GUIDA per la richiesta, il download e l’utilizzo del certificato di autenticazione

Sommario

1 Introduzione

La verifica e la convalida dei buoni di acquisto da parte degli esercenti online avverrà tramite l'utilizzo di un web service legato ad un **certificato di autenticazione** da installare nel proprio client del servizio e da utilizzare nella chiamata SOAP per effettuare l'autenticazione in modalità SSL con certificato client.

Tale certificato X509 sarà generabile e scaricabile in formato .cer direttamente tramite l'applicazione web dedicata agli esercenti, in area autenticata.

In particolare il processo di generazione del certificato prevede due step:

1. richiesta del certificato

   a seguito di questa operazione il sistema prende in carico la richiesta

2. verifica esito della richiesta questa operazione controlla se è pronto il certificato emesso da CA dedicata ed eventualmente lo rende disponibile per il download.

Durante il primo step sarà necessario caricare un file **.der** che contiene la richiesta di certificato alla CA dedicata al progetto. Tale .csr deve presentare le seguenti caratteristiche:

- algoritmo generazione chiavi: RSA
- lunghezza chiavi: 2048 bit

Il certificato emesso dalla CA va scaricato in locale e installato, insieme alla corrispondente chiave privata, nel client utilizzato per il servizio di verifica voucher.
Pertanto l'evento di download del certificato non rappresenta la definitiva attivazione dell'esercente.

E' stato previsto uno step di **attivazione**, di tipo "Check" che deve avere i seguenti valori di input:

- tipo operazione = 1
- codice voucher = 11aa22bb

La chiamata al servizio con questa operazione equivale ad una transazione di attivazione, il cui unico effetto è quello di portare l'esercente nello stato attivo, dunque visibile nella sezione "Dove Usare i buoni".

2 Come generare il certificato

Per ottenere tale certificato è necessario installare un software per la gestione dei certificati. In questa guida sono descritti due strumenti utili per la gestione dei certificati:

- **OpenSSL**: una libreria opensource che permette di generare chiavi e certificati attraverso delle istruziuoni eseguibili dal prompt dei comandi
- **XCA**: un software opensource che fornisce un'interfaccia grafica per la generazione di chiavi e certificati digitali attraverso l'utilizzo di OpenSSL.

3 Generare un certificato usando OpenSSL

Di seguito i passi per generare un certificato di autenticazione attraverso l'uso di OpenSSL.

3.1 Installazione

1. Scaricare il software al link https://slproweb.com/download/Win64OpenSSL-3_1_4.exe
2. Installando il software mantenendo le impostazioni di default, il pacchetto dovrebbe essere nella directory C:\OpenSSL-Win64
3. Inserire il puntamento alla directory di openssl.exe fra le variabili di ambiente, aggiungendo la directory C:\OpenSSL-Win64\bin fra quelle definite nella variabile "Path"
4. Il software sarà così pronto all'uso

3.2 Creare i file key.der e req.der

1. Aprire il prompt dei comandi e posizionarsi sulla directory C:\ con il comando:

   cd c:

2. Scrivere il seguente comando e premere invio **openssl req -newkey rsa:2048 -keyout key.der -out req.der -outform DER**

3. Se il comando precedente verrà accettato, vi verrà richiesto di scegliere una password da utilizzare per la creazione del certificato e successivamente di confermarla:

   Enter PEM pass phrase:
   Verifying - Enter PEM pass phrase:

   La password che digiterete non verrà visualizzata per questioni di sicurezza

4. Inserire i dati richiesti:
   - Country Name (2 letter code) [AU]: **IT**
   - State or Province Name (full name) [Some-State]: **Italy** (campo facoltativo)
   - Locality Name (eg, city) [ ]: **Rome** (campo facoltativo)
   - Organization Name (eg, company) [Internet Widgits Pty Ltd]: **Ministero della cultura**
   - Organizational Unit Name (eg, section) [ ]: **Servizi Web**
   - Common Name (e.g. server FQDN or YOUR name) [ ]:"inserire in questo campo il codice fiscale dell'azienda per cui si richiede il certificato"
   - Emai Address [ ]: "inserire in questo campo la propria mail" (campo facoltativo)
   - A challange password [ ]: "Inserire una password per il certificato"
   - An optional company name [ ]: **Ministero della cultura**

5. Inseriti i dati corretti verranno creati i file **key.der** e **req.der** nella directory C:\

3.3 Eseguire l'upload del file req.der, richiedere e scaricare il certificato

Per effettuare l'upload del file **req.der** creato in precedenza, cliccare su "Richiedi Certificato"

Fig. 1 - Richiesta certificato

Cliccare su “Scegli file”

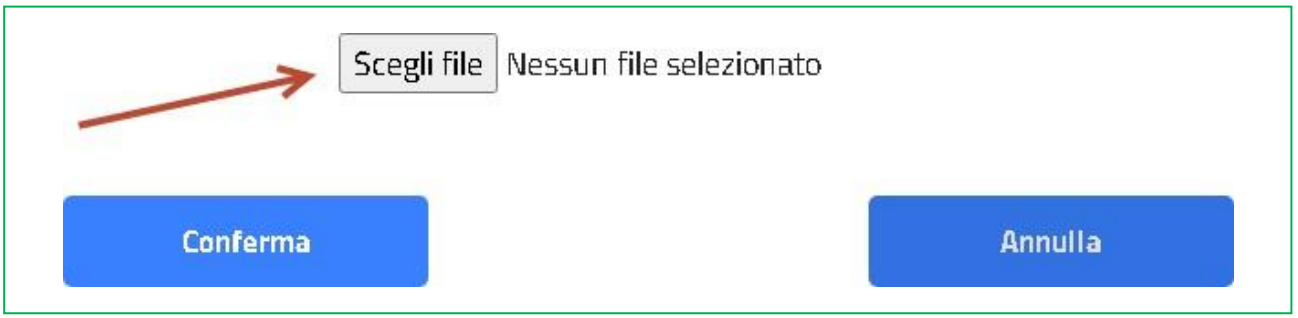

Fig. 2 – Upload del file .der

1. Andare sulla directory “C:/”
2. Selezionare il file req.der e cliccare su “Apri”
3. Una volta effettuato l’upload procedere con la richiesta del certificato cliccando su “Conferma”

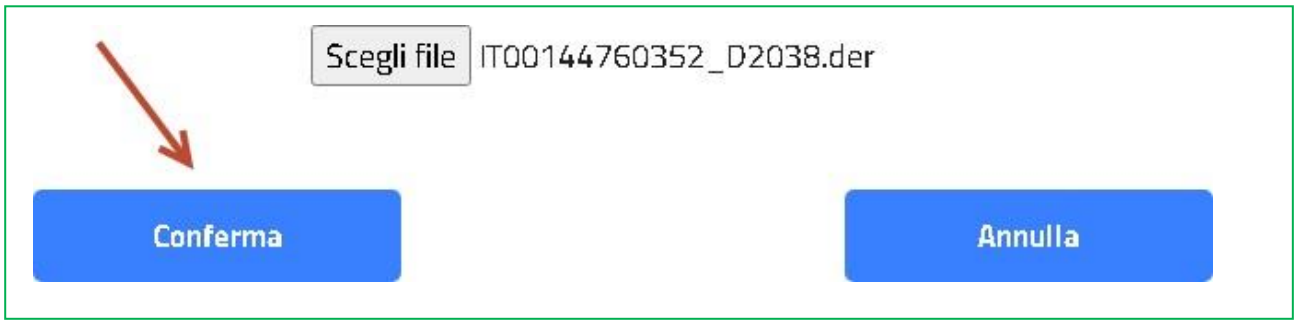

Fig. 3 – Conferma upload

Quando il certificato sarà stato prodotto si deve procedere adesso con lo scarico del certificato cliccando su “Download Certificato” e salvare il file scaricato nella directory “C:\”

3.4 Convertire un certificato.cer in formato .pem

1. Aprire il prompt dei comandi e posizionarsi sulla directory C:\ con il comando:

   cd c:
2. Scrivere il seguente comando sostituendo le ‘xxxxx’ con il nome del file .cer e le ‘yyyyy’ con il nome che si vuole dare al file .pem e premere invio

openssl x509 –inform der –in xxxxx.cer –out yyyyy.pem

3. Se il comando verrà accettato verrà creato il file **yyyyy.pem** nella directory C:\

3.5 Convertire un certificato .pem in formato .p12

1. Aprire il prompt dei comandi e posizionarsi sulla directory C:\ con il comando:

   cd c:

2. Scrivere il seguente comando sostituendo le 'xxxxx' con il nome del file .pem che si è scelto nel passo precedente e le 'yyyyy' con il nome che si vuole dare al file .p12 e premere invio

   openssl pkcs12 -export -inkey key.der -in xxxxx.pem -out yyyyy.p12

3. Verrà richiesta la password scelta in fase di creazione del file key.der inserita nel campo "Enter PEM pass phrase:"

4. Se il comando verrà accettato verrà creato il file **yyyyy.p12** nella directory C:\

4 Generare un certificato usando XCA

Di seguito la procedura per generare un certificato di autenticazione tramite XCA.

4.1 Installazione

1. Scaricare il software opensource al link https://sourceforge.net/projects/xca/ 2. Una volta installato all'apertura avrete la seguente schermata:

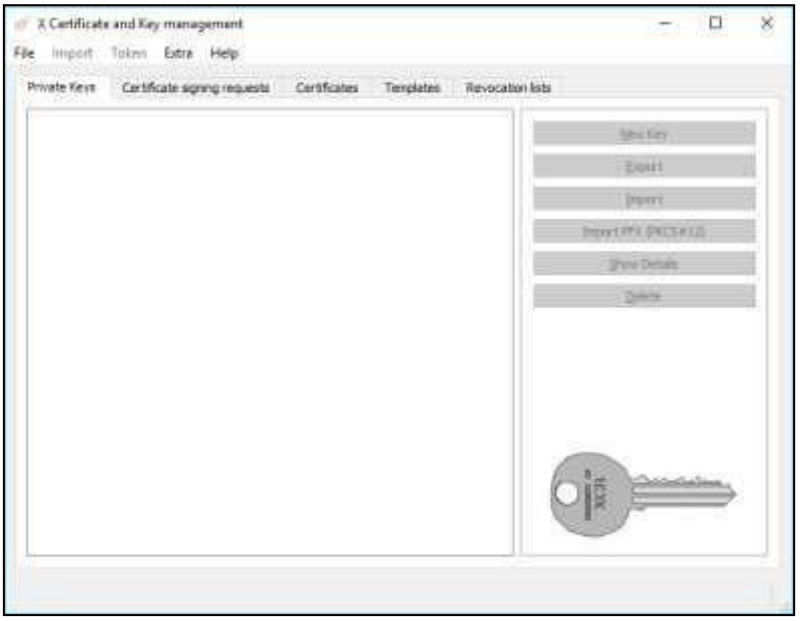

Fig. 4

Andare sul menu "**File**" e selezionare la voce "**New DataBase**"

Così facendo si creerà un file che conterrà tutti i file generati nel vostro spazio di lavoro:

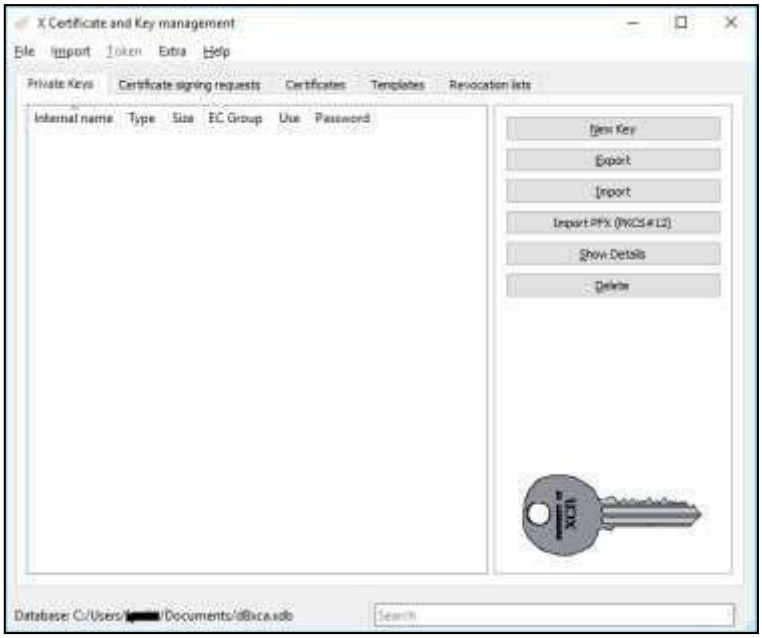

Fig. 5

Una volta indicati il nome del file e la cartella in cui salvarlo verrà chiesto di scegliere una password per proteggere lo spazio di lavoro.

4.2 Creare un file key.der

1. Nella tab “Private Keys” cliccare sul pulsante “New Key” posto a destra.
2. Impostare i seguenti parametri (vedi *Figura 6*):
    - **Name** = key
    - **Keytype** = selezionare ‘RSA’
    - **Keysize** = selezionare ‘2048 bit’

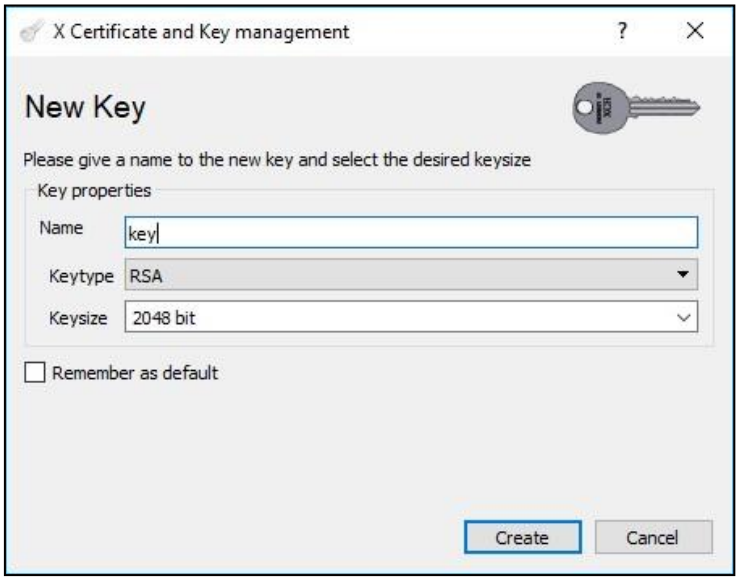

Fig. 6 - Nuova Chiave

3. Si otterrà così una chiave i cui attributi verranno indicati nella tab “Private Keys”

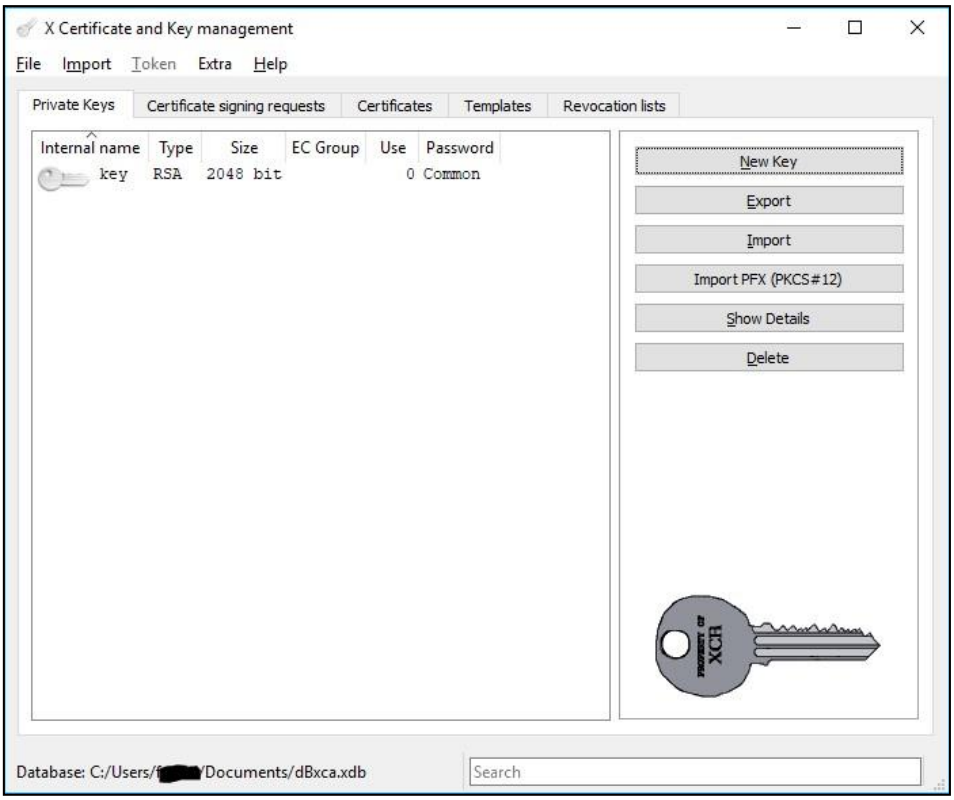

Figura 7 - Chiave generata correttamente

4. Se si vuole esportare il file in formato .der, selezionare la chiave appena creata e cliccare sul pulsante “Export” inserendo i seguenti parametri (vedi *Figura 8*):
    - **Name** = key
    - **Filename** = C:/key.der
    - **Export Format**: selezionare “DER private (*.der)”

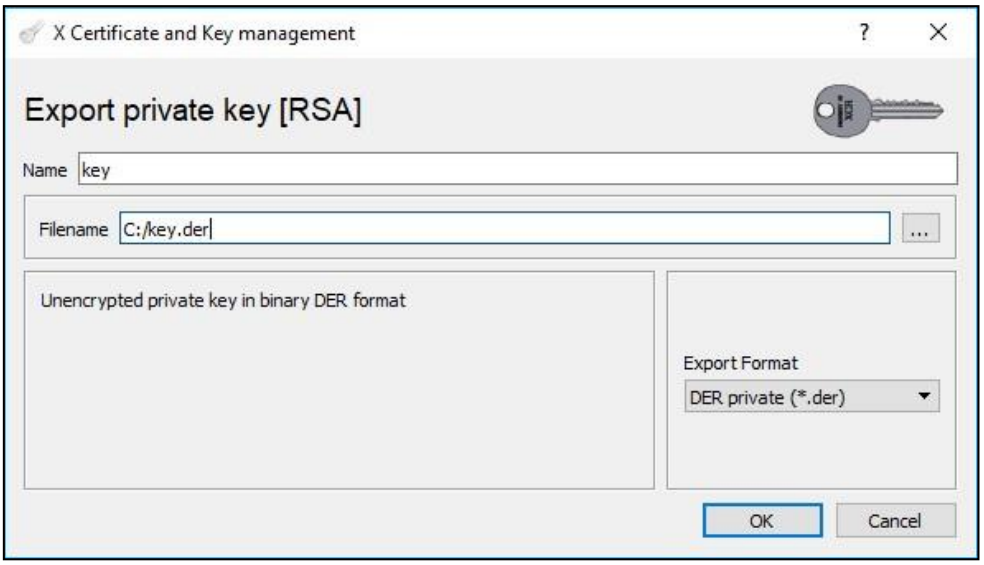

Figura 8 - Salvare il file in formato .der

5. Cliccando su ok verrà creato un file key.der nella directory indicata.

4.3 Creare un file req.der

1. Nella tab “Certificate signing requests” cliccare sul pulsante “New Request” sulla destra verrà aperta una nuova finestra:

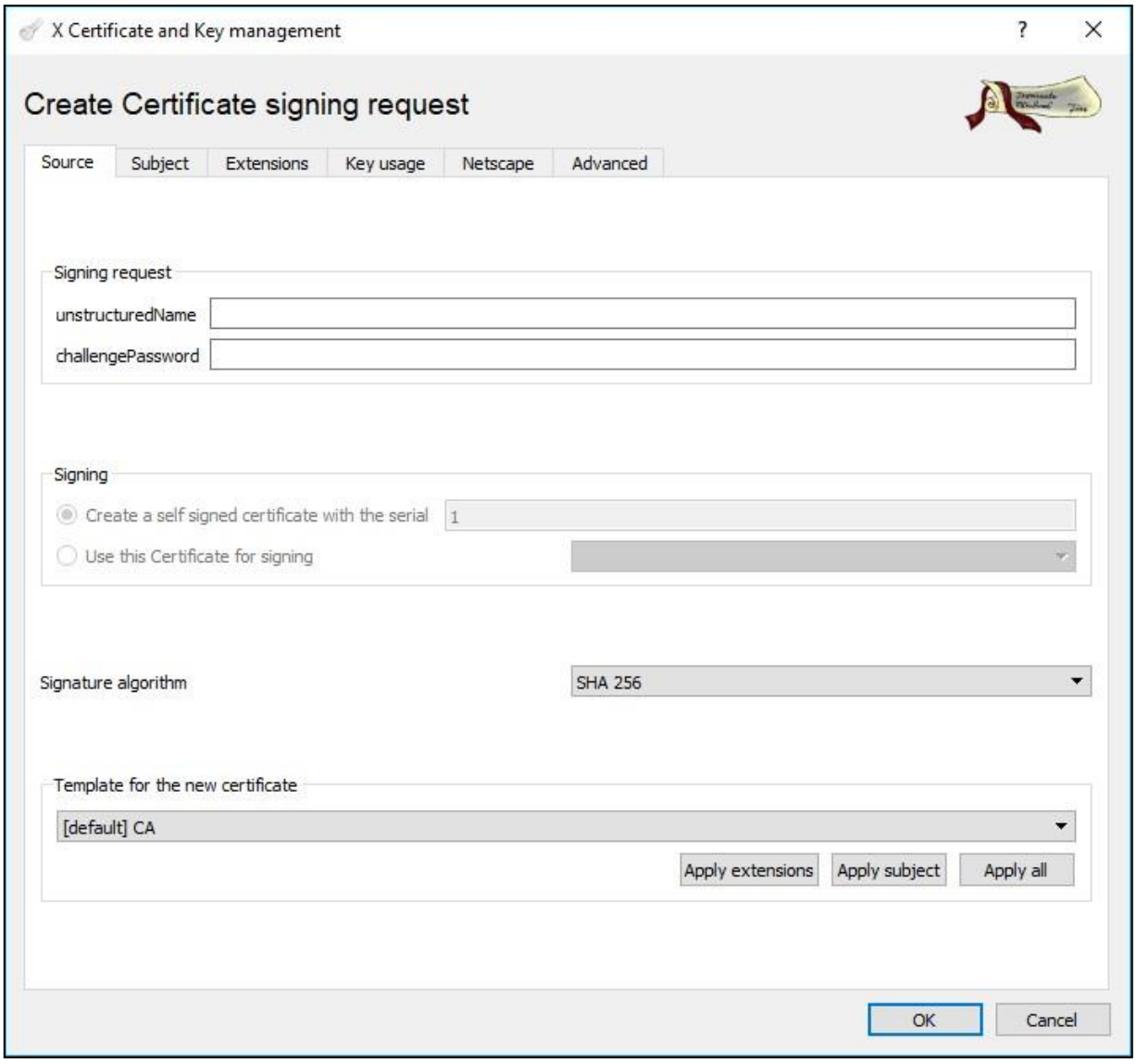

Figura 9 - Nuovo CSR

2. Nella tab “Source” compilare i seguenti campi:
   - **unstructuredName**: *codice fiscale di chi genera la CSR*
   - **challangePassword**: *inserire una password a scelta*
   - **Signature algorithm**: selezionare ‘SHA 256’
   - **Template for the new certificate**: selezionare ‘[default] CA’

3. Nella tab “Subject” compilare i seguenti campi:
    - **Internal name** = req
    - **CountryName** = IT
    - **StateOrProvinceName** = Italy *(campo facoltativo)*
    - **localityName** = Rome *(campo facoltativo)*
    - **organizationName** = Ministero della cultura
    - **organizationalUnitName** = Servizi Web
    - **commonName** = *inserire in questo campo il codice fiscale dell’azienda per cui si richiede il certificato*
    - **emaiAddress** = *inserire in questo campo la propria mail (campo facoltativo)*

4. Nel campo “Private key” in basso, selezionare la chiave nominata “key” creata precedentemente;

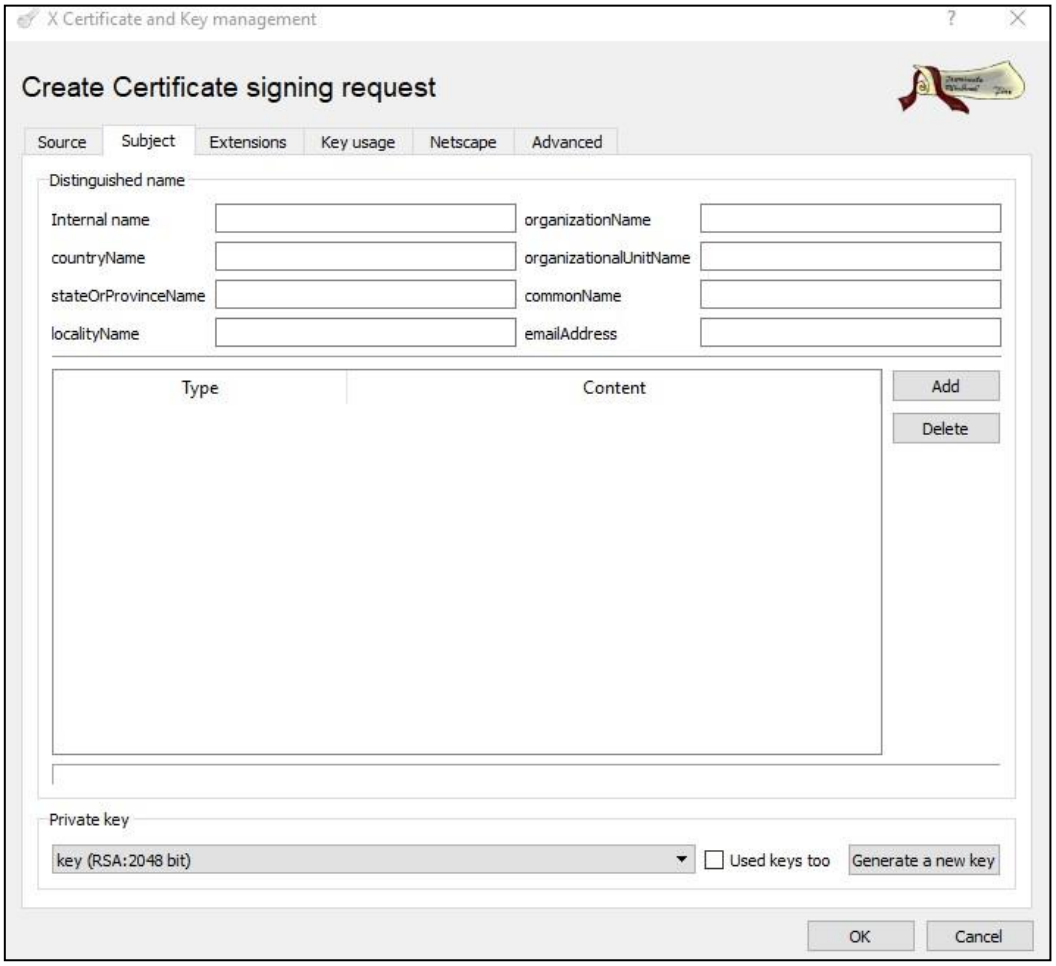

Figura 1 - Creare un file req.der

5. Cliccando ok verrà creata una Certificate Signing Request (CSR) nello spazio di lavoro; 6. Una volta creata la CSR, selezionarla e cliccare “Export”;

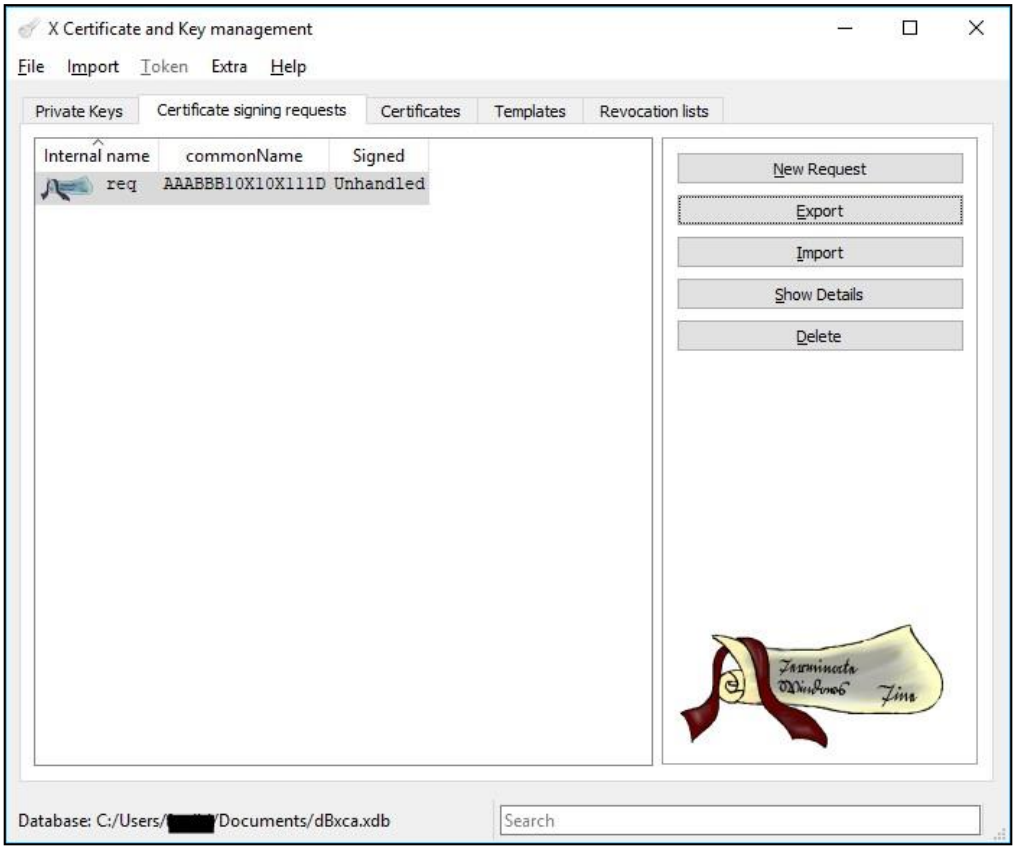

Figura 2 - CSR creato

7. Apparirà la finestra “Certificate request export” e bisognerà compilare i seguenti campi:
    - **Name** = req
    - **Filename** = C:/req.der
    - **Export Format** = DER (*.der)

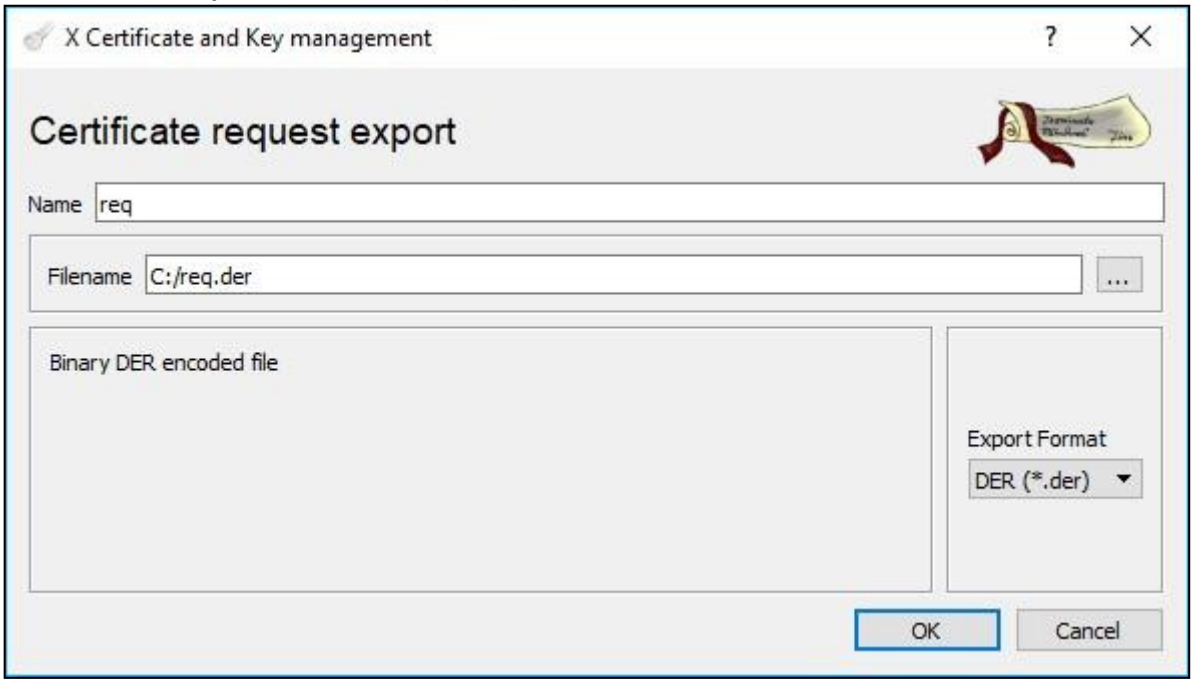

Figura 3 - Export di una CSR

8. Infine cliccare su ok per creare il file '*req.der*' nella directory indicata.

4.4 Eseguire l'upload del file req.der, richiedere e scaricare il certificato

Fig. 73 - Richiesta certificato

Cliccare su "Scegli file"

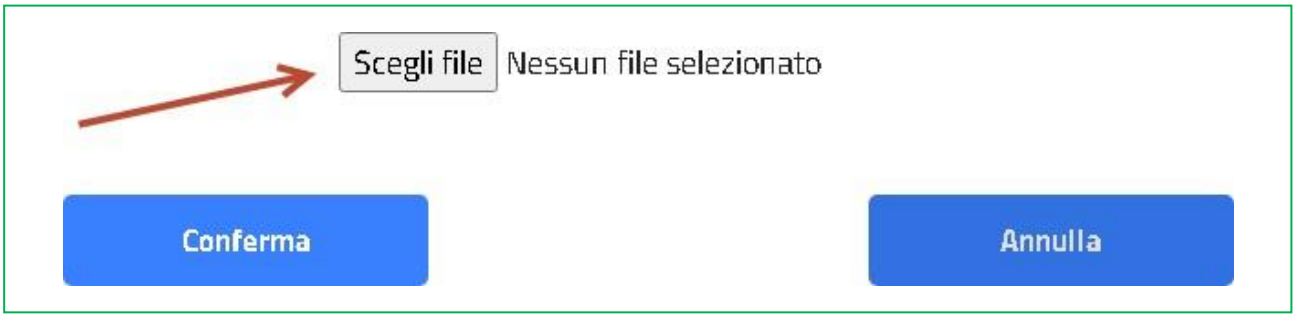

Fig. 14– Upload del file .der

Andare sulla directory "C:/" e selezionare il file req.der e cliccare su "Apri".

Una volta effettuato l'upload procedere con la richiesta del certificato cliccando su "Conferma"

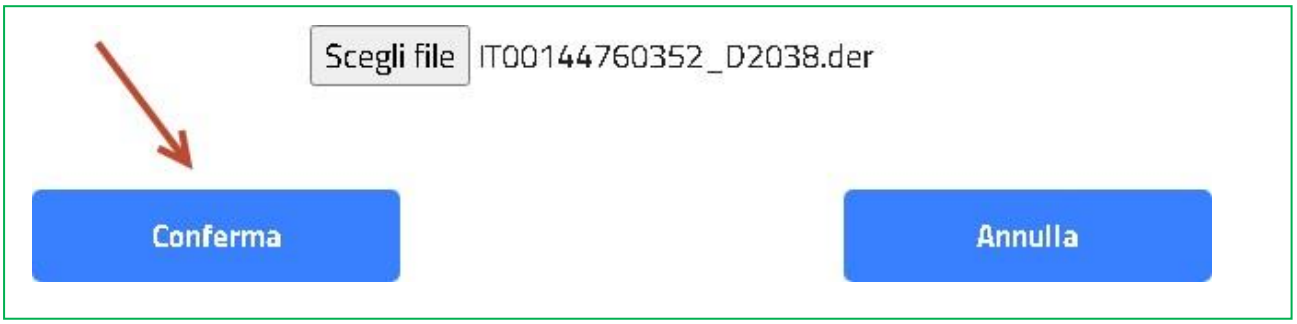

Fig. 15 – Conferma upload

Quando il certificato sarà stato prodotto, si dovrà procedere con lo scarico del certificato.

Cliccare su "Download Certificato" e salvare il file scaricato nella directory "C:\"

4.5 Convertire un certificato.cer in formato .pem o .p12

1. Nella tab “Certificates” cliccare sul pulsante “Import” e selezionare un “*certificato.cer*”
2. Una volta importato nello spazio di lavoro selezionarlo e cliccare “Export”
3. Apparirà una finestra in cui bisognerà impostare i campi come in *Figura 15* selezionando dal campo “Export Format”:
   - PEM all (*.pem)
   - PKCS #12 (*.p12)

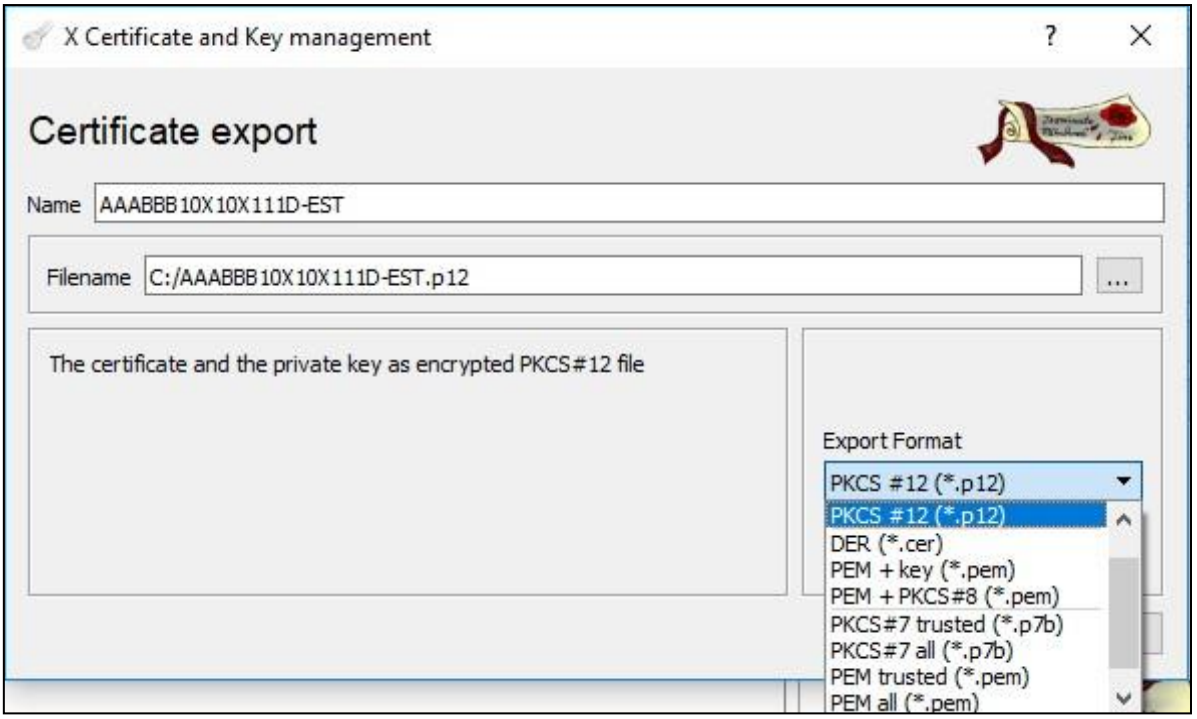

Figura 16 - Export di un certificato