Resolució d'incidències – ALERTES PSIS

ÍNDEX

1 Introducció

PSIS (Plataforma de Serveis d'Identificació i Signatura) és la plataforma tecnològica des d'on es presta el servei de validació.

El servei de validació (en endavant PSIS) ofereix principalment la validació de certificats i signatures digitals. També permet la creació i validació de segells de temps, i la creació de signatures digitals de forma segura i desatesa.

L'objectiu del present document és definir el procediment d'actuació dels tècnics davant la recepció dels correus d'error de la sonda de monitorització del servei web de PSIS.

Aquesta sonda envia un conjunt de transaccions de servei web via IP pública a la plataforma de PSIS. La sonda de monitorització de servei està ubicada al CPD d'NTT.

2 Sonda

La sonda de serveis web s'executa cada 10 minuts, i es llencen un conjunt de transaccions que recullen validació de certificats i signatures, i creació i validació de segells de temps.

2.1 Transaccions

Les transaccions que es llencen per PSIS són les següents:

Nom	Descripció	Protocol	Endpoint
ID-300 AVS Certificate CPISR1 OK	Validació d´un certificat de persona física de classe 1 (CPISR-1) vàlid.	DSS	http://217.111.232.27/psis/catcert/dss
ID-301 AVS Certificate CPISR1 REV	Validació d´un certificat de persona física de classe 1 (CPISR-1) revocat.	DSS	http://217.111.232.27/psis/catcert/dss
ID-302 AVS Certificate FNMT OK	Validació d´un certificat de la FNMT (Fábrica Nacional de Moneda y Timbre) vàlid.	DSS	http://217.111.232.27/psis/catcert/dss
ID-313 AVS Certificate eDNI OK	Validació d´un certificat eDNI vàlid.	DSS	http://217.111.232.27/psis/catcert/dss
ID-303 AVS CMS Signature Detached CPISR1 OK	Validació d´una signatura CMS detached vàlida, generada amb un certificat de persona física de classe 1 (CPISR-1).	DSS	http://217.111.232.27/psis/catcert/dss
ID-314 AVS CAdES-BES Signature Detached Hash CPISR1 OK	Validació d´una signatura CAdES-BES detached vàlida, generada amb un certificat de persona física de classe 1 (CPISR-1).	DSS	http://217.111.232.27/psis/catcert/dss
ID-304 AVS XML Signature Detached CPISR1 OK	Validació d´una signatura XML detached vàlida, generada amb un certificat de persona física de classe 1 (CPISR-1).	DSS	http://217.111.232.27/psis/catcert/dss
ID-311 AVS XAdES-T Signature Detached Hash CPISR1 OK	Validació d´una signatura XAdES-T detached vàlida, generada amb un certificat de persona física de classe 1 (CPISR-1).	DSS	http://217.111.232.27/psis/catcert/dss
ID-312 AVS XAdES-T Signature Detached Hash Signed Response CPISR1 OK	Validació d´una signatura XAdES-T detached vàlida, generada amb un certificat de persona física de classe 1 (CPISR-1). Sol·licitud de resposta signada.	DSS	http://217.111.232.27/psis/catcert/dss

ID-305 TSA RFC3161 Request	Generació de TimeStamp mitjançant el protocol RFC3161.	TSP	http://217.111.232.27/psis/catcert/tsp
ID-306 TSA CMS Verify TimeStamp PSISTSA OK	Validació d´un TimeStamp CMS vàlid.	DSS	http://217.111.232.27/psis/catcert/dss
ID-307 TSA XML Verify TimeStamp PSISTSA OK	Validació d´un TimeStamp XML vàlid.	DSS	http://217.111.232.27/psis/catcert/dss
ID-308 TSA CMS Create TimeStamp	Creació d´un TimeStamp CMS.	DSS	http://217.111.232.27/psis/catcert/dss
ID-309 TSA XML Create TimeStamp	Creació d´un TimeStamp XML.	DSS	http://217.111.232.27/psis/catcert/dss

Les transaccions, com veiem a la taula anterior, fan servir els protocols següents:

- DSS → Protocol Digital Signature Services d'OASIS. Missatgeria XML.

  Més informació a: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss
- TSP → Protocol que segueix les recomanacions del RFC3161 (Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)).

  Més informació a: https://www.ietf.org/rfc/rfc3161.txt

I els endpoints que es sonden són aquests:

- Per missatgeria DSS: http://217.111.232.27/psis/catcert/dss
- Per missatgeria RFC3161: http://217.111.232.27/psis/catcert/tsp

2.2 Correus d'alerta

Quan la sonda enregistra un error, s'envia un e-mail d'alerta. S'envia un e-mail diferent per cada transacció que falli.

Els correus d'incidència tenen aquest format:

- L'assumpte serà "*ALERTA SERVEI PSIS-ATLAS PRODUCCIO*".
- Al cos del missatge, s'especifica l'entorn (ATLAS PRODUCCIÓ), i la transacció sobre la que s'ha enregistrat l'error. En l'exemple:

  ID-309 TSA XML Create TimeStamp

  Això vol dir que és la transacció amb identificador "309", i que és la creació d'un segell de temps.
- Al cos del missatge s'inclouen els últims resultats erronis recollits per aquella transacció concreta després de l'últim resultat satisfactori, amb un màxim de fins a 5 (poden haver-hi més, però només es reporten al correu els últims 5). Els errors s'eliminen quan es recull un resultat satisfactori. Per tant, els que estiguin inclosos al correu seran sempre errors consecutius.

```
-----Mensaje original-----
De: Operacions Sistemes Consorci AOC
Enviado el: domingo, 30 de abril de 2017 15:59
Para: Aurea Alcaide <aalcaide@aoc.cat>
Asunto: ALERTA SERVEI PSIS-ATLAS PRODUCCIO

Entorn:      PSIS-NEXTRET PRODUCCIO
Transaccio: ID-309 TSA XML Create TimeStamp

Resultats de les ultimes transaccions:

Data:                    29/04/2017 16:12
Temps de resposta:  -
Resultat:                KO
Error:              Could not invoke service.. Nested exception is
org.codehaus.xfire.fault.XFireFault: Couldn't send message.

Data:                    29/04/2017 12:12
Temps de resposta:  -
Resultat:                KO
Error:              Could not invoke service.. Nested exception is
org.codehaus.xfire.fault.XFireFault: Couldn't send message.

Data:                    29/04/2017 12:02
Temps de resposta:  -
Resultat:                KO
Error:              Could not invoke service.. Nested exception is
org.codehaus.xfire.fault.XFireFault: Couldn't send message.

Data:                    29/04/2017 11:52
Temps de resposta:  -
Resultat:                KO
Error:              Could not invoke service.. Nested exception is
org.codehaus.xfire.fault.XFireFault: Couldn't send message.

Data:                    29/04/2017 11:42
Temps de resposta:  -
Resultat:                KO
Error:              Could not invoke service.. Nested exception is
org.codehaus.xfire.fault.XFireFault: Couldn't send message.

Procediment de restauracio del servei:
http://172.18.2.25/wiki/index.php5/P%C3%A1gina_Principal
```

2.3 Consola web

URL d'accés a la consola de la sonda:

http://10.124.95.14:8080/monitors/

Per poder accedir a aquesta URL cal que us connecteu a la VPN del Consorci AOC. Cal fer servir el client de **GlobalProtect**, i accedir a la URL del portal **vpn-ssl.aoc.cat** amb l'usuari i contrasenya corresponents.

A la home, clicar a "**CONSOLA**". Un cop dins de Consola, teniu el llistat de les categories de serveis que es sonden. En aquest cas PSIS pertany a la categoria "**Signatura electrònica**". Veureu que hi ha un **PSIS_Atlas** (entorn primari) i un **PSIS_Nextret** (entorn secundari). El que us interessa a vosaltres és únicament PSIS_Atlas.

La consola ens mostra totes les transaccions del servei, pels entorns de PRODUCCIÓ i de PREPRODUCCIÓ:

Consorci Administració Oberta de Catalunya

Servei de Monitorització

CONSOLA

Seleccioni la transacció de la que vol consultar les estadístiques:

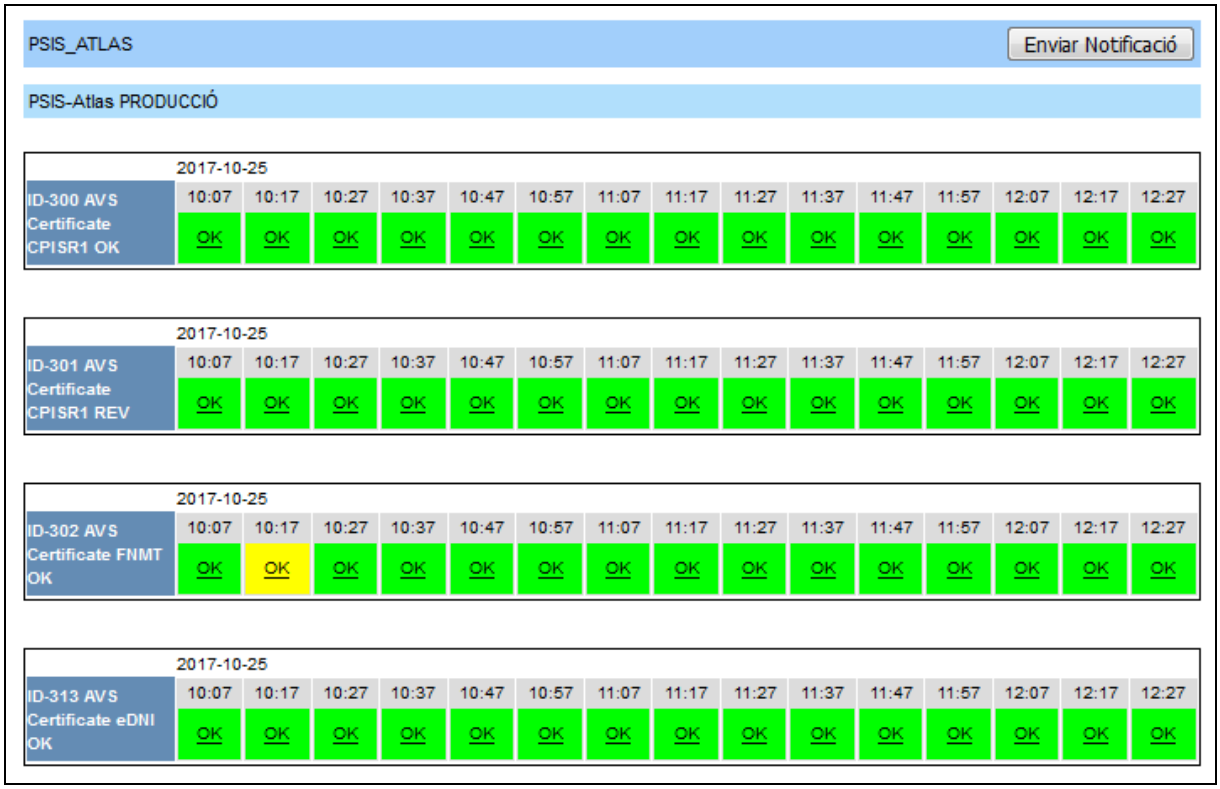
SERVEI	ENTORN	TRANSACCIÓ
PSIS_ATLAS	PRODUCCIÓ	ID-300 AVS Certificate CPISR1 OK
		ID-301 AVS Certificate CPISR1 REV
		ID-302 AVS Certificate FNMT OK
		ID-313 AVS Certificate eDNI OK
		ID-303 AVS CMS Signature Detached CPISR1 OK
		ID-314 AVS CAdES-BES Signature Detached Hash CPISR1 OK
		ID-304 AVS XML Signature Detached CPISR1 OK
		ID-311 AVS XAdES-T Signature Detached Hash CPISR1 OK
		ID-312 AVS XAdES-T Signature Detached Hash Signed Response CPISR1 OK
		ID-305 TSA RFC3161 Request
		ID-306 TSA CMS Verify TimeStamp PSISTSA OK
		ID-307 TSA XML Verify TimeStamp PSISTSA OK
		ID-308 TSA CMS Create TimeStamp
		ID-309 TSA XML Create TimeStamp
	PREPRODUCCIÓ	ID-350 AVS Certificate CPISR1 OK
		ID-351 AVS Certificate CPISR1 REV
		ID-352 AVS Certificate FNMT OK
		ID-363 AVS Certificate eDNI OK
		ID-353 AVS CMS Signature Detached CPISR1 OK
		ID-364 AVS CAdES-BES Signature Detached Hash CPISR1 OK
		ID-354 AVS XML Signature Detached CPISR1 OK
		ID-361 AVS XAdES-T Signature Detached Hash CPISR1 OK
		ID-362 AVS XAdES-T Signature Detached Hash Signed Response CPISR1 OK
		ID-355 TSA RFC3161 Request
		ID-356 TSA CMS Verify TimeStamp PSISTSA OK
		ID-357 TSA XML Verify TimeStamp PSISTSA OK
		ID-358 TSA CMS Create TimeStamp
		ID-359 TSA XML Create TimeStamp

Últims resultats

Tots els resultats (màxim fins a 999) entre 25/10/2017 00:00 i 25/10/2017 12:25

Enviar

Les seleccionem totes i cliquem “Enviar”. La consola ens mostrarà per defecte els últims 15 resultats recollits de la sonda. Per exemple, per les 4 primeres transaccions:



L’ordre dels resultats mostrats és d’esquerra a dreta i d’abaix a dalt (en cas de que ser més de 15, es pintaran en una fila immediatament inferior). Els resultats més recents els tindrem sempre a la primera fila, a la dreta.

Com podem veure, per cada transacció seleccionada, es mostren per defecte els 15 últims resultats guardats en base de dades.

Cada requadre de color, indica el resultat d’una transacció.

Per cada requadre tenim la següent informació:

- Data i instant de temps en què es va llençar la transacció a la sonda.
- Resultat:

  OK: El resultat de la transacció ha sigut l’esperat.

  KO: La transacció no ha pogut ser processada, o sí que ha sigut processada però el resultat de la transacció no ha sigut l’esperat.
- Colors:

  El significat dels diferents colors amb què es pinten els requadres, és:

  - Verd: La transacció ha finalitzat satisfactòriament i el temps de resposta del servidor ha sigut inferior al marge de temps considerat “WARNING”.

- Groc: La transacció ha finalitzat satisfactòriament, però el temps de resposta del servidor ha sigut superior o igual al marge de temps considerat "WARNING", malgrat que inferior al marge de temps considerat "POOR".
- Vermell: La transacció ha finalitzat satisfactòriament, però el temps de resposta del servidor ha sigut superior o igual al marge de temps considerat "POOR", malgrat que inferior al marge de temps considerat "TIMEOUT".
- Negre: La transacció no ha finalitzat satisfactòriament, o s'ha produït un timeout. També si la transacció ha finalitzat satisfactòriament i el temps de resposta del servidor ha sigut igual o superior al marge de temps considerat "TIMEOUT".

Per últim, podem obtenir informació més concreta sobre cada resultat, clicant a sobre del text OK/KO de cada requadre. En clicar, s'obrirà un pop-up amb la següent informació:

RESULTAT DE LA TRANSACCIÓ	
NOM DE LA TRANSACCIÓ	ID-07 AVS Certificate FNMT OK
DATA	24-05-201700:12
RESULTAT	**OK**
TEMPS DE RESPOSTA	**1323 milisegons**

Marges temporals en milisegons	
Temps resposta OK:	t < 1500
Temps resposta WARNING:	1500< = t < 8000
Temps resposta POOR:	8000< = t < 45000
TIME OUT:	45000< = t

Com podem veure, tenim informació sobre els valors dels marges de temps OK, WARNING, POOR, i TIMEOUT per aquella transacció.

En cas de produir-se un error, també tindrem un camp "ERROR" que ens mostrarà el missatge d'error recollit per la sonda. Per exemple:

RESULTAT DE LA TRANSACCIÓ	
NOM DE LA TRANSACCIÓ	ID-07 AVS Certificate FNMT OK
DATA	23-05-201722:02
RESULTAT	**KO**
ERROR	expected:[...valid:certificate:Definitive] but was: [...unknown:certificate:PathValidationFails]
TEMPS DE RESPOSTA	**53306 milisegons**

Marges temporals en milisegons	
Temps resposta OK:	t < 1500
Temps resposta WARNING:	1500< = t < 8000
Temps resposta POOR:	8000< = t < 45000
TIME OUT:	45000< = t

2.4 Observacions

- La sonda s'executa cada 10 minuts i envia una alerta per cada transacció, amb cada KO recollit per aquella transacció concreta: al primer KO i mentre es produeixen KOs consecutius (cada 10 minuts).
- En casos en que la incidència sigui generalitzada o que no es tanqui de forma immediata, la sonda pot bombardejar amb alertes. Concretament, cada 10 minuts.
- Poden haver-hi falses alarmes si:
  - **a.** Hi ha problemes amb les línies de comunicacions d'NTT.
  - **b.** Si els certificats, signatures i/o segells de temps a validar caduquen.

3 Splunk

L'Splunk monitoritza en temps real totes les operacions que s'executen a PSIS.

La URL d'accés a l'Splunk és:

http://10.120.1.235/

Usuari: catcert

A la opció de menú "Producció", seleccionar "Temps Real – Entorn de Producció", per veure les operacions que s'estan processant a PSIS en temps real.

L'Splunk ens permet detectar si un node està caigut, o errors amb una entitat de certificació concreta, per exemple. Amb la sonda no és possible detectar aquests errors, doncs els certificats que valida la sonda són de CATCert, de la FNMT, i del DNIe, però no en valida de cap altre entitat de certificació. De la mateixa manera, si un node cau, automàticament és desbalanceja, amb la qual cosa la sonda no ho detectaria, doncs la seva petició seria atesa per un altre node.

És molt important accedir a l'Splunk per detectar clarament si el servei està caigut o no, el volum de peticions que estan arribant al servei i per node, i si tots els nodes estan funcionant correctament.

4 Procediment

A continuació es descriu el procediment a portar a terme en funció de la transacció que falli en cada cas, segons el cos del correu electrònic.

4.1 Pas 1 – Revisió alertes sistemes

Revisar estat de tots els monitors de sistema.

4.2 Pas 2 – Revisió de l'estat general de la sonda

Entrar a la web de consulta dels resultats de la sonda, i comprovar quin és l'estat general de PSIS.

4.3 Pas 3 – Comprovar si es tracta d'un problema de xarxa

En el cas de que totes les transaccions estiguin en estat KO, caldrà revisar si hi ha algun problema de xarxa: balancejadors, frontals web, servidors de DNS, etc...

- Comprovar si el WSDL del servei es pot descarregar.

  El WSDL està penjat a l'Apache, i està accessible des de la següent URL:

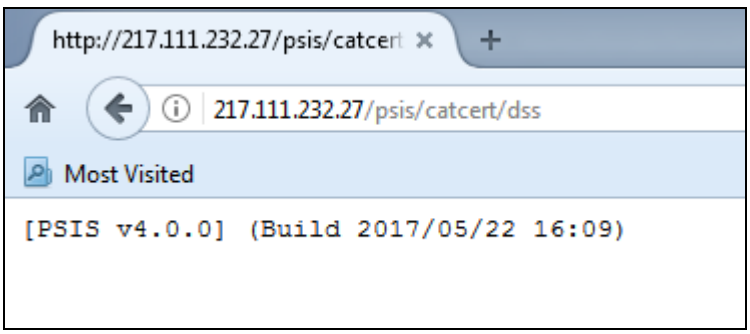
  http://217.111.232.27/wsdl/dss.wsdl

  Si no està accessible, comprovar DNS, balancejadors, i Apaches.

- Comprovar que el servei PSIS està accessible:

  http://217.111.232.27/psis/catcert/dss

  Ha d'aparèixer una plana del tipus:



  Com veiem apareix el nom de PSIS i la versió desplegada (en aquest cas, la 4.0.0).

  Podem provar per cadascun dels nodes, per veure si algun d'ells està donant problemes.

  http://10.124.18.11:8080/psis/catcert/tdss
  http://10.124.18.12:8080/psis/catcert/tdss
  http://10.124.18.13:8080/psis/catcert/tdss
  http://10.124.18.14:8080/psis/catcert/tdss

  Si tot és correcte, la plana que apareixerà ha de ser del mateix tipus que l'anterior.

4.4 Pas 4 – Revisió dels nodes de la plataforma

Revisar estat dels nodes de la plataforma des d'una màquina Windows (local) amb una JRE v.1.5 mínim instal·lada.

Repetir el següent procediment des de cada servidor d'aplicacions.

El projecte **SoapUI** de nom "**PSIS-Sonda**", executa les mateixes transaccions que es llencen periòdicament amb la sonda.

1. Obrir el projecte des de l'aplicatiu SoapUI.

2. Configurar a les propietats del projecte, l'adreça del servei que ens interessi:

   endpoint.dss

   IP pública del servei per l'endpoint "dss", o directament IP del JBoss de cadascun dels nodes. Els possibles valors són:

   Frontal: http://217.111.232.27/psis/catcert/dss
   Node 1: http://10.124.18.11:8080/psis/catcert/tdss
   Node 2: http://10.124.18.12:8080/psis/catcert/dss
   Node 3: http://10.124.18.13:8080/psis/catcert/dss
   Node 4: http://10.124.18.14:8080/psis/catcert/dss

   endpoint.tsp

   Ídem per l'endpoint "tsp":

   Frontal: http://217.111.232.27/psis/catcert/tsp
   Node 1: http://10.124.18.11:8080/psis/catcert/tsp
   Node 2: http://10.124.18.12:8080/psis/catcert/tsp
   Node 3: http://10.124.18.13:8080/psis/catcert/tsp
   Node 4: http://10.124.18.14:8080/psis/catcert/tsp

3. Llençar els tests

   Podem comprovar l'estat del servidor en funció dels resultats dels tests.

   Si tots els tests s'executen de manera que totes les assercions són correctes i els temps de resposta no superen els 5 segons, voldrà dir que els JBoss estan treballant correctament.

   Cas que no, depenent del tipus d'error, conclourem si el servidor està treballant correctament o no. Encara que alguna asserció falli, observar a la resposta de PSIS el contingut del camp *ResultMessage* per si aporta informació de l'error.

   Comprovar també quin error queda enregistrat al server.log del JBoss.

   Si les transaccions que fallen són només ID-302 i ID-313, segurament el problema estarà en el consum de serveis de tercers. Aleshores, anar directament al punt 0.

4. Si algun node no està responent correctament, reiniciar-lo.

   a. ***/etc/init.d/jboss stop***

   b. Si el procés no finalitza, caldrà eliminar-lo (en cas d'haver hi un procés JBoss actiu)

   ps xua | grep jboss i fer un ***kill -9 pid_process***

c. ***/etc/init.d/jboss start***

d. Comprovar que l'aturada i l'arrencada del JBoss és correcta consultant el server.log:

tailf /srv/application/logs/PsisServer/server.log

4.5 Pas 5 – Comprovar si es tracta d'un problema de base de dades

Consultar el server.log del JBoss per comprovar si hi ha errors d'Oracle (ORA-). En cas de que així sigui, depenent de l'error, caldrà o no reiniciar la instància.

- Comprovar que totes les instàncies estan activades. Tots els serveis han d'estar ONLINE.
- Reiniciar les instàncies de base de dades, si s'escau.
- Qualsevol dubte escalar al DBA que estigui disponible.

4.6 Pas 6 – Revisió de serveis de tercers

Actualment PSIS es recolza en un parell de serveis externs per:

- Validar certificats de la FNMT i certificats no classificats: **@firma**
- Validar el DNIE: **OCSP del DNIE**

Les transaccions que poden fallar per errors d'aquests serveis de tercers són:

ID-302 AVS Certificate FNMT OK → PSIS en aquest cas consumeix ***@firma***.

ID-313 AVS Certificate eDNI OK → PSIS en aquest cas consumeix el servei ***OCSP del DNIE***.

Caldrà revisar la connectivitat dels servidors d'aplicacions amb aquests serveis.

La casuística es pot tractar via *telnet* o mitjançant un gestor de baixades, cas del *wget* (permet la baixada de continguts web).

4.6.1 @firma

Revisar connectivitat dels servidors d'aplicació de la plataforma amb la URL:
https://afirma.redsara.es/afirmaws/services/DSSAfirmaVerifyCertificate

NOTA: Cal tenir en compte que PSIS accedeix al servei d'@firma mitjançant la xarxa SARA. Al fitxer ***/etc/hosts*** tenim la següent entrada:
10.127.32.124 afirma.redsara.es

Per revisar la connectivitat amb @firma:

1. Executar la comanda:

   telnet afirma.redsara.es 443

```
[jboss@psis01c ~]$ telnet afirma.redsara.es 443
Trying 10.127.32.124...
Connected to afirma.redsara.es.
Escape character is '^]'.
```

Alternativament, també podem provar amb la comanda wget:

wget https://afirma.redsara.es/afirmaws/services/DSSAfirmaVerifyCertificate

```
[jboss@psis01c ~]$ wget https://afirma.redsara.es/afirmaws/services/DSSAfirmaVerifyCertificate
--2017-05-29 10:37:38--  https://afirma.redsara.es/afirmaws/services/DSSAfirmaVerifyCertificate
Resolving afirma.redsara.es... 10.127.32.124
Connecting to afirma.redsara.es|10.127.32.124|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 150 [text/html]
Saving to: âDSSAfirmaVerifyCertificate.1â

100%[======================================================================>] 150         --.-K/s   in 0s

2017-05-29 10:37:38 (30.7 MB/s) - âDSSAfirmaVerifyCertificate.1â
```

2. Si falla i és un problema del servidor destí, obrir tiquet al *Centro de Atención a Integradores y Desarrolladores* (CAID) del Ministerio de Hacienda y Adminsitraciones Públicas (MINHAPF):

   https://ssweb.seap.minhap.es/ayuda/consulta/CAID

   Especificar:

   - Organisme: ***Consorci AOC***
   - Aplicació/servei : ***@firma: Validación de certificados y firmas***
   - Entorn afectat: ***Producción***
   - El cos del missatge podria ser:

> Buenos días,
>
> Les escribo desde el departamento de Operaciones del Consorcio AOC. Nuestro validador PSIS utiliza @firma para la validación de certificados de la FNMT.
>
> Tenemos problemas con el acceso al servicio: https://afirma.redsara.es/afirmaws/services/DSSAfirmaVerifyCertificate
>
> ¿Nos podrían confirmar si el servicio está operativo en este momento?
>
> En caso de que no lo esté, ¿qué previsión de restablecimiento del mismo nos pueden dar?
>
> Atentamente,
>
> Operacions – AOC

4.6.2 DNIE

Revisar connectivitat dels servidors d'aplicacions de la plataforma amb la URL: http://ocsp.dnie.es/.

1. Executar la comanda:
   telnet ocsp.dnie.es 80

```
[jboss@psis01c ~]$ telnet ocsp.dnie.es 80
Trying 193.104.0.240...
Connected to ocsp.dnie.es.
Escape character is '^]'.
```

Alternativament, també podem provar amb la comanda wget:
wget http://ocsp.dnie.es/

```
[jboss@psis01c ~]$ wget http://ocsp.dnie.es
--2017-05-29 10:39:59--  http://ocsp.dnie.es/
Resolving ocsp.dnie.es... 193.104.0.240
Connecting to ocsp.dnie.es|193.104.0.240|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://www.cert.fnmt.es/welcome-ocsp.html [following]
--2017-05-29 10:39:59--  http://www.cert.fnmt.es/welcome-ocsp.html
Resolving www.cert.fnmt.es... 193.104.0.210
Connecting to www.cert.fnmt.es|193.104.0.210|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: âwelcome-ocsp.html.3â

    [ <=>                                                                ] 32,142      --.-K/s   in 0.1s

2017-05-29 10:40:00 (284 KB/s) - âwelcome-ocsp.html.3â
```

2. Si falla i és un problema del servidor destí:
   a. **Horari laborable (de 8 a 19h)**

      Trucar al **902 364 444**

      Si no hi ha resposta a la trucada, enviar e-mail:

> Para: soportetecnico@dnielectronico.es,
> oficinatecnica@dnielectronico.es
>
> CC: OperacionsAOC@aoc.cat
>
> Asunto: Problemas de acceso al servicio http://ocsp.dnie.es
>
> Mensaje:
>
> Les escribo desde el departamento de Operaciones del Consorcio AOC (Consorcio de Administración Abierta de Catalunya). Desde nuestro validador PSIS tenemos problemas con el acceso al servicio http://ocsp.dnie.es. ¿Nos podrían confirmar si el servicio está operativo en este momento? En caso de que no, ¿qué previsión de restablecimiento del mismo nos pueden dar?
>
> Muchas gracias por adelantado.
>
> Atentamente,
>
> Soporte PSIS-AOC

   b. ***Horari no laborable***

      Enviar e-mail.