



AGENZIA
DOGANE
MONOPOLI



sogei

MANUALE GESTIONE CERTIFICATI

Guida al Download del Certificato di Autenticazione

Versione del 05 marzo 2020

Sommario

1	Introduzione	3
2	Generare un certificato usando OpenSSL	3
2.1	Installazione	3
2.2	Creare i file key.der e req.der	3
2.3	Eseguire l'upload del file req.der, richiedere e scaricare il certificato	4
2.4	Convertire un certificato.cer in formato .pem.....	6
2.5	Convertire un certificato.pem in formato .p12.....	6
3	Generare un certificato usando XCA.....	7
3.1	Installazione	7
3.2	Creare un file key.der.....	8
3.3	Creare un file req.der.....	10
3.4	Eseguire l'upload del file req.der, richiedere e scaricare il certificato	14
3.5	Convertire un certificato.cer in formato .pem o .p12.....	16

1 Introduzione

L'applicazione Gestione Certificati, disponibile sul portale dei servizi dell'Agenzia delle Dogane e Monopoli nella sezione "Interattivi", permette di scaricare il Certificato di Autenticazione per l'utilizzo dei Web Service. Sono disponibili due tipologie di certificato di autenticazione, una per l'ambiente di addestramento e una per l'ambiente reale. Per utilizzare tale applicazione 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 open source che permette di generare chiavi e certificati attraverso delle istruzioni eseguibili dal prompt dei comandi
- **XCA**: è un software open source che fornisce un'interfaccia grafica per la generazione di chiavi e certificati digitali attraverso l'utilizzo di OpenSSL.

2 Generare un certificato usando OpenSSL

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

2.1 Installazione

1. Scaricare il software al link https://slproweb.com/download/Win64OpenSSL-1_0_2u.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

2.2 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]:** Agenzia delle Dogane
 - **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 challenge password []:** *“Inserire una password per il certificato”*
 - **An optional company name []:** Agenzia delle Dogane
5. Inseriti i dati corretti verranno creati i file **key.der** e **req.der** nella directory C:\

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

1. Per effettuare l'upload del file req.der creato in precedenza, cliccare su “Sfoglia”

Figura 1 - Riquadro dei file di cui fare l'upload

2. Andare sulla directory “C:”
3. Selezionare il file req.der e cliccare su “Apri”
4. Si vedrà apparire il file nella lista dei file selezionati

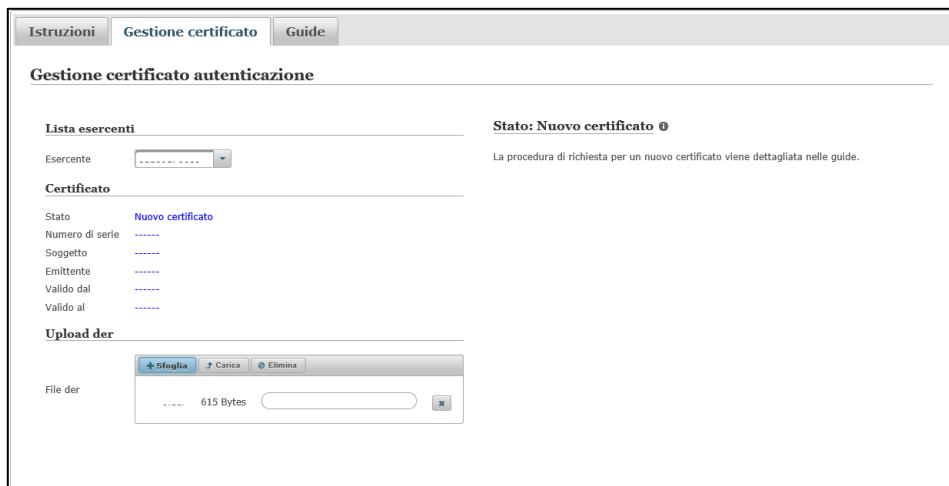


Figura 2 - File req.der selezionato

5. Cliccare su "Carica" per eseguire l'upload del file, la barra bianca si colorerà visualizzando l'avanzamento del caricamento
6. terminato l'upload si avrà la seguente schermata:

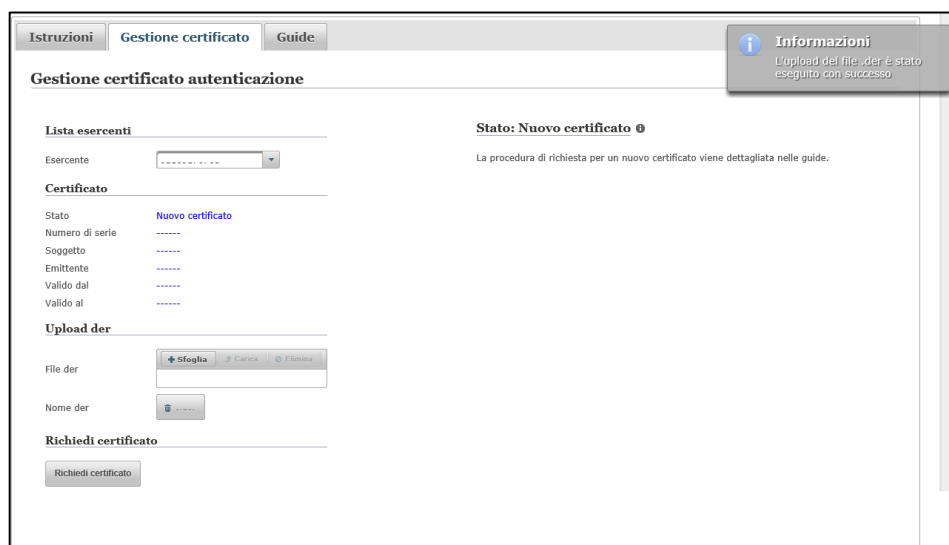


Figura 3 - Upload avvenuto con successo

7. L'Upload del file req.der è avvenuto con successo
8. Procedere con la richiesta del certificato cliccando su "Richiedi Certificato"



Figura 4 - Certificato richiesto

Procedere adesso con lo scarico del certificato cliccando su "Download Certificato" e salvare il file scaricato nella directory "C:\"

2.4 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:\

2.5 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:\

3 Generare un certificato usando XCA

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

3.1 Installazione

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

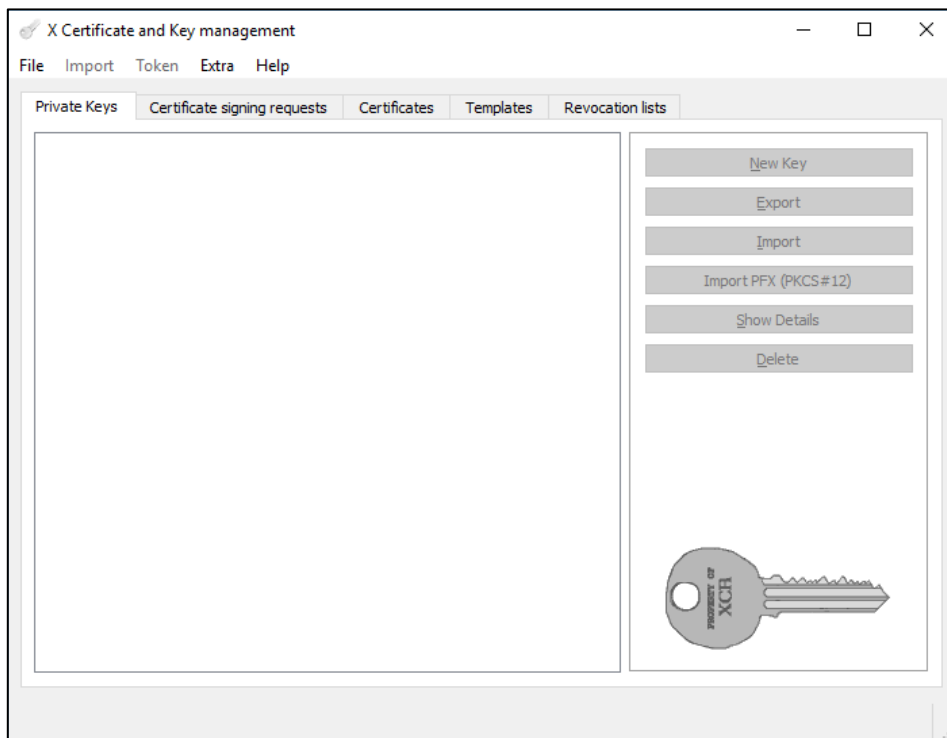


Figura 5 - Schermata iniziale

3. Andare sul menu "File" e selezionare la voce "New DataBase"
4. Così facendo si creerà un file che conterrà tutti i file generati nel vostro spazio di lavoro:

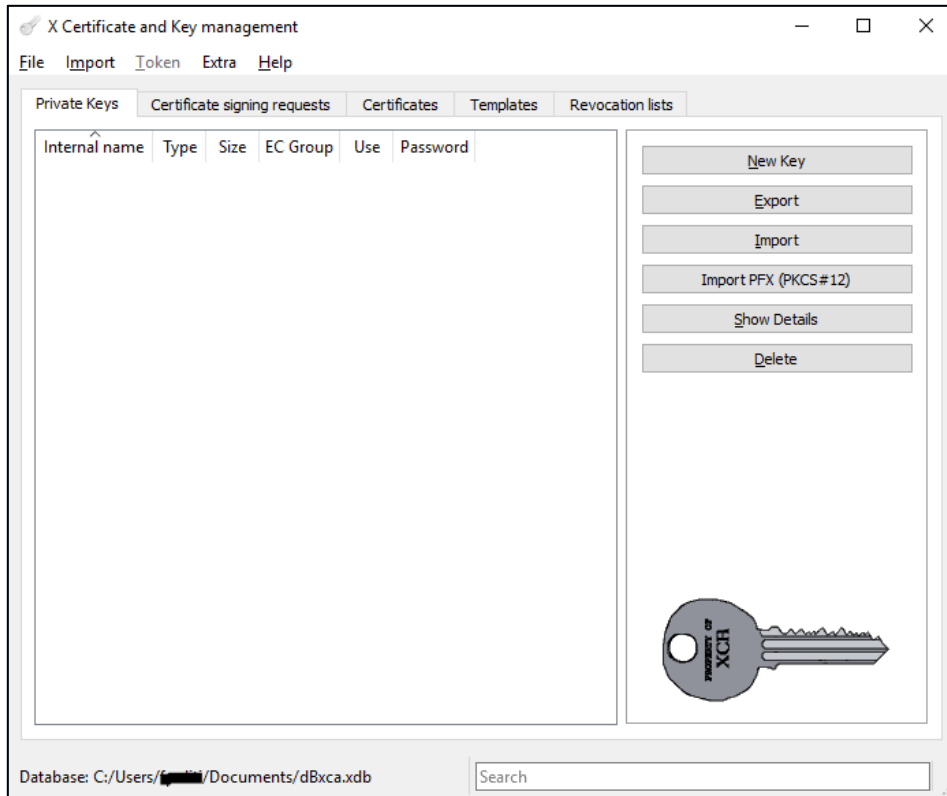


Figura 6 - Schermata dello spazio di lavoro

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.

3.2 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 7):
 - **Name** = key
 - **Keytype** = selezionare 'RSA'
 - **Keysize** = selezionare '2048 bit'

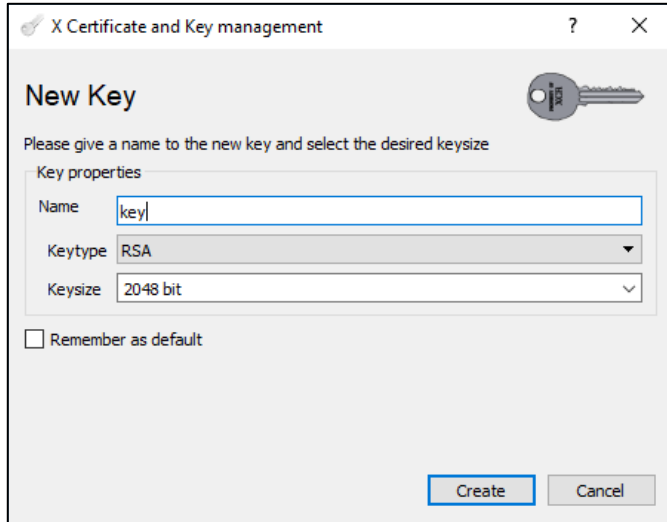


Figura 7 - Nuova Chiave

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

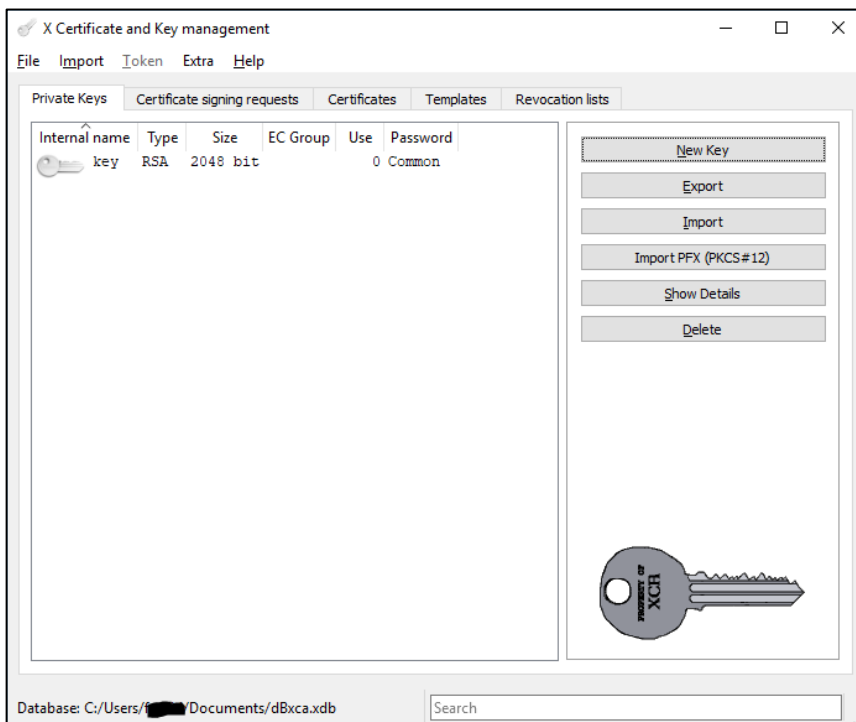
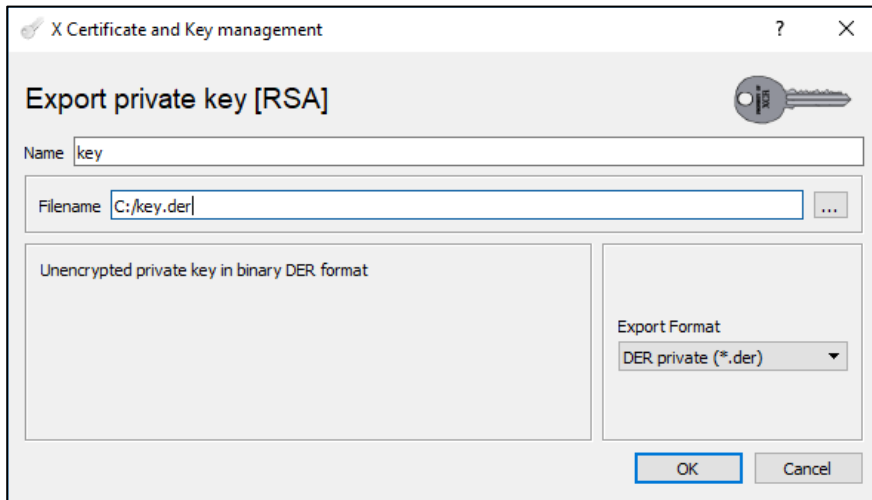


Figura 8 - Chiave generata correttamente

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 9*):

- **Name** = key
- **Filename** = C:/key.der
- **Export Format**: selezionare 'DER private (*.der)'



Formattato: Inglese (Stati Uniti)

Formattato: Inglese (Stati Uniti)

Formattato: Inglese (Stati Uniti)

Figura 9 - Salvare il file in formato .der

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

3.3 Creare un file req.der

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

X Certificate and Key management

Create Certificate signing request

Source | Subject | Extensions | Key usage | Netscape | Advanced

Signing request

unstructuredName

challengePassword

Signing

Create a self signed certificate with the serial

Use this Certificate for signing

Signature algorithm

Template for the new certificate

Figura 10 - Nuovo CSR

2. Nella tab "Source" compilare i seguenti campi:

- **unstructuredName**: codice fiscale di chi genera la CSR
- **challengePassword**: 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** = Agenzia delle Dogane
- **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;

X Certificate and Key management

Create Certificate signing request

Source Subject Extensions Key usage Netscape Advanced

Distinguished name

Internal name organizationName

countryName organizationalUnitName

stateOrProvinceName commonName

localityName emailAddress

Type	Content
------	---------

Add
Delete

Private key

key (RSA:2048 bit) Used keys too

OK Cancel

Figura 11 - 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";

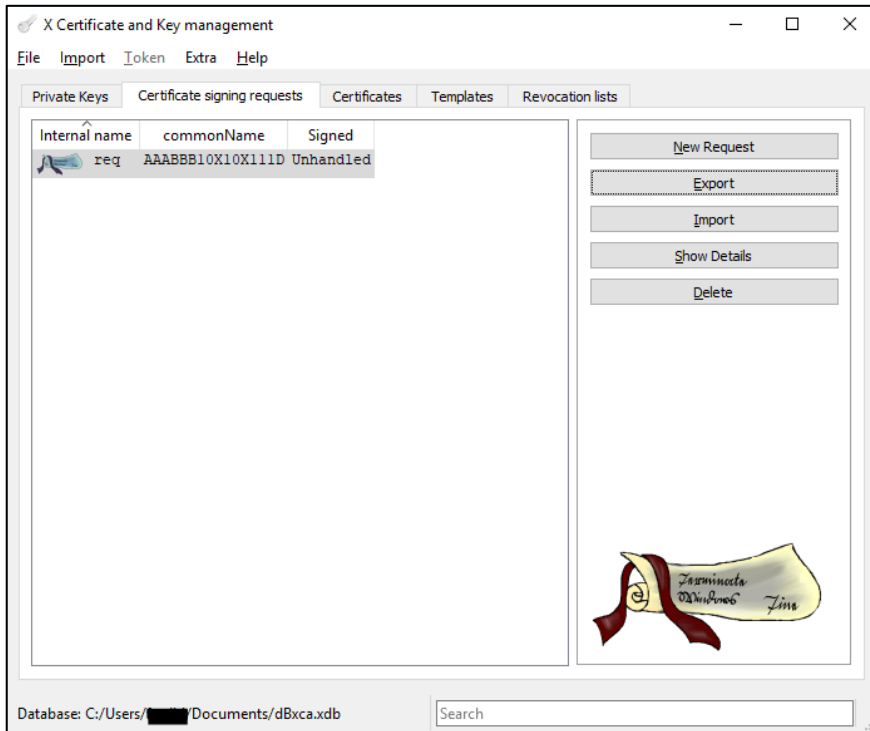


Figura 12 - CSR creato

7. Apparirà la finestra "Certificate request export" e bisognerà compilare i seguenti campi:

- **Name** = req
- **Filename** = C:/req.der
- **Export Format** = DER (*.der)

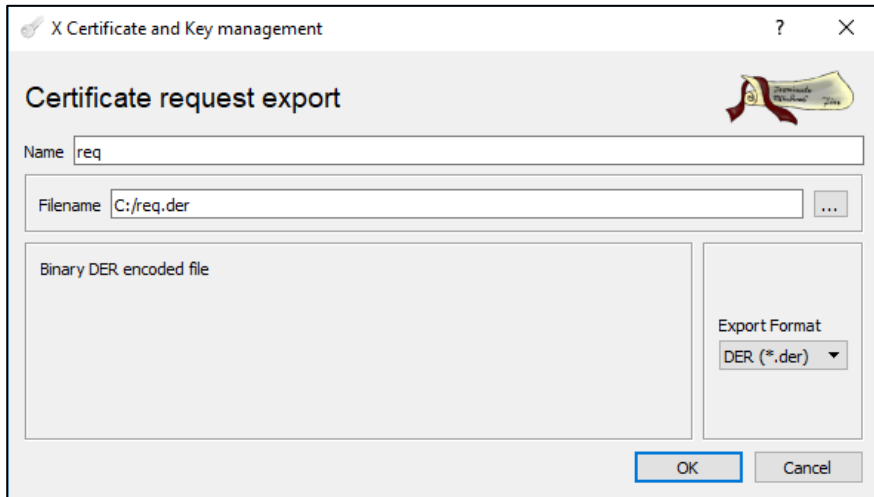


Figura 13 - Export di una CSR

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

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

9. Per effettuare l'upload del file req.der creato in precedenza, cliccare su "Sfoglia"

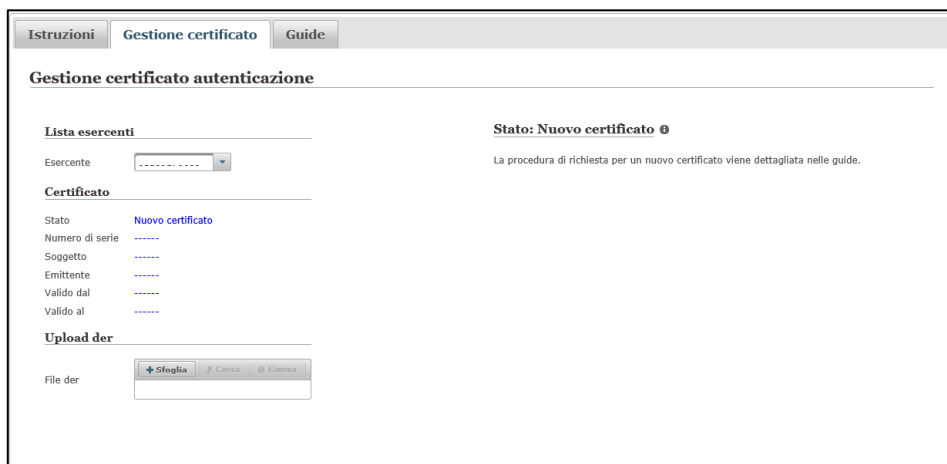


Figura 14 - Riquadro dei file di cui fare l'upload

10. Andare sulla directory "C:"

11. Selezionare il file req.der e cliccare su "Apri"

12. Si vedrà apparire il file nella lista dei file selezionati

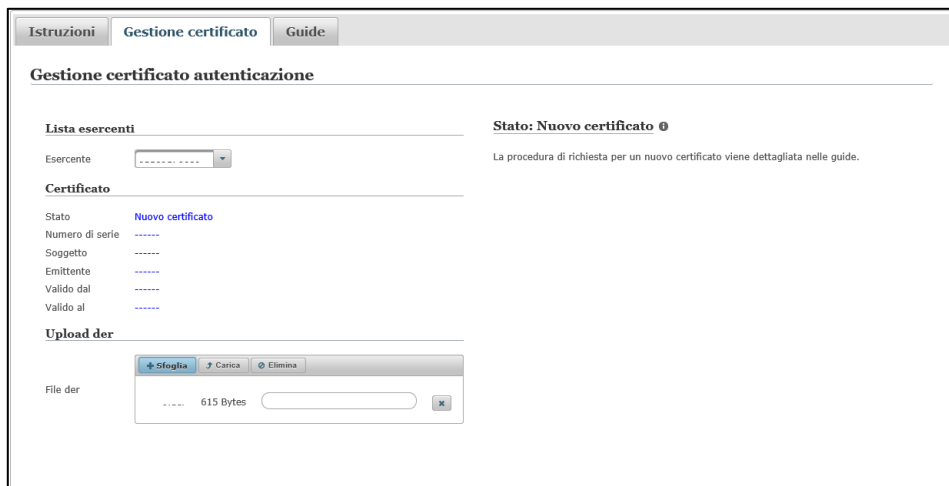


Figura 15 - File req.der selezionato

13. Cliccare su "Upload" per eseguire l'upload del file, la barra bianca si colorerà visualizzando l'avanzamento del caricamento
14. terminato l'upload si avrà la seguente schermata:

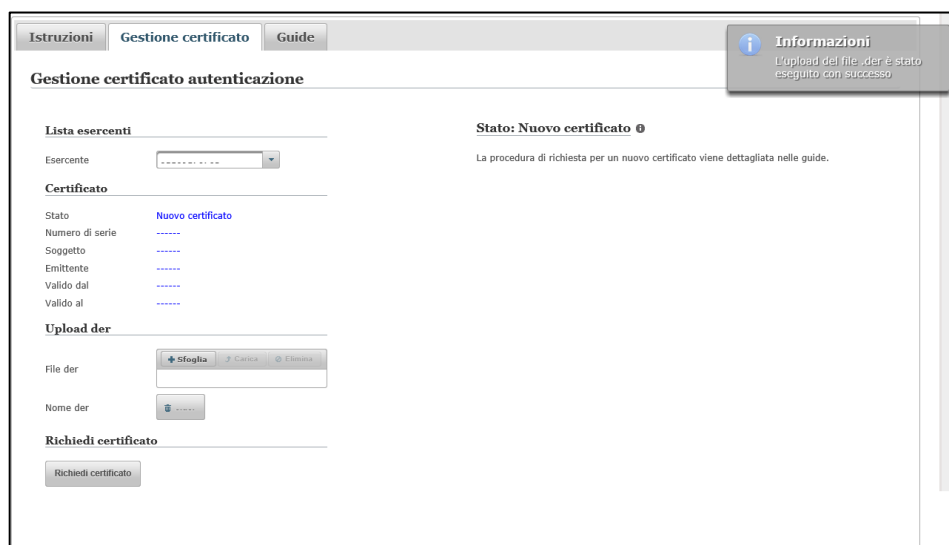


Figura 16 - Upload avvenuto con successo

15. L'Upload del file req.der è avvenuto con successo
16. Procedere con la richiesta del certificato cliccando su "Richiedi Certificato"



Figura 17 - Certificato richiesto

17. Procedere adesso con lo scarico del certificato cliccando su "Download Certificato" e salvare il file scaricato nella directory "C:/"

3.5 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 18* selezionando dal campo "Export Format":
 - PEM all (*.pem)
 - PKCS #12 (*.p12)

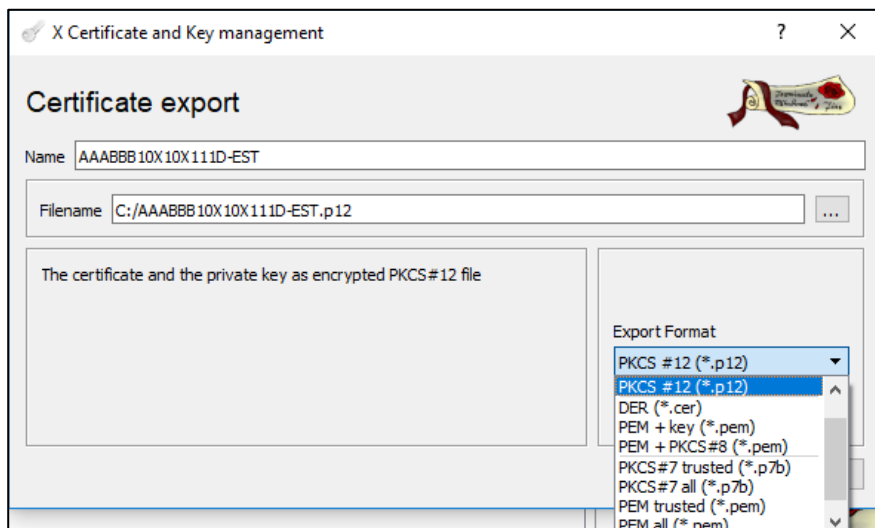


Figura 18 - Export di un certificato