemple en .net de validació de signatura XML

Validació de signatura XAdES

```

using System;
using System.Web;
using net.catcert.psis;

public class ValidacioSignaturaXAdES
{
    public ValidacioSignaturaXAdES ()
    {
    }

    static void Main()

```

```

{

    // Utilitats
    Utils utils = new Utils();

    // Objectes temporals
    Object[] objects = null;
    ItemsChoiceType6[] types6 = null;

    // Inicialització del client
    digitalSignatureService proxy = new digitalSignatureService();

    // Indicar l'adreça del servidor
    proxy.Url = "http://psisbeta.catcert.net/psis/catcert-test/dss";

    // Codi de composició del missatge

    // Dades de prova
    System.Xml.XmlElement signature = utils.XMLFile("c:/psis/xades-signature.dat");

    // Creació de l'element amb la signatura XMLDsig
    SignatureObjectType signaturetype = new SignatureObjectType();
    signaturetype.Any = signature;

    // Creació de l'element amb els paràmetres opcionals a consultar
    OptionalInputs optInputs = new OptionalInputs();

    objects = new Object[1];
    objects[0] = new Object();

    types6 = new ItemsChoiceType6[1];
    types6[0] = ItemsChoiceType6.ReturnProcessingDetails;

    optInputs.Items = objects;
    optInputs.ItemsElementName = types6;

    // Creació del missatge DSS
    VerifyRequest requestDocument = new VerifyRequest();
    requestDocument.SignatureObject = signaturetype;
    requestDocument.OptionalInputs = optInputs;

    // Execució del servei per a verificar
    VerifyResponse responseDocument = proxy.verify(requestDocument);

    // Visualització de la petició
    Console.WriteLine(utils.MessageToString(requestDocument));

    // Visualització de la resposta
    Console.WriteLine(utils.MessageToString(responseDocument));

}
}

```

Figura 40 Exemple en .net de validació de signatura XAdES

Validació de document PDF signat

```

using System;
using System.Web;

using net.catcert.psis;

public class ValidacioPDF
{
    public ValidacioPDF()
    {
    }

    static void Main()
    {
        // Utilitats
        Utils utils = new Utils();

        // Objectes temporals
        Object[] objects=null;
        ItemsChoiceType7[] types7 = null;

        // Inicialització del client
        digitalSignatureService proxy = new digitalSignatureService();

        // Indicar l'adreça del servidor
        //
        // ATENCIO: http://.../dsspdf
        //
        proxy.Url = "http://psisbeta.catcert.net/psis/catcert-test/dsspdf";

        // Codi de composició del missatge

        // Document PDF a validar
        byte[] doc = utils.Base64File("c:/psis/doc.pdf");

        // Creació de l'element amb els documents a enviar
        Base64Data b64data = new Base64Data();
        b64data.Value = doc;

        DocumentType[] document = new DocumentType[1];
        document[0] = new DocumentType();
        document[0].Item = b64data;

        InputDocuments inpDocuments = new InputDocuments();
        inpDocuments.Items = document;

        // Creació de l'element amb els paràmetres opcionals a consultar
        OptionalInputs optInputs = new OptionalInputs();

        objects = new object[2];
        objects[0] = new Object();
        objects[1] = new Object();

        types7 = new ItemsChoiceType7[2];
        types7[0] = ItemsChoiceType7.ReturnProcessingDetails;
    }
}

```

```

types7[1] = ItemsChoiceType7.ReturnSignatureReason;

optInputs.Items = objects;
optInputs.ItemsElementName = types7;

// Creació del missatge DSS
VerifyRequest requestDocument = new VerifyRequest();
requestDocument.InputDocuments = inpDocuments;
requestDocument.OptionalInputs = optInputs;

//
// !!! IMPORTANT !!!
//
// Activar perfil PDF
//
requestDocument.Profile = "urn:oasis:names:tc:dss:1.0:profiles:DSS_PDF";

// Execució del servei per a verificar
VerifyResponse responseDocument = proxy.verify (requestDocument);

// Visualització de la petició
Console.WriteLine(utils.MessageToString(requestDocument));

// Visualització de la resposta
Console.WriteLine(utils.MessageToString(responseDocument));

}
}

```

Figura 41 Exemple en .net de validació de document PDF signat

Creació de segells de temps

```

using System;
using System.Web;

using net.catcert.psis;

public class CreacioSegellDeTemps
{
    public CreacioSegellDeTemps()
    {
    }

    static void Main()
    {
        // Utilitats
        Utils utils = new Utils();

        // Objectes temporals
        Object[] objects = null;
        ItemsChoiceType[] types = null;
        ItemsChoiceType1[] types1 = null;
        ItemsChoiceType6[] types6 = null;
    }
}

```

```

// Inicialització del client
digitalSignatureService proxy = new digitalSignatureService();

// Indicar l'adreça del servidor
proxy.Url = "http://psisbeta.catcert.net/psis/catcert-test/dss";

// Codi de composició del missatge

// Dades de prova
byte[] certificate = utils.Base64File("c:/psis/timestamp-certificate.dat");
byte[] digest = utils.Base64File("c:/psis/timestamp-digest1.dat");

// Tipus de signatura disponibles
// TimeStamp amb signatura CMS/CAdes:      urn:ietf:rfc:3161
// TimeStamp amb signatura XMLDsig:
oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken
// TimeStamp amb signatura XAdES:
oasis:names:tc:dss:1.0:core:schema:XAdESTimeStampToken
string signatureType = "oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken";

// Creació de l'element amb un document
DigestMethodType method = new DigestMethodType();
method.Algorithm = "http://www.w3.org/2000/09/xmlsig#sha1";

DocumentHash document = new DocumentHash();
document.ID = "Doc1";
document.DigestMethod = method;
document.DigestValue = digest;

// Creació de l'element amb els documents a signar
InputDocuments documents = new InputDocuments();
documents.Items = new DocumentHash[1] { document };

// Creació de l'element amb un certificat
objects = new Object[1];
objects[0] = certificate;

types = new ItemsChoiceType[1];
types[0] = ItemsChoiceType.X509Certificate;

X509DataType x509DataType = new X509DataType();
x509DataType.Items = objects;
x509DataType.ItemsElementName = types;

// Creació de l'element opcional amb el certificat per fer el segell de temps
// Contindrà el certificat de TSA de CATCert en Base64
objects = new Object[1];
objects[0] = x509DataType;

types1 = new ItemsChoiceType1[1];
types1[0] = ItemsChoiceType1.X509Data;

KeyInfoType keyInfo = new KeyInfoType();
keyInfo.Items = objects;
keyInfo.ItemsElementName = types1;

KeySelector keySelector = new KeySelector();
keySelector.Item = keyInfo;

```

```

// Creació de l'element opcional amb l'objecte
IncludeObject iObject = new IncludeObject();
iObject.ObjId = "Doc1";
iObject.WhichDocument = "Doc1";
iObject.hasObjectTagsAndAttributesSet = false;
iObject.createReference = true;

// Creació de l'element amb el conjunt de paràmetres opcionals a consultar
objects = new Object[3];
objects[0] = keySelector;
objects[1] = signatureType;
objects[2] = iObject;

types6 = new ItemsChoiceType6[3];
types6[0] = ItemsChoiceType6.KeySelector;
types6[1] = ItemsChoiceType6.SignatureType;
types6[2] = ItemsChoiceType6.IncludeObject;

OptionalInputs optInputs = new OptionalInputs();
optInputs.Items = objects;
optInputs.ItemsElementName = types6;

// Creació del missatge DSS
SignRequest requestDocument = new SignRequest();
requestDocument.OptionalInputs = optInputs;
requestDocument.InputDocuments = documents;

// Execució del servei per a verificar
SignResponse responseDocument = proxy.sign(requestDocument);

// Visualització de la petició
Console.WriteLine(utils.MessageToString(requestDocument));

// Visualització de la resposta
Console.WriteLine(utils.MessageToString(responseDocument));

}
}

```

Figura 42 Exemple en .net de creació de segell de temps

Validació de segells de temps

```

using System;
using System.Web;

using net.catcert.psis;

public class ValidacioSegellDeTemps
{
    public ValidacioSegellDeTemps()
    {
    }
}

```

```

static void Main()
{

    // Utilitats
    Utils utils = new Utils();

    // Objectes temporals
    Object[] objects=null;
    ItemsChoiceType6[] types6 = null;

    // Inicialització del client
    digitalSignatureService proxy = new digitalSignatureService();

    // Indicar l'adreça del servidor
    proxy.Url = "http://psisbeta.catcert.net/psis/catcert-test/dss";

    // Composició del missatge

    // Dades de prova
    System.Xml.XmlElement timestamp = utils.XMLFile("c:/psis/timestamp-xml.dat");

    byte[] digest = utils.Base64File("c:/psis/timestamp-digest1.dat");

    // Creació de l'element amb un document
    DigestMethodType method = new DigestMethodType();
    method.Algorithm="http://www.w3.org/2000/09/xmlsig#sha1";

    DocumentHash document = new DocumentHash();
    document.ID = "Doc1";
    document.DigestMethod = method;
    document.DigestValue = digest;

    // Creació de l'element amb els documents a verificar
    InputDocuments documents = new InputDocuments();
    documents.Items = new DocumentHash[1] {document};

    // Creació de l'element amb el segell de temps
    SignatureObjectType signaturetype = new SignatureObjectType();
    signaturetype.Any=timestamp;

    // Creació de l'element amb els paràmetres opcionals a consultar
    OptionalInputs optInputs = new OptionalInputs();

    objects = new Object[1];
    objects[0] = new Object();

    types6 = new ItemsChoiceType6[1];
    types6[0] = ItemsChoiceType6.ReturnProcessingDetails;

    optInputs.Items = objects;
    optInputs.ItemsElementName = types6;

    // Creació del missatge DSS
    VerifyRequest requestDocument = new VerifyRequest();
    requestDocument.SignatureObject = signaturetype;
    requestDocument.OptionalInputs = optInputs;
    requestDocument.InputDocuments = documents;

    // Execució del servei per a verificar

```

```

VerifyResponse responseDocument = proxy.verify (requestDocument);

// Visualització de la petició
Console.WriteLine(utils.MessageToString(requestDocument));

// Visualització de la resposta
Console.WriteLine(utils.MessageToString(responseDocument));

}
}

```

Figura 43 Exemple en .net de validació de segell de temps

Validació de certificats amb autenticació SSL

```

using System;
using System.Web;
using System.Security;
using System.Security.Cryptography.X509Certificates;

using net.catcert.psis;

public class ValidacioCertificat
{
    public ValidacioCertificat()
    {
    }

    static void Main()
    {
        // Utilitats
        Utils utils = new Utils();

        //Keystore client
        X509Certificate2 p12client = null;
        p12client = new X509Certificate2("path_to_p12", "password_p12");

        // Dades de prova
        byte[] certificate = utils.Base64File("c:/psis/certificate.dat");

        // Inicialització del client
        digitalSignatureService proxy = new digitalSignatureService();

        // Indicar l'adreça del servidor
        proxy.Url = "http://psisbeta.catcert.net/psis/catcert-test/dss";
        proxy.ClientCertificates.Add(p12client);

        // Composició del missatge
        X509DataType x509DataType = new X509DataType();

        Object[] certificates = new Object[1];
        certificates[0] = certificate;
    }
}

```

```

ItemsChoiceType[] certificateType = new ItemsChoiceType[1];
certificateType[0] = ItemsChoiceType.X509Certificate;

x509DataType = new X509DataType();
x509DataType.Items = certificates;
x509DataType.ItemsElementName = certificateType;

SignatureObjectTypeOther other = new SignatureObjectTypeOther();
other.X509Data = x509DataType;

SignatureObjectType signature = new SignatureObjectType();
signature.Item = other;

// Creació del missatge DSS
VerifyRequest requestDocument = new VerifyRequest();
requestDocument.SignatureObject = signature;

// Execució del servei
VerifyResponse responseDocument = proxy.verify (requestDocument);

// Visualització de la petició
Console.WriteLine(utils.MessageToString(requestDocument));

// Visualització de la resposta
Console.WriteLine(utils.MessageToString(responseDocument));

}
}

```

Figura 44 Exemple en .net de validació de segell de temps

9.3. Visual Basic 6

Validació de certificats

```

Public Sub Main()

    'Utilitats
    Set Utils = New PSISClient.Utils

    'Inicialització del client
    Dim proxy As New PSISClient.digitalSignatureService
    proxy.url = "http://psisbeta.catcert.net/psis/catcert-test/dss"

    'Composició del missatge
    Dim certsObj(1)
    certsObj(0) = Utils.Base64File("c:/psis/certificate.dat")

    Dim types(1) As Integer
    types(0) = ItemsChoiceType.ItemsChoiceType_X509Certificate

    Dim certificate As New X509DataType
    certificate.Items = certsObj
    certificate.ItemsElementName = types

```

```

Dim other As New SignatureObjectTypeOther
other.X509Data = certificate

Dim signatureType As New SignatureObjectType
signatureType.Item = other

'Creació del missatge DSS
Dim requestDocument As New PSISClient.VerifyRequest
requestDocument.SignatureObject = signatureType

'Execució del servei
Dim responseDocument As PSISClient.VerifyResponse
Set responseDocument = proxy.verify(requestDocument)

'Visualització de la petició
Debug.Print Utils.MessageToString(requestDocument)

'Visualització de la resposta
Debug.Print Utils.MessageToString(responseDocument)

End Sub

```

Figura 45 Exemple en Visual Basic de validació de certificats

Validació de signatura PKCS#7 / CMS

```

Public Sub Main()

    'Utilitats
    Set Utils = New PSISClient.Utils

    'Inicialització del client
    Dim proxy As New PSISClient.digitalSignatureService
    proxy.url = "http://psisbeta.catcert.net/psis/catcert-test/dss"

    'Codi de composició del missatge

    'Creació de l'element amb la signatura CMS a verificar
    Dim signature As New PSISClient.Base64Signature
    signature.Type = "urn:ietf:rfc:3852"
    signature.Value = Utils.Base64File("c:/psis/cms-signature.dat")

    Dim sign As New PSISClient.SignatureObjectType
    Set sign.Item = signature

    'Documents a enviar
    Dim data As New PSISClient.Base64Data
    data.Value = Utils.Base64File("c:/psis/cms-doc.dat")

    Dim docType(1) As PSISClient.DocumentType
    Set docType(0) = New PSISClient.DocumentType
    Set docType(0).Item = data

    Dim clearText As New PSISClient.InputDocuments
    clearText.Items = docType

```

```

'Creació de l'element amb els paràmetres opcionals a consultar
Dim optInputs As PSISClient.OptionalInputs
Set optInputs = New PSISClient.OptionalInputs

Dim objects(1) As Object
Dim type7(1) As Long

Set objects(0) = New ObjectType
type7(0) = PSISClient.ItemsChoiceType7_ReturnProcessingDetails

optInputs.Items = objects
optInputs.ItemsElementName = type7

'Creació del missatge DSS
Dim requestDocument As New PSISClient.VerifyRequest
Set requestDocument.SignatureObject = sign
Set requestDocument.InputDocuments = clearText
Set requestDocument.OptionalInputs = optInputs

'Execució del servei per verificar
Dim responseDocument As PSISClient.VerifyResponse
Set responseDocument = proxy.verify(requestDocument)

'Visualització de la petició
Debug.Print Utils.MessageToString(requestDocument)

'Visualització de la resposta
Debug.Print Utils.MessageToString(responseDocument)

End Sub

```

Figura 46 Exemple en Visual Basic de signatura CMS

Validació de signatura XMLDsig
<pre> Private Sub main() 'Utilitats Set Utils = New PSISClient.Utils 'Inicialització del client Dim proxy As New PSISClient.digitalSignatureService proxy.url = "http://psisbeta.catcert.net/psis/catcert-test/dss" 'Composició del missatge 'Creació de l'element amb la signatura XMLDsig Dim signatureType As New SignatureObjectType signatureType.Any = Utils.XMLFile("c:/psis/xmldsig-signature.dat") 'Creació de l'element amb els paràmetres opcionals a consultar Dim optInputs As New OptionalInputs Dim types7(1) As Long types7(0) = ItemsChoiceType7.ItemsChoiceType7_ReturnProcessingDetails </pre>

```

Dim objInputs(1)
Set objInputs(0) = New ObjectType

optInputs.Items = objInputs
optInputs.ItemsElementName = types7

'Creació del missatge DSS
Dim requestDocument As New PSISClient.VerifyRequest
requestDocument.SignatureObject = signatureType
requestDocument.OptionalInputs = optInputs

'Execució del servei per verificar
Set responseDocument = proxy.verify(requestDocument)

'Visualització de la petició
Debug.Print Utils.MessageToString(requestDocument)

'Visualització de la resposta
Debug.Print Utils.MessageToString(responseDocument)

End Sub

```

Figura 47 Exemple en Visual Basic de signatura XML

Validació de signatura XAdES

```

Private Sub main()

'Utilitats
Set Utils = New PSISClient.Utils

'Inicialització del client
Dim proxy As New PSISClient.digitalSignatureService
proxy.url = "http://psisbeta.catcert.net/psis/catcert-test/dss"

'Composició del missatge

'Creació de l'element amb la signatura XMLDsig
Dim signatureType As New SignatureObjectType
signatureType.Any = Utils.XMLFile("c:/psis/xades-signature.dat")

'Creació de l'element amb els paràmetres opcionals a consultar
Dim optInputs As New OptionalInputs

Dim types7(1) As Long
types7(0) = ItemsChoiceType7.ItemsChoiceType7_ReturnProcessingDetails

Dim objInputs(1)
Set objInputs(0) = New ObjectType

optInputs.Items = objInputs
optInputs.ItemsElementName = types7

'Creació del missatge DSS
Dim requestDocument As New PSISClient.VerifyRequest
requestDocument.SignatureObject = signatureType

```

```

requestDocument.OptionalInputs = optInputs

'Execució del servei per verificar
Set responseDocument = proxy.verify(requestDocument)

'Visualització de la petició
Debug.Print Utils.MessageToString(requestDocument)

'Visualització de la resposta
Debug.Print Utils.MessageToString(responseDocument)

End Sub

```

Figura 48 Exemple en Visual Basic de signatura XAdES

Validació de document PDF signat

```

Private Sub Main()

'Utilitats
Set Utils = New PSISClient.Utils

'Inicialització del client. Atenció a la URL (http://.../dsspdf
Dim proxy As New PSISClient.digitalSignatureService
proxy.url = "http://psisbeta.catcert.net/psis/catcert-test/dsspdf"

'Codi de composició del missatge

'Documentos a enviar
Dim data As New PSISClient.Base64Data
data.Value = Utils.Base64File("c:/psis/doc.pdf")

Dim docType(1) As PSISClient.DocumentType
Set docType(0) = New PSISClient.DocumentType
Set docType(0).Item = data

Dim clearText As New PSISClient.InputDocuments
clearText.Items = docType

'Creació de l'element amb els paràmetres opcionals a consultar
Dim optInputs As PSISClient.OptionalInputs
Set optInputs = New PSISClient.OptionalInputs

Dim objects(2) As Object
Dim type7(2) As Long

Set objects(0) = New ObjectType
type7(0) = PSISClient.ItemsChoiceType7_ReturnProcessingDetails

Set objects(1) = New ObjectType
type7(1) = PSISClient.ItemsChoiceType7_ReturnSignatureReason

optInputs.Items = objects
optInputs.ItemsElementName = type7

'Creació del missatge DSS

```

```

Dim requestDocument As New PSISClient.VerifyRequest
Set requestDocument.InputDocuments = clearText
Set requestDocument.OptionalInputs = optInputs

'!!! IMPORTANT !!!
'
'Activar perfil PDF
request.Profile = "urn:oasis:names:tc:dss:1.0:profiles:DSS_PDF"

'Execució del servei per verificar
Set responseDocument = proxy.verify(requestDocument)

'Visualització de la petició
Debug.Print Utils.MessageToString(requestDocument)

'Visualització de la resposta
Debug.Print Utils.MessageToString(responseDocument)

End Sub

```

Figura 49 Exemple en Visual Basic de document PDF signat

Creació de segells de temps

```

Private Sub main()

'Utilitats
Set Utils = New PSISClient.Utils

'Tipus de signatura disponibles
'TimeStamp amb signatura CMS/CAdes:   urn:ietf:rfc:3161
'TimeStamp amb signatura XMLDsig:     oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken
'TimeStamp amb signatura XAdES:
oasis:names:tc:dss:1.0:core:schema:XAdESTimeStampToken
Dim signatureType As String
signatureType = "oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken"

'Inicialització del client
Dim proxy As New PSISClient.digitalSignatureService
proxy.url = "http://psisbeta.catcert.net/psis/catcert-test/dss"

'Codi de composició del missatge

'Creació de l'element amb un document
Dim method As New DigestMethodType
method.Algorithm = "http://www.w3.org/2000/09/xmlsig#sha1"

Dim document(1) As DocumentHash
Set document(0) = New DocumentHash
document(0).ID = "Doc1"
document(0).digestMethod = method
document(0).DigestValue = Utils.Base64File("c:/psis/timestamp-digest1.dat")

'Creació de l'element amb els documents a signar
Dim documents As New InputDocuments
documents.Items = document

```

```

'Creació de l'element amb un certificat
Dim certificats(1)
certificats(0) = Utils.Base64File("c:/psis/timestamp-certificate.dat")

Dim types(1) As Long
types(0) = ItemsChoiceType.ItemsChoiceType_X509Certificate

Dim certData As New X509DataType
certData.Items = certificats
certData.ItemsElementName = types

'Creació de l'element opcional amb el certificat per fer el segell de temps
Dim dataObject(1) As Object
Set dataObject(0) = certData

Dim types1(1) As Long
types1(0) = ItemsChoiceType1.ItemsChoiceType1_X509Data

Dim keyInfo As New KeyInfoType
keyInfo.Items = dataObject
keyInfo.ItemsElementName = types1

Dim keySlt As New KeySelector
Set keySlt.Item = keyInfo

'Creació de l'element amb el conjunt de paràmetres opcionals a consultar
Dim optObjects(2)
Set optObjects(0) = keySlt
optObjects(1) = signatureType
optObjects(2) = iObject

Dim types7(2) As Long
types7(0) = ItemsChoiceType7.ItemsChoiceType7_KeySelector
types7(1) = ItemsChoiceType7.ItemsChoiceType7_SignatureType

Dim optInputs As New OptionalInputs
optInputs.Items = optObjects
optInputs.ItemsElementName = types7

'Creació del missatge DSS
Dim requestDocument As New PSISClient.SignRequest
Set requestDocument.InputDocuments = documents
Set requestDocument.OptionalInputs = optInputs

'Execució del servei per signar
Set responseDocument = proxy.sign(requestDocument)

'Visualització de la petició
Debug.Print Utils.MessageToString(requestDocument)

'Visualització de la resposta
Debug.Print Utils.MessageToString(responseDocument)

End Sub

```

Figura 50 Exemple en Visual Basic de creació de segell de temps

Validació de segells de temps

```

Private Sub main()
    'Utilitats
    Set Utils = New PSISClient.Utils

    'Inicialització del client
    Dim proxy As New PSISClient.digitalSignatureService
    proxy.url = "http://psisbeta.catcert.net/psis/catcert-test/dss"

    'Composició del missatge

    'Creació de l'element amb un document
    Dim method As New DigestMethodType
    method.Algorithm = "http://www.w3.org/2000/09/xmlsig#sha1"

    Dim document(1) As DocumentHash
    Set document(0) = New DocumentHash
    document(0).ID = "Doc1"
    document(0).digestMethod = method
    document(0).DigestValue = Utils.Base64File("c:/psis/timestamp-digest1.dat")

    'Creació de l'element amb els documents a verificar
    Dim documents As New InputDocuments
    documents.Items = document

    ' Creació de l'element amb el segell de temps
    Dim signatureType As New SignatureObjectType
    signatureType.Any = Utils.XMLFile("c:/psis/timestamp-xml.dat")

    'Creació de l'element amb els paràmetres opcionals a consultar
    Dim optInputs As New OptionalInputs

    Dim types7(1) As Long
    types7(0) = ItemsChoiceType7.ItemsChoiceType7_ReturnProcessingDetails

    Dim objInputs(1)
    Set objInputs(0) = New ObjectType

    optInputs.Items = objInputs
    optInputs.ItemsElementName = types7

    'Creació del missatge DSS
    Dim requestDocument As New PSISClient.VerifyRequest
    requestDocument.SignatureObject = signatureType
    requestDocument.OptionalInputs = optInputs
    requestDocument.InputDocuments = documents

    'Execució del servei per verificar
    Set responseDocument = proxy.verify(requestDocument)

    'Visualització de la petició
    Debug.Print Utils.MessageToString(requestDocument)

    'Visualització de la resposta
    Debug.Print Utils.MessageToString(responseDocument)

End Sub

```

Figura 51 Exemple en Visual Basic de creació de segell de temps

10. Annexes

10.1. Referències

Fitxer	Títol
dss-v1[1].0-spec-cd-Core-r03.pdf	<i>Digital Signature Service Core Protocols, Elements, and Bindings</i>
OASIS-dss-1.0-core-profiles-XSS-spec-wd02.doc	<i>eXtended Signature Services (XSS) Profile of the OASIS Digital Signature Service (DSS)</i>

URL	Descripció
http://www.OASIS-open.org/committees/tc_home.php?wg_abbrev=dss	Pàgina web oficial d'estandardització del protocol DSS
http://www.webservices.org/	Pàgina web d'informació general referent als serveis web
http://www.w3.org/TR/soap/	Pàgina web d'estandardització del protocol SOAP
http://www.w3.org/TR/XAdES/	Pàgina web d'estandardització de signatures digitals XAdES
http://www.w3.org/TR/XMLDsig-core/	Pàgina web d'estandardització de signatures digitals DSIG
http://ws.apache.org/axis/	Pàgina web oficial d'AXIS
http://XMLbeans.apache.org/	Pàgina web oficial de XMLBeans
http://xfire.codehaus.org/	Pàgina web oficial de XFire

10.2. Atributs de consulta d'un certificat

El perfil XSS que permet l'extracció de camps dels certificats validats a PSIS (ja sigui per validació directa o per estar inclosos dins d'una signatura a validar) possibilita també un processat semàntic del contingut dels mateixos, ja que no es tracta únicament d'una extracció simple. Això propicia que la informació recuperada sigui la mateixa, independentment de la política presa per l'emissor del certificat. Per exemple, ens permetria extreure el DNI del titular del certificat independentment d'on i de com ho hagi inclòs l'emissor del certificat.

urn:oasis:names:tc:dss:1.0:profiles:XSS:certificateAttributes:[Paràmetre]		
Paràmetre	Descripció	Tipus
<i>Version</i>	Sol·licitud de la versió del certificat	Global
<i>SerialNumber</i>	Sol·licitud del nombre de sèrie del certificat	Global
<i>Signature</i>	Sol·licitud de la signatura del certificat	Global
<i>SignatureAlgorithm</i>	Sol·licitud de l'algorisme usat per a signar el certificat	Global
<i>IssuerDistinguishedName</i>	Nom de l'emissor del certificat	Global
<i>SubjectDistinguishedName</i>	Nom del subjecte del certificat	Global
<i>NotBefore</i>	Sol·licitud de la data d'inici de validesa del certificat	Global
<i>NotAfter</i>	Sol·licitud de la data de finalització de validesa del certificat	Global
<i>SubjectPublicKeyAlgorithm</i>	Sol·licitud de l'algorisme de generació de la clau pública	Global
<i>SubjectPublicKey</i>	Sol·licitud de la clau pública del certificat	Global
<i>CertificatePolicies</i>	Polítiques de certificació	Global
<i>KeyUsages</i>	Sol·licitud dels usos permesos de la clau del certificat	Global
<i>SubjectEmail</i>	Direcció de correu electrònic del subjecte	
<i>IssuerDistinguishedName:commonName</i>	Nom de l'emissor del certificat	Global
<i>SubjectDistinguishedName:serialNumber</i>	Nombre de sèrie del certificat del subjecte del certificat	Global
<i>SubjectDistinguishedName:commonName</i>	Nom de pila del subjecte del certificat	Global
<i>SubjectDistinguishedName:givenName</i>	Nom del subjecte del certificat	Global
<i>SubjectDistinguishedName:surname</i>	Cognom del subjecte del certificat	Global
<i>SubjectDistinguishedName:title</i>	Títol del subjecte del certificat	Global
<i>SubjectDistinguishedName:organizationName</i>	Nom de l'organització de la qual forma part el subjecte del certificat	Global
<i>SubjectDistinguishedName:organizationUnitName</i>	Nom del departament del qual forma part el subjecte del certificat	Global
<i>SubjectDistinguishedName:countryName</i>	Nom del país del subjecte del certificat	Global
<i>SubjectDistinguishedName:stateOrProvinceName</i>	Nom de la província del subjecte del certificat	Global
<i>Extensions</i>	No disponible	Global

urn:catcert:psis:certificateAttributes:notaries:[Paràmetre]		
Paràmetre	Descripció	Tipus
<i>AuthorizingNotary</i>	Notari que autoritza	Particular CATCERT
<i>RepresentationDocumentLocationData</i>	Localització de les dades del document de representació	Particular CATCERT
<i>EntitlementsRegistryLocationData</i>	Localització de les dades de registre de drets.	Particular CATCERT

urn:catcert:psis:certificateAttributes:professionalAssociations:+[Paràmetre]		
Paràmetre	Descripció	Tipus
<i>ProfessionalAssociationName</i>	Nom de l'associació professional	Particular CATCERT
<i>ProfessionalAssociationInitials</i>	Inicials de l'associació professional	Particular CATCERT
<i>ProfessionalAssociationNumber</i>	Número de l'associació professional	Particular CATCERT
<i>ProfessionalAssociationZone</i>	Zona de l'associació professional	Particular CATCERT
<i>ProfessionalAssociationEmployeeNumber</i>	Número d'empleat a l'associació professional	Particular CATCERT
<i>ProfessionalAssociationCIF</i>	CIF de l'associació professional	Particular CATCERT

urn:catcert:psis:certificateAttributes:+[Paràmetre]		
Paràmetre	Descripció	Tipus
<i>KeyOwnerNIF</i>	Consulta del NIF incorporat al certificat	Particular CATCERT
<i>NaturalPersonIdentityType</i>	Tipus del document d'identificació de la persona natural	Particular CATCERT
<i>NaturalPersonCountryCode</i>	Codi de país de la persona natural	Particular CATCERT
<i>LegalEntityCIF</i>	CIF de l'entitat legal	Particular CATCERT
<i>LegalEntityGlobalCIF</i>	CIF global de l'entitat legal	Particular CATCERT
<i>Department</i>	Departament	Particular CATCERT
<i>SubjectName</i>	Nom del subjecte	Particular CATCERT
<i>CertIssuerName</i>	Nom de l'emissor del certificat	Particular CATCERT
<i>QuantitativeUsageLimitations</i>	Limitacions d'ús en quantitat	Particular CATCERT
<i>QualitativeUsageLimitations</i>	Limitacions d'ús en qualitat	Particular CATCERT
<i>ClassificationLevel</i>	Nivell de classificació (número)	Particular CATCERT
<i>Title</i>	Títol	Particular CATCERT
<i>Attribute</i>	Atribut addicional	Particular CATCERT
<i>VinculatedPersonFullName</i>	Nom complet de la persona vinculada	Particular CATCERT
<i>VinculatedPersonName</i>	Nom de la persona vinculada	Particular CATCERT
<i>VinculatedPersonSurname</i>	Cognom de la persona vinculada	Particular CATCERT
<i>VinculatedPersonNIForNIE</i>	NIF/NIE de la persona vinculada	Particular CATCERT
<i>VinculatedCompanyCIF</i>	CIF de la companyia de la persona vinculada	Particular CATCERT
<i>LegalPersonIdentityType</i>	Tipus del document d'identificació de la persona legal	Particular CATCERT
<i>LegalPersonCountryCode</i>	Codi de país de la persona legal	Particular CATCERT
<i>VinculatedCompanyName</i>	Nom de la companyia vinculada	Particular CATCERT
<i>issuerCA</i>	Emissor del certificat	Particular CATCERT
<i>UsageProperties</i>	Propietats d'ús del certificat	Particular CATCERT

<i>RegisterJoint</i>	Registre conjunt	Particular CATCERT
<i>LegalDocumentType</i>	Tipus de document legal	Particular CATCERT
<i>CertificateType</i>	Tipus de certificat en llenguatge entenedor	Particular CATCERT
<i>CertificateTypeCode</i>	Tipus de certificat en codi	Particular CATCERT
<i>Pseudonym</i>	Pseudònim	Particular CATCERT

10.3. Atributs de consulta d'una signatura

urn:OASIS:names:tc:dss:1.0:profiles:XSS:signatureAttributes:+[Paràmetre]	
Paràmetre	Descripció
<i>DigestAlgorithm</i>	Sol·licitud de consulta de l'algorisme utilitzat per a generar el valor de <i>Digest</i>
<i>DigestEncryptionAlgorithm</i>	Sol·licitud de consulta de l'algorisme d'enciptació aplicat al digest per a generar la signatura
<i>SignatureAlgorithm</i>	Sol·licitud de consulta de l'algorisme utilitzat per a generar la signatura
<i>SignatureValue</i>	Sol·licitud de consulta del valor de signatura

10.4. Esquema del protocol DSS i el seu perfil XSS

Protocol DSS
<pre> <?XML version="1.0" encoding="UTF-8"?> <xs:schema Xmlns:dss="urn:OASIS:names:tc:dss:1.0:core:schema" Xmlns:ds="http://www.w3.org/2000/09/XMLDsig#" Xmlns:xs="http://www.w3.org/2001/XMLSchema" Xmlns:saml="urn:OASIS:names:tc:SAML:1.0:assertion" targetNamespace="urn:OASIS:names:tc:dss:1.0:core:schema" elementFormDefault="qualified" attributeFormDefault="unqualified"> <!-- --> <xs:annotation> <xs:documentation XML:lang="en"> This Schema defines the Digital Signature Service Core Protocols, Elements, and Bindings Working Draft 34 </xs:documentation> </xs:annotation> <!-- --> <xs:import namespace="http://www.w3.org/2000/09/XMLDsig#" schemaLocation="http://www.w3.org/TR/XMLDsig-core/XMLDsig-core-schema.xsd"/> <xs:import namespace="urn:OASIS:names:tc:SAML:1.0:assertion" schemaLocation="http://www.OASIS-open.org/committees/download.php/3408/OASIS-sstc-saml- schema-protocol-1.1.xsd"/> <xs:import namespace="http://www.w3.org/XML/1998/namespace" schemaLocation="http://www.w3.org/2001/XML.xsd"/> <!-- COMMON PROTOCOL STRUCTURES --> <xs:complexType name="AnyType"> <xs:annotation> </pre>

```

        <xs:documentation XML:lang="en">
            This Type type is used to match optional inputs, optional
            outputs and to make the Schema extensible where
            &lt;xs:any namespace="##other" processContents="lax"/&gt;
            is not possible due to unique particle attribution rules.
        </xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:any processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
<!-- -->
<xs:complexType name="InlineXMLType">
    <xs:annotation>
        <xs:documentation XML:lang="en">
            This Type clearly expresses the fact that content of
            InlineXML should be
            one
            Comments before
            ignorePIsComments indicates
            will also
            PI's and
            would have
            wanted them to be signed.
        </xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:any processContents="lax"/>
    </xs:sequence>
    <xs:attribute name="ignorePIs" type="xs:boolean" use="optional"
default="true"/>
    <xs:attribute name="ignoreComments" type="xs:boolean" use="optional"
default="true"/>
</xs:complexType>
<!-- -->
<xs:complexType name="InternationalStringType">
    <xs:simpleContent>
        <xs:extension base="xs:string">
            <xs:attribute ref="XML:lang" use="required"/>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
<!-- -->
<xs:element name="InputDocuments">
    <xs:annotation>
        <xs:documentation XML:lang="en">
            <!-- Re: UPA Problem rationale behind these changes [FW:
FROM JC THROUGH KONRAD] -->
            <!--
            &lt;xs:any namespace="##other" processContents="lax"/&gt;
            allows to introduce new top level elements from other
namespaces
            to support other types of documents in the future.
        </xs:documentation>
    </xs:annotation>

```

```

-->
                                <!-- Solution consistent with other places -->
                                &lt;xs:element name="Other" type="dss:AnyType"/&gt;
                                allows to introduce new top level elements from
namespaces including
                                dss to support other types of input documents in the
future.
                                </xs:documentation>
                                </xs:annotation>
                                <xs:complexType>
                                    <xs:sequence>
                                        <xs:choice maxOccurs="unbounded">
                                            <xs:element ref="dss:Document"/>
                                            <xs:element ref="dss:TransformedData"/>
                                            <xs:element ref="dss:DocumentHash"/>
                                            <xs:element name="Other" type="dss:AnyType"/>
                                        </xs:choice>
                                    </xs:sequence>
                                </xs:complexType>
                            </xs:element>
                            <!-- -->
                            <xs:complexType name="DocumentBaseType" abstract="true">
                                <xs:attribute name="ID" type="xs:ID" use="optional"/>
                                <xs:attribute name="RefURI" type="xs:anyURI" use="optional"/>
                                <xs:attribute name="RefType" type="xs:anyURI" use="optional"/>
                                <xs:attribute name="SchemaRefs" type="xs:IDREFS" use="optional"/>
                            </xs:complexType>
                            <!-- -->
                            <xs:element name="Document" type="dss:DocumentType"/>
                            <xs:complexType name="DocumentType">
                                <xs:complexContent>
                                    <xs:extension base="dss:DocumentBaseType">
                                        <xs:sequence>
                                            <xs:choice>
                                                <xs:element name="InlineXML"
type="dss:InlineXMLType"/>
                                                <xs:element name="Base64XML"
type="xs:base64Binary"/>
                                                <xs:element name="EscapedXML"
type="xs:string"/>
                                                <xs:element ref="dss:Base64Data"/>
                                            </xs:choice>
                                        </xs:sequence>
                                    </xs:extension>
                                </xs:complexContent>
                            </xs:complexType>
                            <!-- -->
                            <xs:element name="Base64Data">
                                <xs:complexType>
                                    <xs:simpleContent>
                                        <xs:extension base="xs:base64Binary">
                                            <xs:attribute name="MimeType" type="xs:string"
use="optional"/>
                                        </xs:extension>
                                    </xs:simpleContent>
                                </xs:complexType>
                            </xs:element>
                            <!-- -->
                            <xs:element name="DocumentHash">
                                <xs:complexType>

```

```

        <xs:complexContent>
            <xs:extension base="dss:DocumentBaseType">
                <xs:sequence>
                    <xs:element ref="ds:Transforms"
minOccurs="0"/>
                    <xs:element ref="ds:DigestMethod"/>
                    <xs:element ref="ds:DigestValue"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
</xs:element>
<!-- -->
<xs:element name="TransformedData">
    <xs:complexType>
        <xs:complexContent>
            <xs:extension base="dss:DocumentBaseType">
                <xs:sequence>
                    <xs:element ref="ds:Transforms"
minOccurs="0"/>
                    <xs:element ref="dss:Base64Data"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
</xs:element>
<!-- -->
<xs:element name="SignatureObject" type="dss:SignatureObjectType"/>
<xs:complexType name="SignatureObjectType">
    <xs:annotation>
        <xs:documentation XML:lang="en">
            &lt;xs:any namespace="##other" processContents="lax"/&gt;
is not
possible here to allow extensibility as more than one
namespace
(i.e. ds, dss) are used in the choice hence
&lt;xs:element name="Other" type="dss:AnyType"/&gt;
allows to introduce new top level elements from
namespaces including
dss to support other types of signatures in the future.
        </xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:choice>
            <xs:element ref="ds:Signature"/>
            <xs:element ref="dss:Timestamp"/>
            <xs:element ref="dss:Base64Signature"/>
            <xs:element ref="dss:SignaturePtr"/>
            <xs:element name="Other" type="dss:AnyType"/>
        </xs:choice>
    </xs:sequence>
    <xs:attribute name="SchemaRefs" type="xs:IDREFS" use="optional"/>
</xs:complexType>
<!-- -->
<xs:element name="Base64Signature">
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="xs:base64Binary">
                <xs:attribute name="Type" type="xs:anyURI"/>
            </xs:extension>

```

```

        </xs:simpleContent>
    </xs:complexType>
</xs:element>
<!-- -->
<xs:element name="SignaturePtr">
    <xs:complexType>
        <xs:attribute name="WhichDocument" type="xs:IDREF"/>
        <xs:attribute name="XPath" type="xs:string" use="optional"/>
    </xs:complexType>
</xs:element>
<!-- -->
<xs:element name="Result">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="ResultMajor" type="xs:anyURI"/>
            <xs:element name="ResultMinor" type="xs:anyURI"
minOccurs="0"/>
            <xs:element name="ResultMessage"
type="dss:InternationalStringType" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<!-- -->
<xs:element name="OptionalInputs" type="dss:AnyType">
    <xs:annotation>
        <xs:documentation XML:lang="en">
            "dss:AnyType"/> matches any top level element of any
elements.
            namespace, hence OptionalInputs can contain 0..* top level
            It should however not contain elements that are not
declared as
            optional inputs by normative text of the dss-core or dss-
profiles.
        </xs:documentation>
    </xs:annotation>
</xs:element>
<!-- -->
<xs:element name="OptionalOutputs" type="dss:AnyType">
    <xs:annotation>
        <xs:documentation XML:lang="en">
            "dss:AnyType"/> matches any top level element of any
elements.
            namespace, hence OptionalInputs can contain 0..* top level
            It should however not contain elements that are not
declared as
            optional outputs by normative text of the dss-core or dss-
profiles.
        </xs:documentation>
    </xs:annotation>
</xs:element>
<!-- -->
<xs:element name="ServicePolicy" type="xs:anyURI"/>
<!-- -->
<xs:element name="ClaimedIdentity">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="Name" type="saml:NameIdentifierType"/>
            <xs:element name="SupportingInfo" type="dss:AnyType"
minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>

```

```

        </xs:complexType>
    </xs:element>
    <!-- -->
    <xs:element name="Language" type="xs:language"/>
    <!-- -->
    <xs:element name="AdditionalProfile" type="xs:anyURI"/>
    <!-- COMMON PROTOCOL STRUCTURES -->
    <!-- PROTOCOL MESSAGES BEGIN -->
    <!-- -->
    <xs:complexType name="RequestBaseType">
        <xs:sequence>
            <xs:element ref="dss:OptionalInputs" minOccurs="0"/>
            <xs:element ref="dss:InputDocuments"/>
        </xs:sequence>
        <xs:attribute name="RequestID" type="xs:string" use="optional"/>
        <xs:attribute name="Profile" type="xs:anyURI" use="optional"/>
    </xs:complexType>
    <!-- -->
    <xs:element name="SignRequest">
        <xs:complexType>
            <xs:complexContent>
                <xs:extension base="dss:RequestBaseType">
                    <xs:attribute name="Type" type="xs:anyURI"/>
                </xs:extension>
            </xs:complexContent>
        </xs:complexType>
    </xs:element>
    <!-- -->
    <xs:element name="IncludeObject">
        <xs:complexType>
            <xs:attribute name="WhichDocument" type="xs:IDREF"/>
            <xs:attribute name="hasObjectTagsAndAttributesSet"
type="xs:boolean" default="false"/>
            <xs:attribute name="ObjId" type="xs:string" use="optional"/>
            <xs:attribute name="createReference" type="xs:boolean"
use="optional" default="true"/>
        </xs:complexType>
    </xs:element>
    <!-- -->
    <xs:element name="SignaturePlacement">
        <xs:complexType>
            <xs:sequence>
                <xs:choice>
                    <xs:element name="XPathAfter" type="xs:string"/>
                    <xs:element name="XPathFirstChildOf"
type="xs:string"/>
                </xs:choice>
            </xs:sequence>
            <xs:attribute name="WhichDocument" type="xs:IDREF"/>
            <xs:attribute name="createEnvelopedSignature" type="xs:boolean"
default="true"/>
        </xs:complexType>
    </xs:element>
    <!-- -->
    <xs:complexType name="ResponseBaseType">
        <xs:sequence>
            <xs:element ref="dss:Result"/>
            <xs:element ref="dss:OptionalOutputs" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="RequestID" type="xs:string" use="optional"/>
    </xs:complexType>

```

```

        <xs:attribute name="Profile" type="xs:anyURI" use="required"/>
    </xs:complexType>
    <!-- -->
    <xs:element name="Response" type="dss:ResponseBaseType"/>
    <!-- -->
    <xs:element name="SignResponse">
        <xs:complexType>
            <xs:complexContent>
                <xs:extension base="dss:ResponseBaseType">
                    <xs:sequence>
                        <xs:element ref="dss:SignatureObject"
minOccurs="0"/>
                    </xs:sequence>
                </xs:extension>
            </xs:complexContent>
        </xs:complexType>
    </xs:element>
    <!-- -->
    <!-- SIGNRESPONSE OPTIONAL OUTPUTS START -->
    <xs:element name="DocumentWithSignature">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="dss:Document"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <!-- SIGNRESPONSE OPTIONAL OUTPUTS END -->
    <xs:element name="VerifyRequest">
        <xs:complexType>
            <xs:complexContent>
                <xs:extension base="dss:RequestBaseType">
                    <xs:sequence>
                        <xs:element ref="dss:SignatureObject"
minOccurs="0"/>
                    </xs:sequence>
                </xs:extension>
            </xs:complexContent>
        </xs:complexType>
    </xs:element>
    <!-- -->
    <xs:element name="VerifyResponse">
        <xs:complexType>
            <xs:complexContent>
                <xs:extension base="dss:ResponseBaseType"/>
            </xs:complexContent>
        </xs:complexType>
    </xs:element>
    <!-- -->
    <!-- PROTOCOL MESSAGES END -->
    <!-- SIGNREQUEST OPTIONAL INPUTS START -->
    <xs:element name="SignatureType" type="xs:anyURI"/>
    <xs:element name="AddTimestamp">
        <xs:complexType>
            <xs:attribute name="Type" type="xs:anyURI" use="optional"/>
        </xs:complexType>
    </xs:element>
    <!-- -->
    <xs:element name="IntendedAudience">
        <xs:complexType>
            <xs:sequence>

```

```

        <xs:element name="Recipient"
type="saml:NameIdentifierType" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
</xs:element>
<!-- -->
<xs:element name="KeySelector">
    <xs:annotation>
        <xs:documentation XML:lang="en">
            &lt;xs:any namespace="##other" processContents="lax"/&gt;
is not
                possible here to allow extensibility as another namespace
than
                the target namespace is used in the choice hence
                &lt;xs:element name="Other" type="dss:AnyType"/&gt;
namespaces including
                allows to introduce new top level elements from
target namespace.
                dss to support other types of key selectors in the future.
                Note that namespace="##other" is the complement of the
other namespaces
                Note also that XML schema does not support complements for
                or sets of namespaces which is a defect in XML schema.
                It only supports sets of namespaces which is not useful
however as we cannot
                know which namespaces might be relevant in the future.
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:sequence>
            <xs:choice>
                <xs:element ref="ds:KeyInfo"/>
                <xs:element name="Other" type="dss:AnyType"/>
            </xs:choice>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<!-- -->
<xs:element name="SignedReferences">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="dss:SignedReference"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<!-- -->
<xs:element name="Properties">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="SignedProperties"
type="dss:PropertiesType" minOccurs="0"/>
            <xs:element name="UnsignedProperties"
type="dss:PropertiesType" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<!-- -->
<xs:element name="Property">
    <xs:complexType>

```

```

                <xs:sequence>
                    <xs:element name="Identifier" type="xs:anyURI"/>
                    <xs:element name="Value" type="dss:AnyType"
minOccurs="0"/>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <!-- -->
        <xs:complexType name="PropertiesType">
            <xs:sequence>
                <xs:element ref="dss:Property" maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
        <!-- -->
        <xs:element name="SignedReference">
            <xs:annotation>
                <xs:documentation XML:lang="en">
                    RefURI overrides the of <math>\langle \text{dss:Document} \rangle</math>
                </xs:documentation>
            </xs:annotation>
            <xs:complexType>
                <xs:sequence>
                    <xs:element ref="ds:Transforms" minOccurs="0"/>
                </xs:sequence>
                <xs:attribute name="WhichDocument" type="xs:IDREF"
use="required"/>
                <xs:attribute name="RefURI" type="xs:anyURI" use="optional"/>
                <xs:attribute name="RefId" type="xs:string" use="optional"/>
            </xs:complexType>
        </xs:element>
        <!-- -->
        <xs:element name="Schema" type="dss:DocumentType"/>
        <!-- -->
        <xs:element name="Schemas" type="dss:SchemasType"/>
        <xs:complexType name="SchemasType">
            <xs:sequence>
                <xs:element ref="dss:Schema" maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
        <!-- SIGNREQUEST OPTIONAL INPUTS END -->
        <!-- VERIFYREQUEST OPTIONAL INPUTS START -->
        <xs:element name="VerifyManifests"/>
        <xs:element name="VerificationTime" type="xs:dateTime"/>
        <xs:element name="AdditionalKeyInfo">
            <xs:complexType>
                <xs:sequence>
                    <xs:element ref="ds:KeyInfo"/>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <!-- -->
        <xs:element name="ReturnProcessingDetails"/>
        <!-- -->
        <xs:element name="ReturnSigningTime"/>
        <!-- -->
        <xs:element name="ReturnTimestampTime"/>
        <!-- -->
        <xs:element name="ReturnSignerIdentity"/>
        <!-- -->
        <xs:element name="ReturnUpdatedSignature">

```

```

        <xs:complexType>
            <xs:attribute name="Type" type="xs:anyURI" use="optional"/>
        </xs:complexType>
    </xs:element>
    <!-- -->
    <xs:element name="ReturnTransformedDocument">
        <xs:complexType>
            <xs:attribute name="WhichReference" type="xs:integer"
use="required"/>
        </xs:complexType>
    </xs:element>
    <!-- VERIFYREQUEST OPTIONAL INPUTS END -->
    <!-- VERIFYRESPONSE OPTIONAL OUTPUTS START -->
    <xs:element name="ProcessingDetails">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="ValidDetail" type="dss:DetailType"
minOccurs="0" maxOccurs="unbounded"/>
                <xs:element name="IndeterminateDetail"
type="dss:DetailType" minOccurs="0" maxOccurs="unbounded"/>
                <xs:element name="InvalidDetail" type="dss:DetailType"
minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <!-- -->
    <xs:element name="SigningTime">
        <xs:complexType>
            <xs:simpleContent>
                <xs:extension base="xs:dateTime">
                    <xs:attribute name="ThirdPartyTimestamp"
type="xs:boolean" use="required"/>
                </xs:extension>
            </xs:simpleContent>
        </xs:complexType>
    </xs:element>
    <!-- -->
    <xs:element name="TimestampTime" type="xs:dateTime"/>
    <!-- -->
    <xs:element name="SignerIdentity" type="saml:NameIdentifierType"/>
    <!-- -->
    <xs:element name="UpdatedSignature">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="dss:SignatureObject"/>
            </xs:sequence>
            <xs:attribute name="Type" type="xs:anyURI" use="optional"/>
        </xs:complexType>
    </xs:element>
    <!-- -->
    <xs:element name="TransformedDocument">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="dss:Document"/>
            </xs:sequence>
            <xs:attribute name="WhichReference" type="xs:integer"
use="required"/>
        </xs:complexType>
    </xs:element>
    <!-- -->

```

```

<xs:complexType name="DetailType">
  <xs:sequence>
    <xs:element name="Code" type="xs:anyURI" minOccurs="0"/>
    <xs:element name="Message" type="dss:InternationalStringType"
minOccurs="0"/>
    <xs:any namespace="##other" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="Type" type="xs:anyURI" use="required"/>
</xs:complexType>
<!-- VERIFYRESPONSE OPTIONAL OUTPUTS END -->
<!-- TIMESTAMP BEGIN -->
<xs:element name="Timestamp">
  <xs:complexType>
    <xs:sequence>
      <xs:choice>
        <xs:element ref="ds:Signature"/>
        <xs:element name="RFC3161TimeStampToken"
type="xs:base64Binary"/>
        <xs:element name="Other" type="dss:AnyType"/>
      </xs:choice>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<!-- -->
<xs:element name="TstInfo">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="SerialNumber" type="xs:integer"/>
      <xs:element name="CreationTime" type="xs:dateTime"/>
      <xs:element name="Policy" type="xs:anyURI" minOccurs="0"/>
      <xs:element name="ErrorBound" type="xs:duration"
minOccurs="0"/>
      <xs:element name="Ordered" type="xs:boolean"
default="false" minOccurs="0"/>
      <xs:element name="TSA" type="saml:NameIdentifierType"
minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<!-- REQUESTER IDENTITY BEGIN -->
<xs:element name="RequesterIdentity">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="Name" type="saml:NameIdentifierType"/>
      <xs:element name="SupportingInfo" type="dss:AnyType"
minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<!-- REQUESTER IDENTITY END -->
<xs:element name="VerifyManifestResults" type="dss:VerifyManifestResultsType"/>
<xs:complexType name="VerifyManifestResultsType">
  <xs:sequence>
    <xs:element ref="dss:ManifestResult" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
<xs:element name="ManifestResult">
  <xs:complexType>
    <xs:sequence>

```

```

        <xs:element name="ReferenceXPath" type="xs:string"/>
        <xs:element name="Status" type="xs:anyURI"/>
    </xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>

```

Protocol XSS

```

<?XML version="1.0" encoding="UTF-8"?>
<!-- XSS Profile of the OASIS DSS Schema v1.0-->
<!--Author: Carlos González-Cadenas-->
<!--Date: December 2005-->
<xs:schema targetNamespace="urn:OASIS:names:tc:dss:1.0:profiles:XSS"
  Xmlns:archp="urn:OASIS:names:tc:dss:1.0:profiles:archive"
  Xmlns:xsp="http://uri.etsi.org/2038/v1.1.1#" Xmlns:tstl="http://uri.etsi.org/02231/v1.0bis
  2005-04#" Xmlns:dss="http://www.docs.OASIS-open.org/dss/OASIS-dss-1.0-core-schema-cd-02.xsd"
  Xmlns:xs="http://www.w3.org/2001/XMLSchema" Xmlns:ds="http://www.w3.org/2000/09/XMLDsig#"
  Xmlns:saml20="urn:OASIS:names:tc:SAML:2.0:assertion"
  Xmlns="urn:OASIS:names:tc:dss:1.0:profiles:XSS" elementFormDefault="qualified"
  attributeFormDefault="unqualified">
  <xs:import namespace="http://uri.etsi.org/02231/v1.0bis 2005-04#"
    schemaLocation="TS101231v1_2_1.xsd"/>
  <xs:import namespace="urn:OASIS:names:tc:dss:1.0:profiles:archive"
    schemaLocation="OASIS-dss-1.0-profiles-archive-schema-wd01-errata01.xsd"/>
  <xs:import namespace="urn:OASIS:names:tc:SAML:2.0:assertion"
    schemaLocation="http://docs.OASIS-open.org/security/saml/v2.0/saml-schema-assertion-
    2.0.xsd"/>
  <xs:import namespace="http://uri.etsi.org/2038/v1.1.1#"
    schemaLocation="SigPolicy.xsd"/>
  <xs:element name="SignaturePolicy">
    <xs:complexType>
      <xs:complexContent>
        <xs:extension base="XAdES:ObjectIdentifierType">
          <xs:attribute name="allowPolicyMappings"
            type="xs:boolean" use="optional" default="false"/>
        </xs:extension>
      </xs:complexContent>
    </xs:complexType>
  </xs:element>
  <xs:element name="SignaturePolicyInfo">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="SignaturePolicyIssuer" type="xs:string"/>
        <xs:element name="SignaturePolicyIdentifier"
          type="XAdES:ObjectIdentifierType"/>
        <xs:element name="SignaturePolicyDigestAlgorithm"
          type="XAdES:ObjectIdentifierType"/>
        <xs:element name="SignaturePolicyDigestValue"
          type="ds:DigestValueType"/>
        <xs:element ref="ds:Transforms" minOccurs="0"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="ReturnSignedResponse">

```

```

        <xs:complexType>
            <xs:sequence>
                <xs:element name="RequiredCommitments" minOccurs="0">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="CommitmentType"
type="xsp:CommitmentType" maxOccurs="unbounded"/>
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="ResponseSignature">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ds:Signature"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="ReturnSignatureInfo">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="AttributeDesignator"
type="saml20:AttributeType" maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="SignatureInfo">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="Attribute" type="saml20:AttributeType"
maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:complexType name="BinaryAttributeValueType">
        <xs:simpleContent>
            <xs:extension base="xs:base64Binary">
                <xs:attribute name="Attribute" type="xs:anyURI"
use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:element name="ReturnX509CertificateInfo">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="AttributeDesignator"
type="saml20:AttributeType" maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="X509CertificateInfo">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="Attribute" type="saml20:AttributeType"
maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>

```

```

<xs:element name="Scheme">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="SchemeName"
type="tsl:InternationalNamesType"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="SchemeInfo">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="SchemeName"
type="tsl:InternationalNamesType"/>
      <xs:element name="TSLSequenceNumber" type="xs:integer"/>
      <xs:element name="TSLDigestAlgorithm"
type="XAdES:ObjectIdentifierType"/>
      <xs:element name="TSLDigestValue" type="ds:DigestValueType"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="X509CertificateValidationOptions"
type="xsp:CertificateTrustTreesType"/>
  <xs:element name="RequireQualifiedCertificate"/>
  <xs:element name="Archive">
    <xs:complexType>
      <xs:sequence>
        <xs:choice>
          <xs:element ref="archp:ArchivePolicy" minOccurs="0"/>
          <xs:element ref="archp:RetentionPeriod" minOccurs="0"/>
        </xs:choice>
          <xs:element ref="archp:UpdateSignature" minOccurs="0"/>
          <xs:element ref="archp:ArchiveMode" minOccurs="0"/>
        </xs:sequence>
      </xs:complexType>
</xs:element>
<xs:element name="ArchiveInfo">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="ArchiveIdentifier"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="CounterSignature">
  <xs:complexType>
    <xs:attribute name="WhichDocument" type="xs:IDREF" use="required"/>
  </xs:complexType>
</xs:element>
<xs:element name="ParallelSignature"/>
</xs:schema>

```