Consorci
Administració Oberta
de Catalunya

FAQs de PSA

(Programari de Signatura Avançada)

Control documental

Estat formal	**Elaborat per:** Joan Mir Rubio	**Aprovat per:** Àrea Tècnica
Data de creació	31/08/2008	
Control de versions	**Data:**	08/11/2017
	Descripció:	2.6 Revisió general
	Data:	23/02/2012
	Descripció:	2.5 Revisió general
	Data:	09/06/2010
	Descripció:	2.4 Revisió general
	Data:	08/02/2010
	Descripció:	2.3 Revisió general i noves preguntes
	Data:	26/01/2010
	Descripció:	2.2 Noves preguntes
	Data:	28/09/2009
	Descripció:	2.1 Canvi de polítiques de procediment a signatura múltiple
	Data:	03/06/2009
	Descripció:	1.9 Revisió del CAU
Nivell accés informació	pública	
Títol	FAQs de PSA	
Fitxer	D1313 -FAQ del PSA v2.6.docx	
Control de còpies	Només les còpies disponibles al Consorci AOC garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades.	
Drets d'autor	Aquesta obra està subjecta a una llicència Reconeixement-No comercial-Sense obres derivades 2.5 Espanya de Creative Commons. Per veure'n una còpia, visiteu http://creativecommons.org/licenses/by-nc-nd/2.5/es/ o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA	

Índex

1. Introducció

Aquest document recull el conjunt de preguntes més freqüents sobre el servei de PSA o **P**rogramari de **S**ignatura **A**vançada. El conjunt de preguntes aborda qüestions de nivell funcional, tècnic, arquitectònic, i de concepte. L'objectiu d'aquest document és donar resposta a aquestes preguntes, i si s'escau, indicar al lector què ha de fer o on pot trobar informació més detallada.

2. FAQ

2.1 Què és PSA?

PSA és un programari que dóna solució a qualsevol aplicació per a la realització de signatures electròniques. Aquesta solució s'ofereix mitjançant serveis web.

PSA ofereix també les funcionalitats necessàries per **signatura en client**. A tal efecte, PSA disposa de la integració amb el Signador (versió APSA-Light), que permet el xifrat de les dades en client, de manera que l'usuari pot signar localment en possessió de la seva clau privada. La resta de funcionalitats relacionades amb la generació de la signatura queden delegades a PSA.

El programari ofereix també eines i mecanismes per a que qualsevol aplicació pugui realitzar **signatures desateses** i signatures múltiples amb suport de polítiques de signatura conforme a estàndards, fent ús de certificats carregats al propi PSA.

PSA també permet realitzar operacions de xifrat i desxifrat de documents.

2.2 Quines funcionalitats ofereix?

PSA ofereix les següents funcionalitats:

- Generació d'una signatura digital d'un document. La signatura es generarà en conformitat a una política de signatura i podrà ser creada:
    - A l'equip de l'usuari final: quan s'hagi d'emprar un certificat que estigui en possessió d'un usuari: emmagatzemat en targeta criptogràfica (com ara un CPISR-1) o en suport software al mateix equip (com l'idCAT).
    - Al component servidor de PSA: quan s'hagi d'emprar un certificat CDA, de segell electrònic o similar, que sigui accessible per al component servidor de PSA.
- Suport a les necessitats de negoci en relació a la gestió de la signatura electrònica. PSA dóna suport a la gestió de polítiques de signatura múltiple, de manera que les aplicacions client poden delegar a PSA les complexes tasques de gestió involucrades en la generació de diferents variants de signatura: signatures solidàries, mancomunades, etc.
- Generació de signatures per a múltiples documents. Amb una sola petició és possible sol·licitar la signatura de múltiples documents.
- Generació de comprovants. L'aplicació de gestió pot sol·licitar a PSA la generació d'un comprovant associat a una signatura digital realitzada. Per això, l'aplicació de gestió ha d'indicar a PSA l'identificador de la transacció que va generar la signatura sobre la qual es desitja generar el comprovant.
- Obtenció del tiquet de validació de la signatura generada. Si el client així ho sol·licita, PSA pot retornar el tiquet signat de validació de PSIS de la signatura generada.

Aquestes funcionalitats estan descrites en més detall en el document de Descripció_del_Servei_PSA.

2.3 Quines signatures digitals pot crear?

PSA dóna suport a tots els atributs (signats i no signats) als que fan referència les versions indicades a continuació de les especificacions tècniques dels següents formats de signatura electrònica:

CMS	*RFC 3852*
CAdES	*ETSI TS 101 733*
XMLDSig	*RFC 3275*
XAdES	*ETSI TS 101 903*

2.4 Quins formats de documents pot signar?

PSA permet signar i verificar els següents tipus de continguts:

- Qualsevol fitxer binari, especialment en la modalitat de signatura cega[1]. Específicament cal tractar en aquest cas la signatura de fitxers gràfics[2] suportant els següents formats:
    - Format JPEG, en les seves diferents versions.
    - Format GIF, en les seves diferents versions.
    - Format TIFF, en les seves diferents versions.
- Qualsevol document XML, amb tractament de les transformacions corresponents a la visualització dels mateixos (com XSLT o XHTML) i, específicament, totes les capacitats de signatura electrònica sobre continguts i metadades dels següents esquemes.
    - Open Document.
    - Open XML Office.
- Qualsevol versió de documents Adobe PDF, fins a l'especificació PDF Reference versió 1.7, amb suport específic per a les signatures anomenades ordinària i MDP[3], amb els mètodes de resum criptogràfic anomenats *Byte Range* i *Object Digest*, i amb suport dels diferents formats de diccionaris de signatura (*Signature Dictionary*) i de manifestacions legals (*Legal Attestation Dictionary*). Dóna suport a l'anomenada *signature appearance*[4] per facilitar la presentació de la signatura a l'usuari. Els documents en format PDF que hagin estat signats mitjançant PSA són compatibles - i les signatures es poden validar - amb l'última versió de l'Adobe Reader, i també amb versions anteriors (a partir de la versió 6).

---

[1] Signatura cega: forma de signatura digital en que no es revela el contingut de les dades signades.

[2] La signatura de fitxers gràfics resulta especialment necessària en els casos de digitalització documental, per convertir documents en paper a les seves versions digitals.

[3] No caldrà donar suport a signatures de dret d'autor.

[4] Conforme al document "Digital Signature Appearances - Version: Acrobat 6.0", de maig de 2003.

- Qualsevol versió de missatges S/MIME, als efectes d'embolcallar documents i signatures electròniques a enviar o rebre en aquest format – freqüentment emprat en correu electrònic segur, considerant específicament l'embolcall simple i, com a mínim, l'embolcall triple (*Triple Wrapping*).

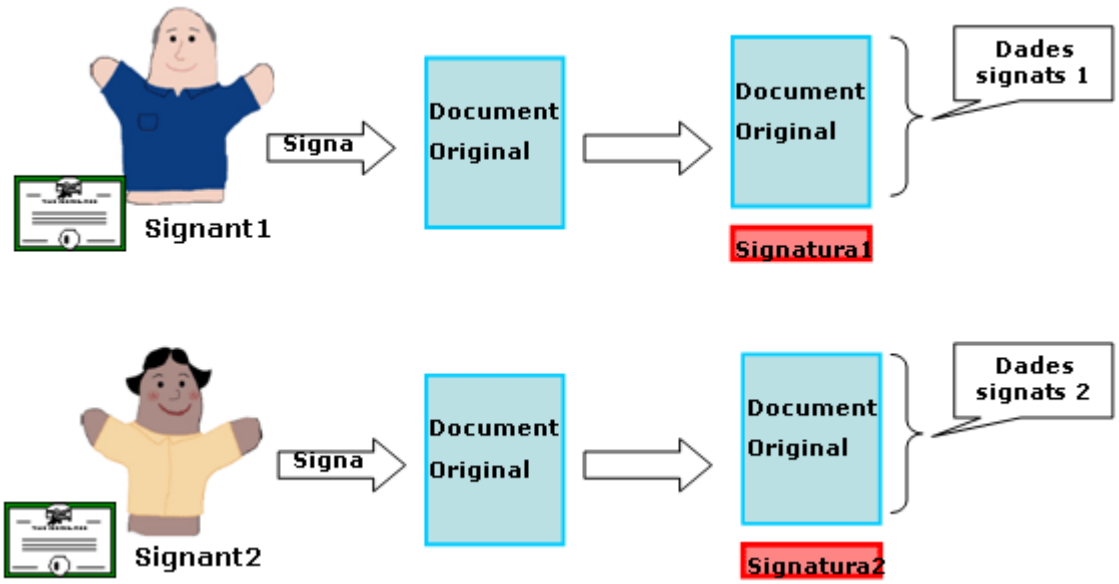
  Els documents en format S/MIME que hagin estat signats mitjançant PSA són compatibles - i les signatures es poden validar - amb les últimes versions dels gestors de correu electrònic Microsoft Outlook i Thunderbird.

- Resum criptogràfic de les dades. PSA també permet generar la signatura a partir del resum criptogràfic de les dades a signar.

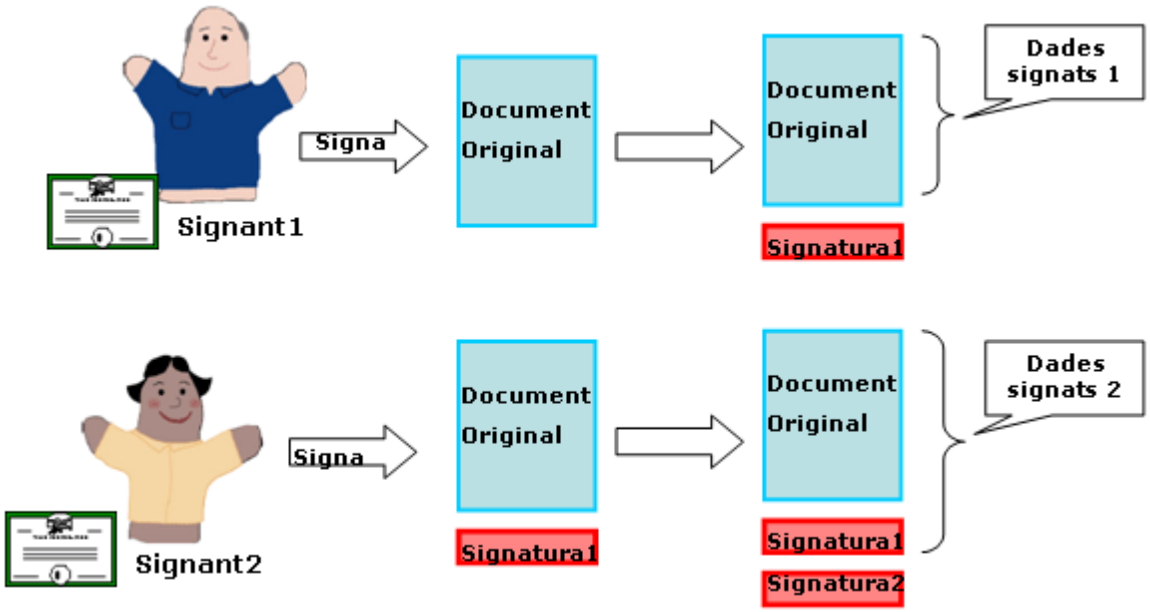
2.5 Quins models de signatura múltiple permet PSA?

Les signatures múltiples es poden classificar en funció de les dades que han estat signades.

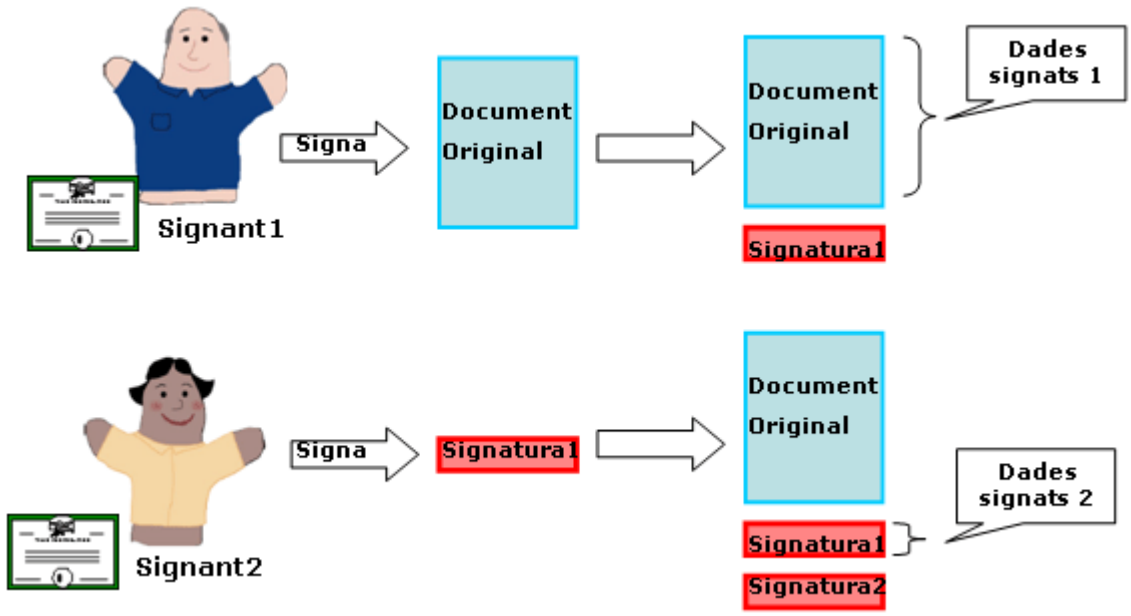
- Co-Signatura. Una signatura múltiple de tipus "co-signada" és una signatura on diversos signants signen el mateix document o dades. En aquesta signatura, l'ordre de les signatures no té importància, ja que no es requereix cap informació en relació al signant anterior per a la realització de la signatura actual. De la mateixa manera, tampoc és important l'ordre per a la validació posterior de les signatures, ja que aquestes validacions són de tipus individual.



- Re-Signatura. Una signatura múltiple de tipus "re-signada" és una signatura on varis signants signen el mateix document o dades originals juntament amb les signatures realitzades anteriorment. En aquesta signatura, l'ordre de les signatures sí que és important, reconeixent tant la signatura anterior com les dades que aquesta ha signat, que en el primer dels casos seran les dades inicials. En aquest tipus de signatura és important també l'ordre de la validació de la signatura, la qual s'ha de realitzat començant per l'última signatura fins a la inicial, tenint en compte quina és la informació que ha estat signada per cada signatari.



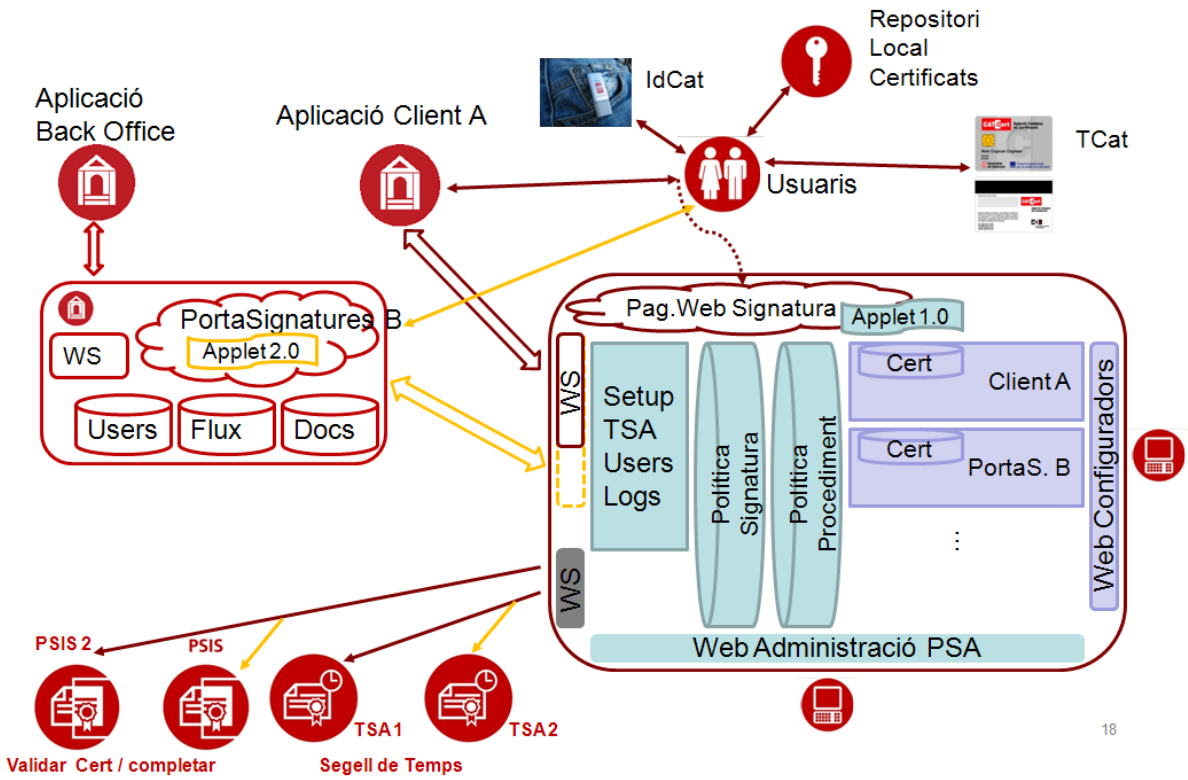
- Counter-Signatura. Una signatura múltiple de tipus “counter-signature” és un cas concret de signatura de tipus re-signatura. La peculiaritat d’aquestes signatures és que en una signatura es pot escollir si el que es vol signar és el document original i les signatures anteriors (mateix cas de la re-signatura) o únicament la signatura anterior



En els formats de documents propietaris (PDF, Open XML i Open Document) no tots els formats de signatura múltiple estan permesos.

2.6 Com integrar-se amb PSA?

PSA és un programari reactiu ideat com a component de back-office per a les aplicacions. **Les aplicacions es comuniquen amb PSA mitjançant serveis web**. La generació de la signatura però es porta a terme sempre en servidor.



L'explicació de com integrar-se està recollida en detall en la Guía_Integració_PSA. En aquesta mateixa guia també s'explica la missatgeria per fer-ne ús.

2.7 Quines tecnologies estan suportades per la integració amb PSA?

Actualment la Guia_Integració_PSA recull el pas a pas per a la integració amb les tecnologies Java i .NET. Qualsevol altre tecnologia que permeti la generació de clients de serveis web a partir de WSDL i suporti seguretat amb Web Service Security, també podrà integrar-se amb PSA.

2.8 Quins són els requeriments pels usuaris finals?

Els usuaris a signar amb un certificat personal simplement necessitaran l'ús d'un navegador actualitzat (Internet Explorer, Mozilla Firefox, Google Chrome, Opera), i la JRE 1.5 o superior. La signatura la realitza l'eina Signador, versió APSA-Light. Per a més informació sobre el Signador, consulta la web del CAOC.

2.9 Què és una política de signatura?

S'entén per política de signatura el document que recull tota la informació relativa al conjunt de regles que s'han d'aplicar per la creació i validació de les signatures electròniques, sota les quals es considera la validesa de les mateixes.

2.10 Què és una política de procediment?

Nom antic amb que ens referíem a les polítiques de signatura múltiple.

2.11 Què és una política de signatura múltiple?

S'entén per política de signatura múltiple el document que recull tota la informació relativa a les especificacions de l'ordre i disposició dels signants així com de les polítiques de signatura a utilitzar en realitzar un procediment administratiu.

PSA dóna suport a la gestió de polítiques de signatura múltiple, de manera que les aplicacions client li poden delegar les complexes tasques de gestió involucrades en la generació de diferents variants de signatures: solidàries, mancomunades, etc.

2.12 Què hem de fer per fer servir PSA?

Les passes a realitzar són:

– Omplir i signar una fitxa de sol·licitud del servei PSA. Aquesta fitxa està disponible a EACAT.

– Integració amb els serveis web de PSA (seguint la guia d'integradors per Java 5, Java 6, o .NET). Es posa també a disposició dels clients uns projectes per Java 5, Java 6 i .NET, que poden servir de guia, i que simplifiquen enormement els passos de la integració. En aquest cas no cal que els clients segueixin els passos de la guia d'integració. Han de consultar però aquesta guia per la descripció de la missatgeria dels serveis web.

– Definir polítiques de signatura i signatura múltiple per a cada tràmit de l'ens. Les polítiques les defineix el Consorci AOC.

– El client ha de proporcionar el certificat d'aplicació amb el qual la seva aplicació s'autenticarà a PSA. AOC haurà de donar d'alta a PSA l'aplicació del client.

– En cas de voler realitzar signatures desatesa, proveir els certificats a PSA i signar l'autorització corresponent.

2.13 On podem obtenir la fitxa d'alta a PSA?

Actualment el servei de PSA no s'ofereix a nous clients.

2.14 Vols estar informat sobre les intervencions al servei de PSA?

Existeix un grup de distribució de notificacions sobre les intervencions al servei de PSA. Si vols estar informat, sol·licita a suport@aoc.cat la incorporació de la teva compte de correu.

2.15 Amb quins certificats pot signar un usuari?

Un usuari pot signar amb qualsevol certificat que tingui carregat al repositori del seu navegador, i amb qualsevol dispositiu criptogràfic que segueixi l'estàndard PKCS#11 o CSP. És a dir, que sigui reconegut pels navegadors Explorer i Firefox. Per exemple, amb targeta criptogràfica o amb el clauer idCAT.

2.16 Es pot cancel·lar un procés de signatura un cop sol·licitat a PSA?

És possible, però no és necessari. PSA no és un magatzem de documents ni de signatures, i passat un temps (configurat a nivell d'instància) els processos de signatura s'esborren automàticament.

2.17 Quin és el paper de PSA en el cas de la signatura en local?

PSA no fa diferències entre signatura en local o remota. Primer s'hauria de definir clarament que és local i que és remota, perquè es podria malentendre (si l'usuari està a casa seva amb el seu PC, que és local o remota?) .

En PSA parlem de signatura d'usuari en browser, i de signatura destesa amb certificat a PSA.

En la signatura en browser qui signa és un usuari (persona) amb un certificat que té disponible a l'equip on està treballant, ja sigui un dispositiu criptogràfic – targeta – connectat a un lector, el seu idCAT personal, o claus carregades al repositori local de l'equip. El client signa (xifra les dades) des del seu navegador mitjançant el Signador de PSA, que es descarrega de forma automàtica i transparent. Més tard, és PSA qui porta a terme el procés de generació de la signatura fent us de les dades xifrades pel client.

La signatura desatesa no requereix d'interacció amb l'usuari. Les claus estan prèviament carregades a PSA, i tot el procés de signatura es porta a terme a PSA.

2.18 Què és el context de signatura i per a què serveix?

Quan parlem de context de signatura ens referim a les característiques tècniques i/o formals que s'han de considerar per tal que la signatura compleixi amb els requeriments que es deriven de la normativa jurídica aplicable a cada acte documentat. El context d'una signatura el marca el tràmit que s'està signant i això internament PSA ho recull amb una política de signatura múltiple.

Aquesta política de signatura múltiple indica a PSA quin tipus de document es vol signar, en quin format, com es vincula amb el document, quants signataris hi ha, etc. Per cada signatari podem tenir una política de signatura – segons recull l'ETSI – que indica quins certificats i Autoritats de Certificació seran admesos, quins atributs s'han de signar, si s'agafen compromisos (commitments), amb quins mecanismes s'han de validar els certificats, quines fonts de temps fiable són vàlides, etc.

2.19 El Signador pot substituir a PSA?

Conceptualment són totalment diferents. L'objectiu és recolzar i actualitzar constantment PSA. PSA es recolza per la part de xifrat en client en una versió més senzilla del Signador (la que en aquest document hem anomenat versió APSA-Light), i la construcció de la

signatura es fa en servidor. Això permet a PSA més potència de càlcul, de la qual queda alliberada la part que s'executa a nivell de client. A nivell funcional, i per clarificar la comparativa, recollim un esquema comparatiu de PSA amb l'applet APSA-Light (que és l'applet de xifrat que va ser substituït pel Signador versió APSA-Light):

PSA (Programari de Signatura Avançada)

- Necessitats de negoci amb signatures múltiples (fluxos de signatura)
- Ús de polítiques de signatura estàndard
- Signatura amb validació posterior a PSIS integrada
- Generació de comprovants de signatura
- Signatura d'open document i office 07
- Xifrat de documents
- Actualitzacions a nous formats de signatura futurs

A nivell tècnic, també hi ha diferències. A continuació en fem també una comparativa:

Aspectes Tècnics	Eina Web de Signatura-e	PSA
Cost implantació:	+ Instal·lar llibreries i parametritzar la crida a l'applet	- Integrar Serveis Web
Comunicacions per operar: -Pes de l'applet a descarregar al client -Descarregar el fitxer al client	- 3,9 MB Mida del fitxer, hash	+ 0,06 MB Hash
Java	= 1.5 +	= 1.5 +
Sistemes operatius	= qualsevol	= qualsevol
Magatzem Certificats Windows Magatzem Certificats Firefox	= +	= +
Mida màxima del document a signar	- Depen de la maquina virtual (<40MB)	+ No afecta
Ús de polítiques	-	+
Connexió a internet de l'usuari	Si, quan fa ús de segell de temps	Si, quan es fa signatura en browser

Llegenda: + positiu, = igual, - negatiu

2.20 Pot PSA tenir certificats de nivell 4 o en hardware criptogràfic?

No, PSA només pot tenir certificats en software fins a nivell 3. PSA actualment no disposa de connexió a un dispositiu criptogràfic segur.

2.21 Qui valida els certificats utilitzats a PSA?

PSA utilitza internament PSIS per a la validació de certificats i de les signatures generades.

2.22 Quina diferència hi ha entre les crides de servei web "Init..." i les de "Continue..."?

Les peticions "Init..." són sempre les inicials. En aquestes crides inicials cal fer la transferència de les dades a signar a PSA (ja sigui document/s o hash/s). Com a resposta, PSA retornarà l'identificador del context de signatura.

Les peticions "Continue..." només es fan servir si cal que intervinguin 2 o més signataris. A la petició caldrà indicar l'identificador del context, per tal que PSA pugui relacionar el signatari amb el context de signatura.

2.23 Si es fa servir la funcionalitat de signatura en manager, què és millor: fer N crides de servei web amb 1 document o una crida amb N documents?

Si fem servir 1 crida amb N documents, la política a utilitzar ha de ser la mateixa per a tots els documents, i s'han de signar tots o cap (no tenim la possibilitat de fer tria). En aquesta

opció només s'ha de passar 1 certificat d'usuari (ja que serà el mateix per tots els documents) i PSA retornarà l'identificador de context amb els N hashs.

Si fem N crides amb 1 document, cada crida pot tenir la seva pròpia política i l'usuari pot triar entre realitzar o no la signatura de cada document. Per contra, s'haurà d'enviar el certificat de l'usuari en cada petició i s'obtindran N identificadors de context.

2.24 Quina paràmetres es poden passar a PSA per a la configuració de la signatura visible en PDF?

A PSA se li pot indicar:

- Coordenades de la capsa de signatura.
- Dades a mostrar a la signatura: nom, cognoms, títol, organització, número de sèrie, localització, motiu de la signatura, CommonName, i número de sèrie del certificat.
- Imatge a mostrar a la signatura.
- Data de la signatura.

O bé es pot especificar:

- Nom del camp de signatura, si aquest ja existeix.

2.25 Què succeeix si es demana signatura de PDF visible, indicant que es posi en un camp de signatura (en lloc d'unes coordenades) i aquest camp no existeix?

PSA retornarà un error i no generarà la signatura.