Open-VA 1.1

Sumari

Capítol 1. Introducció

Benvingut al manual d'usuari d'Open-VA 1.1.

Aquest document explica com instal·lar, configurar i usar Open-VA.

Característiques principals

Open-VA és un codi obert que demostra com implementar un sistema per a validar certificats digitals i documents signats.

Pot usar i estendre'l com desitgi.

Avís

Si fa servir Open-VA, o la distribueix, li agrairíem que inclogués el logo *powered by Open-VA* (veure més avall). Pot trobar aquest logo (`open-VA.gif`) en el seu directori d'instal·lació d'Open-VA. (Veure *document llicència* per les condicions d'us)

Open-VA usa un *WebService* com a frontal i un protocol molt simple com a transport.

Pot usar Open-VA per obtenir l'arxiu `WSDL` i construir els seus propis clients Open-VA.

Sobre aquest manual d'usuari

Aquest manual li dona una visió complerta d'Open-VA. Explica com instal·lar, configurar i usar Open-VA i assumeix que està familiaritzat amb el seu sistema operatiu i conceptes relacionats amb servidors d'aplicacions, servidors de bases de dades i servidors ldap.

El manual d'usuari d'Open-VA està format per:

- *Capítol 1 - Introducció*: Ho està llegint.
- *Capítol 2 - Instal·lació*: Defineix requeriments de plataforma i com preparar els components requerits abans de construir i instal·lar Open-VA.
- *Capítol 3 - Usant Open-VA*: Describeix el protocol Open-VA i com usar-ho.

Capítol 2. Instal·lació

Aquest capítol explica requeriments de sistema i plataforma i procediments d'instal·lació. També proveeix instruccions per a obtenir els components requerits.

Requeriments d'instal·lació

Requeriments de plataforma

Open-VA és una aplicació *multiplataforma* que *no requereix* res en especial de la seva plataforma.

Components requerits

Els components requerits per Open-VA (no subministrats) son:

- Java Software Development Kit (*JSDK*)
- Java Enterprise Edition Application Server (*servidor JEE*)
- Lighweight Directory Access Protocol server (*servidor LDAP*)
- Database server

Requeriment JSDK

Es necessita una JSDK versió 1.4. Els arxius de política de seguretat sense restricció han d'estar instal·lats i BouncyCastle ha d'estar registrat com un proveïdor de seguretat.

Hauria d'assegurar que el seu sistema té una variable d'entorn anomenada `JAVA_HOME` la qual ha esta definida amb el directori d'instal·lació del seu JSDK.

Avís

Aquesta versió no funciona amb altra versió diferent a la 1.4.

Instal·lant la versió JSDK 1.4 de SUN

Pot descarregar-la des de SUN download website [http://java.sun.com/j2se/1.4.2/download.html].

Després de la instal·lació recordi definir la variable d'entorn `JAVA_HOME` tal i com s'ha explicat a la secció anterior.

Instal·lant els Arxius de Política sense Restricció

Per defecte la descàrrega de JSDK inclou arxius de política restringits, els quals no permeten l'us de claus de gran longitud. Per permetre claus de qualsevol longitud ha d'instal·lar els arxius de política sense restricció.

Descarregui'ls des de JCE download website [http://java.sun.com/j2se/1.4.2/download.html#docs] i segueixi les instruccions.

Registrant BouncyCastle

Open-VA requereix BouncyCastle com a proveeïdor de seguretat. Per poder fer-ho ha de seguir els següents punts:

1. Descarregar i instal·lar les llibreries BouncyCastle

2. Registrar BouncyCastle com un proveeïdor de seguretat

Pot descarregar les llibreries BouncyCastle (`bcprov.jar` and `bcmail.jar`) des de BouncyCastle download website [http://www.bouncycastle.org/latest_releases.html]. Un cop fet copíï ambdos arxius a la carpeta `jre/lib/ext` sota el directori d'instal·lació del seu JSDK.

Un cop feta la descàrrega i instalació ha de registrar BouncyCastle com un proveeïdor de seguretat editant l'arxiu de seguretat del seu JSDK. Aquest arxiu és `java.security` i el pot trobar a la carpeta `jre/lib/security` sota el directori d'instal·lació del seu JSDK.

Avís

SUN ha de ser el primer proveeïdor i BouncyCastle el segon. Cerqui les entrades security.provider y editi-les como segueix:

```
...altres entrades ...

security.provider.1=sun.security.provider.Sun
security.provider.2=org.bouncycastle.jce.provider.BouncyCastleProvider
security.provider.3=com.sun.net.ssl.internal.ssl.Provider
security.provider.4=com.sun.rsajca.Provider
security.provider.5=com.sun.crypto.provider.SunJCE
security.provider.6=sun.security.jgss.SunProvider

... altres entrades ...
```

Requeriment servidor JEE

Es requereix un servidor compatible con JEE 1.4.

Amb aquest entrega d'Open-VA es fa servir un servidor d'aplicacions JBoss. Si desitja un altre, haurà de subministrar els descriptors vostè mateix.

Instal·lant el servidor JBoss

Pot descarregar un servidor JBoss (4.02 o major recomanat) des de JBoss download website [http://labs.jboss.com/portal/jbossas/download/index.html].

Requeriment servidor LDAP

No es requireix cap servidor LDAP en especial.

Instal·lant OpenLDAP

Si no disposa de cap servidor LDAP pot usar OpenLDAP. Aquest servidor pot ser descarregat des deOpenLDAP download website [http://www.openldap.org/software/download/]

Un cop descarregat i instal·lat ha de configurar el domini i les credencials. Això es pot fer editant el seu arxiu de configuració (`slapd.conf`) el qual es troba en el directori d'instal·lació d'OpenLDAP.

Editar `suffix` per les dades del domini i `rootdn` y `rootpw` per les dades d'usuari.

Exemple de configuració establint el domini *Open-VA.org* i *admin* com nom d'usuari administrador i *adminpwd* como la seva constrasenya:

```
... altres entrades ...

suffix          "dc=Open-VA,dc=org"
rootdn          "cn=admin,dc=Open-VA,dc=org"
rootpw          adminpwd

... altres entrades ...
```

Important

Recordi usar *noms distingits* per a descriure objectes LDAP.

Requeriment servidor base de dades

No es requireix cap servidor de base de dades en especial.

Instal·lant el servidor MySQL

Si no disposa de cap servidor de base de dades, pot usar MySQL.. Aquest servidor pot ser descarregat des de MySQL download website [http://dev.mysql.com/downloads/mysql/4.1.html].

Per accedir al servidor MySQL des d'una aplicació Java ha de descarregar el conector per a Java. Aquest arxiu pot ser descarregat des de MySQL connector website [http://dev.mysql.com/downloads/connector/j/3.1.html]. Aquest conector ha d'estar en el classpath de l'aplicació com es descriu més avall (*Preparant JBoss*).

Avís

En el momento d'aquest document el connector Java per a MySQL es troba encara en desenvolupament. Degut a això no intenti instal·lar la darrera entrega del servidor MySQL i instal·li la versió 4.

Instal·lant Open-VA

Abans d'instal·lar Open-VA ha de construir i preparar les eines requerides anteriorment.

Preparant eines

Nota

Alguns arxius per a les eines es troben a la carpeta `resources` en el directori d'instal·lació d'Open-VA.

Preparant LDAP

Afegir esquemes *java* i *user* a la instal·lació per defecte.

Per fer-ho ha de copiar `user.schema`, que es troba a `resources`, a la carpeta `schemas` d'OpenLDAP.

Un cop fet registri els esquemes a OpenLDAP editant el seu arxiu de configuració `slapd.conf`

```
... altres entrades ...

include         ./schema/java.schema
include         ./schema/user.schema

... altres entrades  ...
```

LDAP es fa servir per a emmagatzemar certificats acceptats per a que l'aplicació pugui conèixer la ruta de validació i l'estat de revocació.

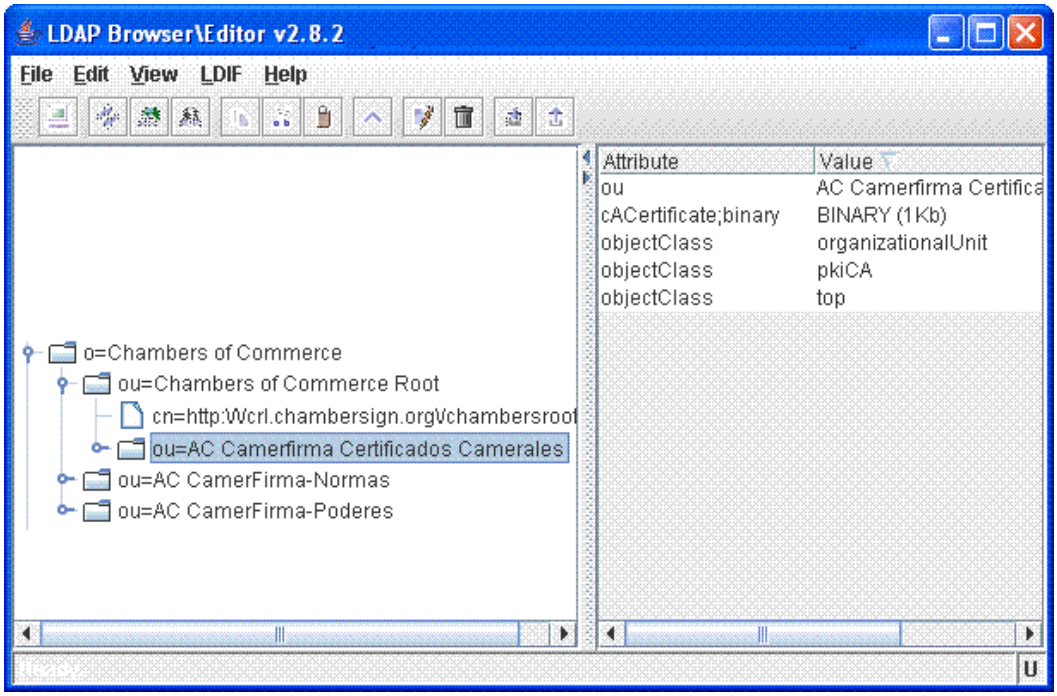
Ha d'emmagatzemar-ho com segueix:

- Crear una *organization (entityClass = o)* només per agrupar certificats.
- Emmagatzemi els seus certificats en *organizational units (entityClass = ou)* del tipus *pkiCA* y amb un atribut binari anomenat *caCertificate* el valor del qual sigui el certificat.

Nota

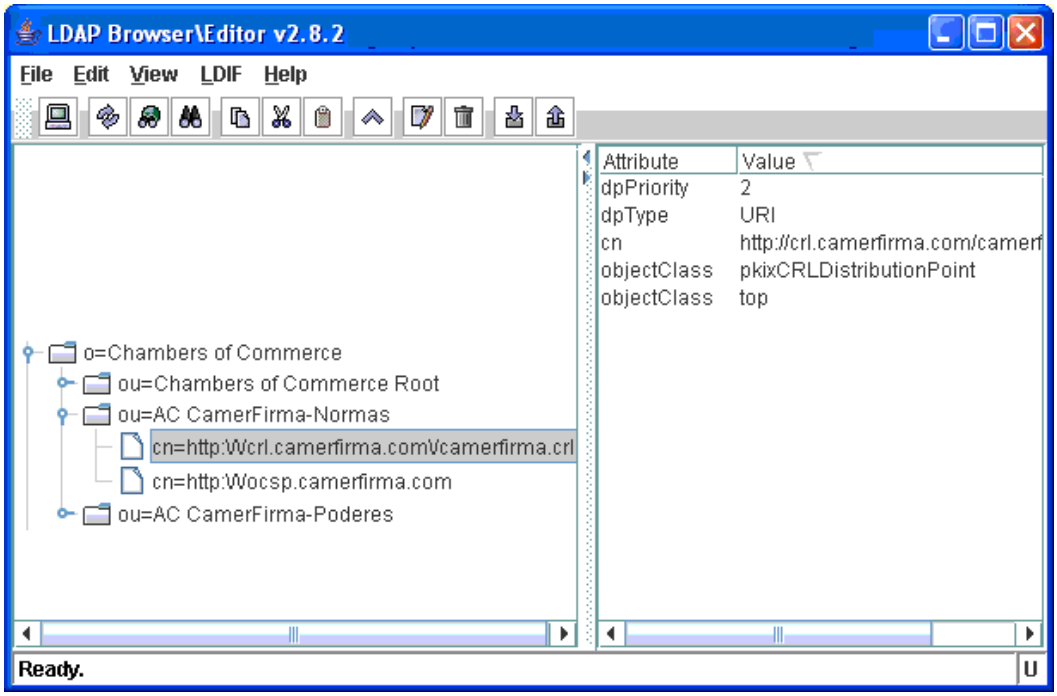
Es recomana, tot i que no és obligatori, respectar la jerarquia de certificats en una manera llegible.

Un exemple d'entrada CA:

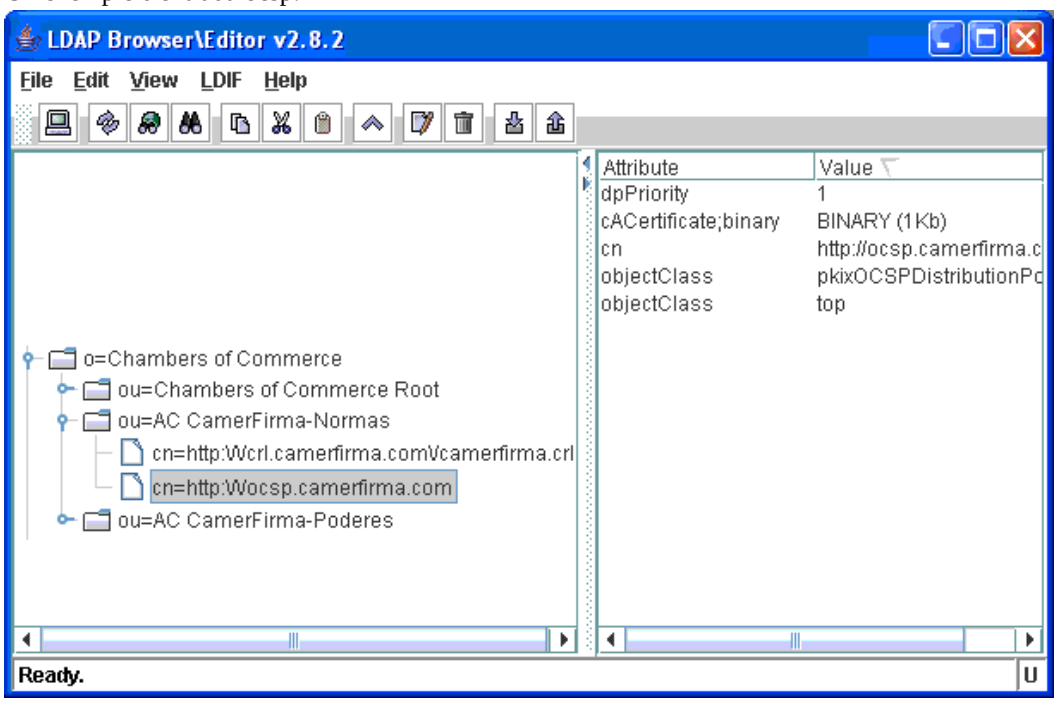


- Cada CA guarda informació de revocació. Aquesta informació inclou mètodes *CRL* i *OCSP* de revocació. Per cada CA diversos mètodes es poden configurar donant a cadascun una prioritat. Per crl només la url complerta és necessària. En el cas d'ocsp a més el certificat ha de ser inclòs per a poder validar la resposta del servidor.

  Un exemple d'entrada crl:



Un exemple d'entrada ocsp:



Preparant el servidor de base de dades

Ha de crear un esquema de base de dades per usar amb Open-VA. A `resources` pot trobar un guió `sql` amb instruccions per crear i omplir les taules.

Hem creat per a vosté dos guions pels més popular servidors de base de dades: MySQL i Oracle.

En aquest guió s'assumeix un esquema amb nom *EPSILON*. Pot canviar-lo però no oblidi actualitzar el guió.

Preparant JBoss

Nota

- Hauria de definir la variable d'entorn `JBOSS_HOME` amb el valor del directori d'instal·lació de JBoss si desitja desplegar Open-VA automàticament.
- Assumim que farem servir el servidor default.
- Copíi els controladors o connectors pel seu servidor de base de dades (no subministrats) a la carpeta `lib`

Atenció

Necessita un arxiu de certificat en format `.pfx` o `.p12`, el qual no s'inclou perquè depend de la seva organització. Aquest arxiu s'ha de copiar a la carpeta `conf` del servidor default de JBoss.

A `resources` té alguns arxius que ha copiar a les carpetes de JBoss. Abans de copiar-los ha d'editar algunes propietats amb els seus propis valors:

- Arxius que s'han de copiar a la carpeta `conf`
  - `KeyStoreConfiguration.properties`

    No editar
  - `ValidationConfiguration.properties`

    No editar
  - `LDAPLoginConfiguration.properties`

Nom de propietat	Descripció de propietat
providerURL	La direcció del seu servidor LDAP
principal	Un nom d'usuari amb drets de consulta en el su servidor LDAP
credentials	La contrasenya

  - `pkiva.webservices.properties`

Nom de propietat	Descripció de propietat
signature.ks	El seu arxiu `.pfx` o `.p12`
signature.ks.password	Contrasenya del seu arxiu de certificats
signature.alias.name	Nom d'usuari del certificat de signatura de respostes
signature.alias.password	Constraenya de l'usuari del certificat de signatura de respostes

- Arxius que s'han de copiar a la carpeta `deploy`

- `open-VA-XXX-db-ds.xml`

  Nota

  Esculleixi XXX entre mysql o oracle, en funció del seu servidor de base de dades. Si te qualsevol altre servidor haurà de crear el seu propi connector.

  Aquest arxiu configura una *font de dades (datasource)* per la base de dades a usar en Open-VA. Ha de respectar l'entrada *JNDI name* (*EPSILON*) i editar la propietat *JDBC* amb el valor correcte pel seu sistema.

- `open-VA-crl_ra-ds.xml`

  No editar

- `open-VA-ldap_ra-ds.xml`

  No editar

- `open-VA-ocsp_ra-ds.xml`

  No editar

Construint Open-VA

Trobarà un guió per a construir Open-VA. El seu nom és `build.cmd` per sistemes Windows i `build.sh` per sistemes UNIX.

Un cop executat aquest guió Open-VA estarà construïda com una *aplicació JEE* amb nom open-VA.ear.

Desplegant Open-VA

Si el servidor JBoss está aturat, arrànquil.

Si ha definit la variable d'entorn `JBOSS_HOME` pot executar **build deploy** i Open-VA serà automàticament desplegada. Si no ha definit aquesta variable d'entorn haurà de copiar manualment l'arxiu `open-VA.ear`. que ha estat creat a la carpeta `dist` de la seva instal·lació Open-VA, a la carpeta `deploy` de JBoss. Si està usando *default* serà: `server/default/deploy`.

Un cop desplegat pot comprovar en el log del servidor (`log/server.log`) que l'arxiu per a l'aplicació Open-VA (`open-VA.ear`) ha estat desplegat i arrencat.

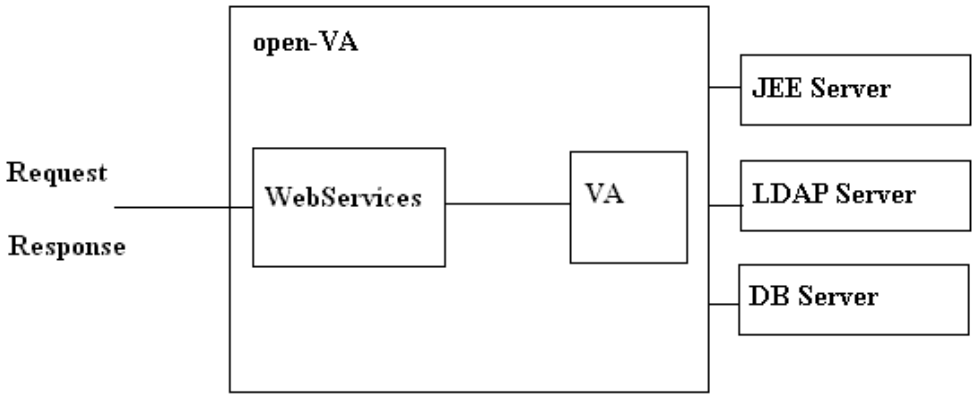
Verificant Open-VA

Després de desplegar i arrencar Open-VA pot verificar que l'aplicació està funcionant invocant la serva plana principal tal i com es mostra a la figura:


open-VA - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://localhost:8080/open-VA/
Go
Getting Started
Latest Headlines
Welcome to open-VA
Powered by open-VA.org
Done

Capítol 3. Usant Open-VA

Open-VA és un codi obert que demostra com validar certificats digitals i documents signats.



Com pot veure en el diagrama anterior Open-VA té un *WebService* com a frontal. Aquest accepta peticions, les processa i retorna una resposta.

Començant

Ha de construir un client *webservice* per poder operar contra Open-VA. Per a fer-ho necessita el descriptor de servei (*WSDL*). No té perquè escriure'l manualment. Pot ser obtingut invocant **Open-VA/ValidateWS?wsdl** en el servidor.

En aquesta entrega d'Open-VA només un métode està disponible: **validate**.

Aquesta operació accepta un *document XML* amb la petició i retorna un altre `xml` amb la resposta.

Nota

Open-VA retorna la resposta signada. Primer calcula la signatura per a la resposta i després afegeix a la resposta un nou camp amb nom `signature`.

Els `dtd` per aquests `xml` son:

- petició

```
<!DOCTYPE request [<!ELEMENT request (elementId,elementContent,?)>
<!ELEMENT elementId (#PCDATA)>
<!ELEMENT elementContent (certificate|signedDoc|(signature,doc))>
<!ELEMENT certificate (#PCDATA)>
<!ELEMENT signedDoc (#PCDATA)>
<!ELEMENT signature (#PCDATA)>
<!ELEMENT doc (#PCDATA)>]>
```

- resposta

```
<!DOCTYPE response [
<!ELEMENT response (value, codeError?, status, statusReason?, signature)>
<!ELEMENT value (#PCDATA)>
<!ELEMENT codeError (#PCDATA)>
<!ELEMENT status (#PCDATA)>
<!ELEMENT statusReason (#PCDATA) ?>
<!ELEMENT signature (#PCDATA)>]>
```

Protocol d'operacions Open-VA

Ha de crear un `xml` en la petició i analitzar la resposta un cop invocada l'operació **validate**, segons el `dtd` a la secció anterior.

Nota

Les dades binàries com certificats, signatures o documents es passen en format *base 64*.

Es dona suport a tres tipus de peticions:

- Validació de certificats

  Ha d'informar el camp **certficate**

- Documents signats amb signatura no adjunta

  Ha d'informar els camps **signature** i **doc**

- Documents signats amb signatura adjunta

  Ha d'informar el camp **signedDoc**

La resposta pot ser una mica confusa perquè hi ha dos codis de resposta.

- `value`

  Indica que el document està ben format i pot ser processat.

  Els seus valors poden ser: *Refused*, *Failure* o *Success*

  Ha de parar atenció perquè *Success* no significa que la validació és correcta. Només significa que la petició ha estat acceptada per a ser processada.

  En el caso de *Refused* o *Failure* el camp *codeError* dóna més informació.

- `status`

  Els seus valors poden ser: *Valid* o *Invalid*

  Un valor de *Valid* indica que la validació ha estat correcte.

  En el caso d'una validació incorrecte el camp *statusReason* dóna més informació.