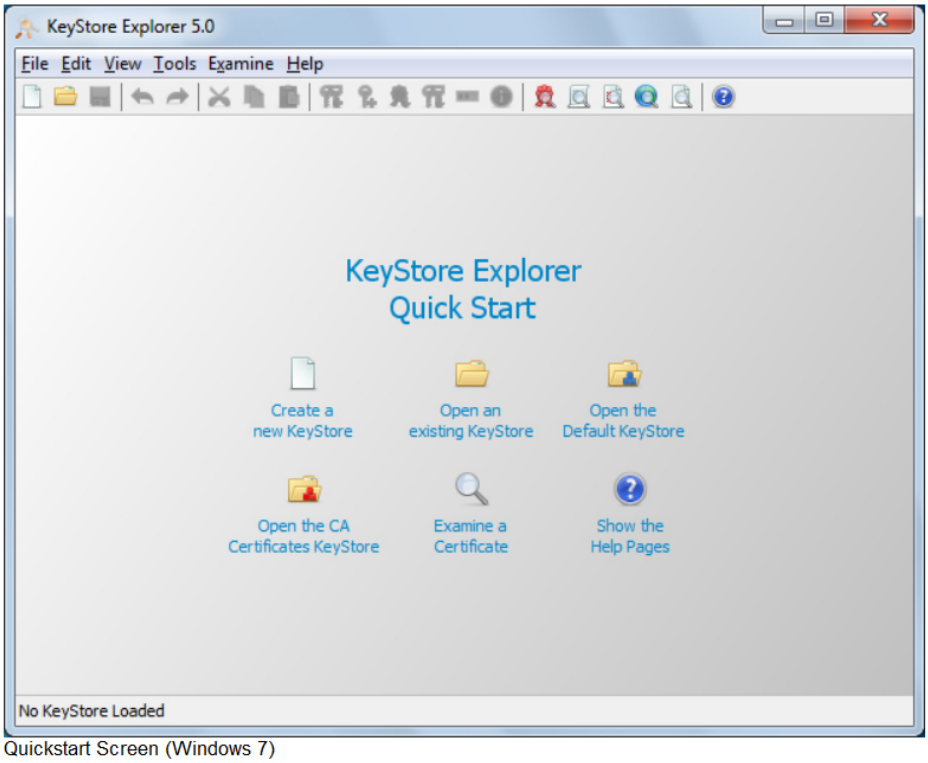
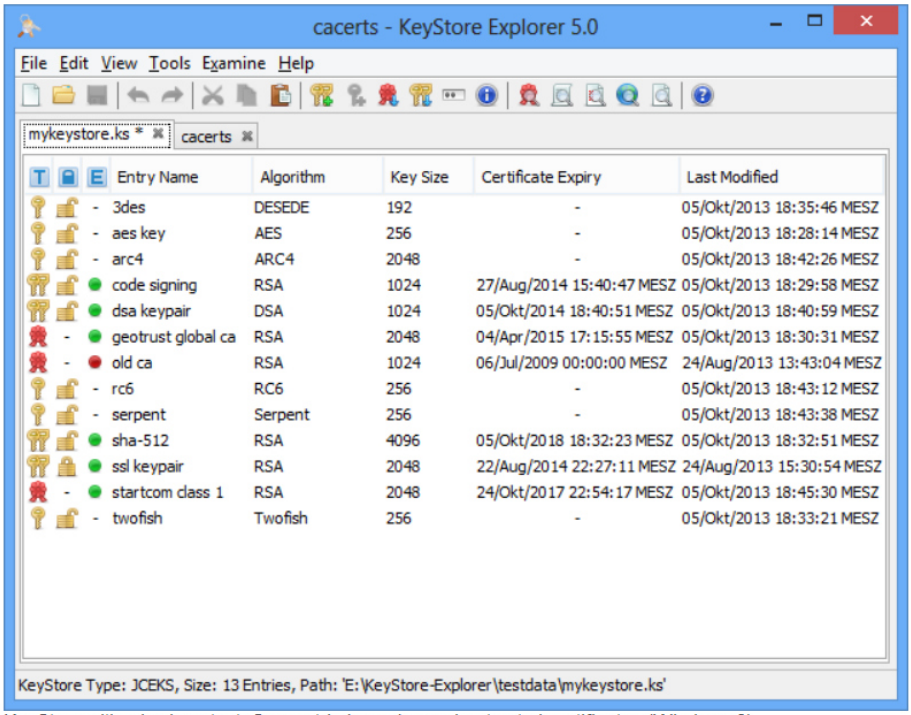
# WEBUI CONFIGURAZIONE IDP

Verrà utilizzato il seguente tool grafico: http://keystore-explorer.sourceforge.net/

Ecco alcuni screenshot:



Quickstart Screen (Windows 7)



KeyStore with mixed content: Symmetric keys, key pairs, trusted certificates (Windows 8)

## Generazione chiavi e certificato

Il primo passo necessario è quello della creazione di una coppia chiave privata-pubblica e di un certificato (anche self signed). Il certificato e le chiavi devono quindi essere importate nel keystore della web-ui.

Il keystore deve essere generato con il tool grafico Keystore Explorer (va selezionato il tipo JKS), nominato saml-keystore.jks e inserito nella cartella dei sorgenti della web-ui main/resources/saml/.

La password scelta alla creazione del keystore va inserita nel file main/resources/application.proprierties alla voce environment.keystore.pwd.

Vanno quindi generate le chiavi e il certificato; è possibile procedere in due modi:

1. Aprire il file main/resources/saml/saml-keystore.jks
   Andare sotto Tools →Generate keypair
   - Lasciare RSA 2048,
   - Per conformità usare CN ed alias uguali
   - Validity del certificato, mettere almeno un anno
   - CN Importante da ricordare mettere ad es. saml-xxxx
   - Ricordarsi la pwd immessa!
   - Salvare

Oppure

2. Stessa configurazione può essere effettuata con i comandi classici di openssl:
   a. Generare coppia di chiavi RSA e certificato con
      `openssl genrsa -des3 -out private.pem 2048`
      oppure
      `openssl genrsa -des3 -out private.key 2048`
   b. Generare certificato autofirmato per RSA key [1]

      `openssl req -key private.key -new -x509 -days 365 -out cert.pem`
      Questo commando crea un certificate da una chiave private precedentemente generata.

Occorre rispondere alla richiesta di informazioni CSR per completare il comando.
L'opzione `-x509` significa che si sta richiedendo un certificate di tipo x509. L'opzione `-days 365` specifica la durata della validità del certificate (in questo caso 365 giorni).
L'opzione `-new` abilita la richiesta di informazioni CSR.
Alternativamente è possibile creare il certificato con il singolo comando

```
openssl req -x509 -newkey rsa:2048 -keyout private.pem -out cert.pem -days 365
```

E' possibile disabilitare la protezione della chiave private tramite password aggiungendo il parametro `-nodes`.

c. Generare file .p12 con il comando

```
openssl pkcs12 -export -in cert.pem -inkey private.pem -out cert.p12
```

d. Importare il file .p12 nel keystore saml-keystore.jks.

Sia nel caso che le chiavi e il certificato vengano generati da Keystore Explorer o da linea di comando è importante che:

1. L'alias e il CN coincidano per uniformità
2. La password di protezione della private key venga inserita nel file application.properties

Va infine modificato il file application.properties nei sorgenti della web-ui PRISMA con i seguenti valori:

- environment.sp.entity.id = Inserire un SP_ENTITY_ID univoco (es. urn o domain name)
- environment.samlkey = l'alias del certificato inserito in saml-keystore.jks
- environment.domain = il domain name della web-ui
- environment.samlkey.pwd = la password della chiave privata importata
- environment.keystore.pwd = la password del keystore saml-keystore.jks

NOTA:

Nel caso la web-ui venga collegata a un IDP in cui si utilizzi ADFS come Identity Provider, il caricamento deve avvenire usando come tipologia di crittografia SHA-1 (di default ADFS usa RSA-SHA256, cosa che causa errore in fase di decodifica delle asserzioni SAML lato SP). Nello specifico vanno lasciate tutte le configurazioni di ADFS di default, tranne quella riportata in Figura 1.

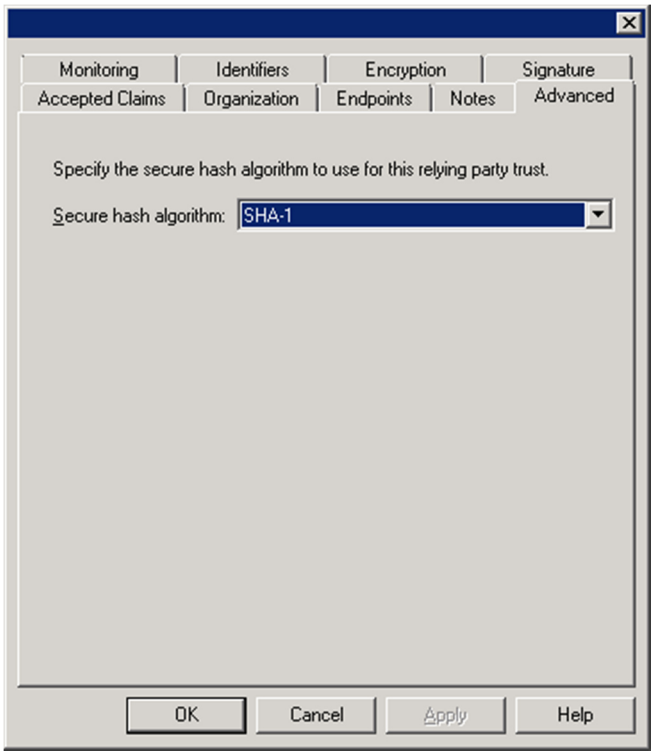



*Figura 1 Parametro da cambiare in ADFS*

# Aggiunta IDP esterno

A questo punto l'aggiunta di un IDP comporta uno scambio di credenziali tra il gestore del portale e quello dell'IDP.

## WEB-UI -> IDP

E' necessario comunicare al gestore dell'IDP

1. Il proprio entity id, come riportato nel file application.properties
2. Il domain name del portale
3. L'indirizzo da cui il gestore dell'idp potrà scaricare i metadata del portale; di default il path è /saml/metadata. E' necessario che l'endpoint sia raggiungibile tramite connessione HTTPS. L'endpoint complessivamente sarà quindi del tipo https://DOMAIN_NAME:(eventuale porta)/saml/metadata

## IDP -> WEB-UI

E' necessario:

1. Farsi comunicare a propria volta l'entity id, domain name e path dei metadata
2. Inserire l'entity id e gli altri dati di info dell'organizzazione a cui l'IDP fa riferimento all'interno del DB del Data Access Layer
3. Scaricare l'XML di metadata dal link comunicato e inserirlo nella cartella /root/saml/metadata/{label-idp}/ dell'host su cui è installato l'application server della web-ui
4. Aggiungere nel file application.yml nei sorgenti della webui l'entry relativa al nuovo IDP; nello specifico i campi più importanti sono:
    a. id : l'id della nuova riga nel db relative all'IDP
    b. label : label dell'IDP, deve essere uguale (case insensitive) alla folder in cui è stato inserito l'XML
    c. entityId : entity ID dell'IDP
    d. metadataPath : path dei metadata nel file system (nome file e estensione compreso)

e. mapping : specifica come mappare la risposta SAML ricevuta dall'IDP con i dati di autenticazione richiesti
f. name : l'username dell'utente autenticato da SAML (es. urn:oid:0.9.2342.19200300.100.1.1); se lasciato vuoto verrà usato il parametro di autenticazione NameID
g. email : l'email dell'utente autenticato da SAML (es. urn:oid:0.9.2342.19200300.100.1.3 o http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress)

# Bibliografia

[1] digitalocean. [Online]. Available: https://www.digitalocean.com/community/tutorials/openssl-essentials-working-with-ssl-certificates-private-keys-and-csrs.