PDF-XChange Viewer Click to buy NOW! www.docu-track.com

Guida alla creazione e certificazione di chiavi di autenticazione SSL MIME Class 2

Indice

1 INTRODUZIONE

Per poter usufruire del servizio Postecom per l'emissione di un certificato di sicurezza Client SSL MIME Class 2 è necessario che il cliente produca una richiesta di certificazione in formato PKCS#10 anche detta CSR (Certificate Signing Request) e che la inoltri a Postecom tramite il portale del MePA.

Postecom provvederà ad emettere ed inviare al cliente un certificato contenente le seguenti informazioni presenti nella richiesta PKCS#10:

- **COMMON NAME (CN)** = [COGNOME NOME]
- **ORGANIZATION NAME (O)** = [NOME DELL'ORGANIZZAZIONE] (es. COMUNE DI XXX)
- **EMAIL ADDRESS (E)**= [indirizzo email] (l'indirizzo sarà utilizzato per il recapito del certificato)

Affinché il certificato sia riconosciuto attendibile all'interno dell'ambito applicativo di utilizzo potrà essere necessario importare preliminarmente il certificato di certificazione Postecom CA3 allegato al catalogo.

Ciò potrà essere necessario anche da parte del servizio al quale ci si autenticherà. **Nel caso del servizio del Centro Nazionale Trapianti, l'accreditamento del certificato di Postecom è già stato effettuato.**

La richiesta di certificazione, relativa alle chiavi crittografiche generate dal cliente, potrà essere prodotta attraverso i software prescelti dal cliente o attraverso le istruzioni e gli strumenti riportati nella presente guida.

Qualora il cliente proceda ad utilizzare un proprio software è importante che la richiesta PKCS#10 prodotta contenga i campi sopra indicati e sia relativa a chiavi di lunghezza 2048bit.

La presente guida è finalizzata ad illustrare le operazioni di:

- creazione chiavi crittografiche e generazione richieste di certificazione (PKCS#10)
- creazione di archivi sicuri per la custodia/importazione delle chiavi crittografiche (PKCS#12)

Nel seguito verranno illustrate le sopracitate procedure mediante le due soluzioni alternative:

- OpenSSL
- Portecle

OpenSSL e Portecle sono due soluzioni Open Source finalizzate alla gestione di chiavi crittografiche; la prima mediante promt dei comandi, la seconda mediante una semplice interfaccia grafica.

2 REQUISITI MINIMI

I requisiti minimi per l'utilizzo di OpenSSL sono:

- Windows XP / 2003 / Vista / 2008 con msvcrt.dll e msvcp60.dll. Se i file msvcrt.dll o msvcp60.dll non sono presenti nella cartella Windows/System, è possibile ottenerli istallando Internet Explorer 4.0 o superiore.

I requisiti minimi per l'utilizzo di Portecle sono:

- Windows XP Professional 32bit
- Java SE 6 o superiore. L'ultima versione di Java SE è reperibile da: http://www.oracle.com/technetwork/java/index.html

Entrambi i tool sono stati testati anche su versioni più recenti di Windows quali Windows 7 and 8 nelle versioni a 32/64 bit.

I tool non richiedono la connessione ad internet.

In quanto soluzioni Open Source esistono versioni anche per altri sistemi operativi per i quali si rimanda direttamente alle pagine dei singoli progetti:

- http://www.openssl.org
- http://portecle.sourceforge.net/

3 INSTALLAZIONE

Di seguito sono illustrate le procedure di installazione delle due soluzioni software alternative. Qualora si incontrassero dei problemi si prega consultare la sezione FAQ della presente guida.

3.1 OPENSSL

OpenSSL è disponibile sul sito del progetto:

- http://www.openssl.org

Suggeriamo di utilizzare la versione portable del tool reperibile presso:

- http://openssl-for-windows.googlecode.com/files/openssl-0.9.8k_WIN32.zip

Una volta scaricato il software scompattare il file compresso in una cartella. L'applicazione si trova nella sottocartella "bin".

3.2 PORTECLE

Portecle è disponibile sul sito del progetto:

- http://portecle.sourceforge.net/ .

La versione per MS Windows è disponibile presso:

- http://sourceforge.net/projects/portecleinstall/?source=recommended_dlp_t4

Per installare il software:

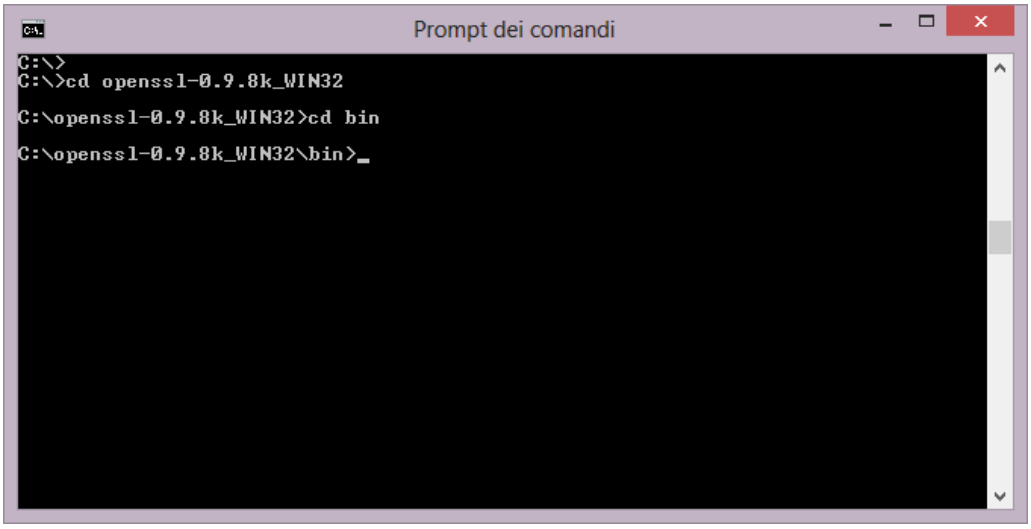
- Effettuare un doppio click sulla versione scaricata "Portecle-Installer-[X.Y].exe" e seguire le istruzioni del Wizard.

4 FASE DI GENERAZIONE DELLE CHIAVI E DELLA RICHIESTA

Di seguito sono illustrate le procedure di generazione delle chiavi e della richiesta mediante le due soluzioni software alternative. Qualora si incontrassero dei problemi si prega consultare la sezione FAQ della presente guida.

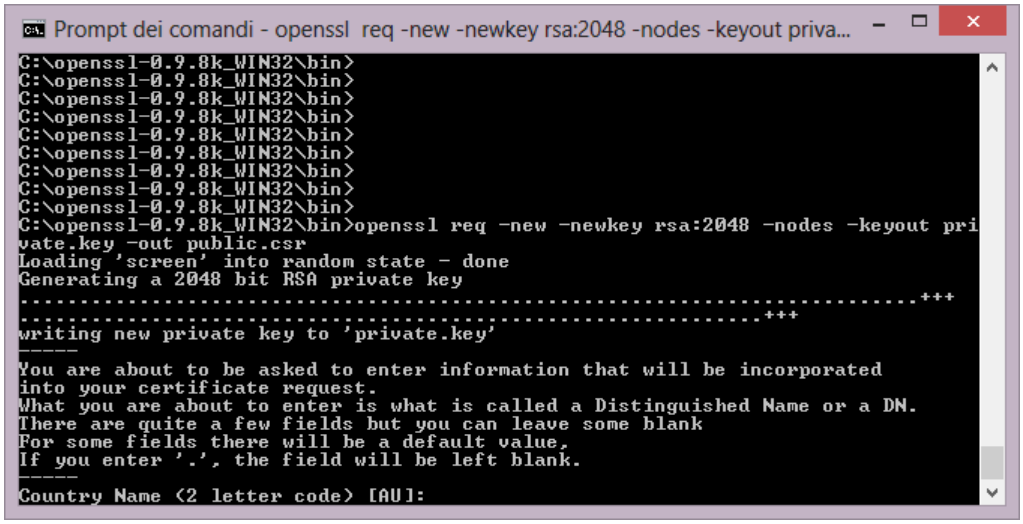
4.1 OPENSSL

Aprire il prompt dei comandi (cmd.exe) e posizionarsi nella cartella “bin” dove è stato scompattato l’archivio di OpenSSL (nel caso specifico c:\openssl-0.9.8k_WIN32\bin)

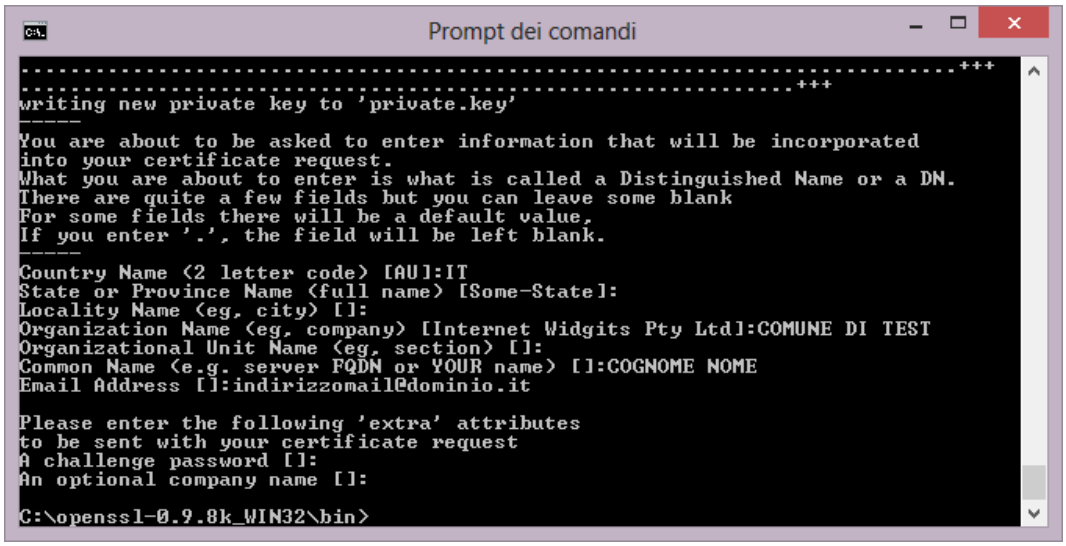


1. Lanciare il comando “**openssl req –new –newkey rsa:2048 -nodes -keyout private.key -out public.csr**”, dove:
   - “private.key” è il nome del contenitore della chiave privata
   - “public.csr” è il nome della richiesta in formato PKCS#10

   I nomi possono essere modificati a piacimento da parte del cliente.
2. Il tool chiederà di inserire i campi da certificare:



3. Inserire:
   - **Country Name**: “IT”.
   - **Organisation Name**: Nome dell’organizzazione di appartenenza (es. COMUNE DI XXX), scritto in lettere maiuscole.
   - **Common Name**: COGNOME NOME del titolare del certificato scritto in lettere maiuscole
   - **E-mail address**: indirizzo della casella di posta elettronica dove recapitare il certificato, scritto in lettere minuscole



4. Effettuare un “invio” per le altre voci e richieste
5. **<u>Il file salvato nella cartella /bin dovrà essere firmato digitalmente e allegato all’ordine MePA.</u>**

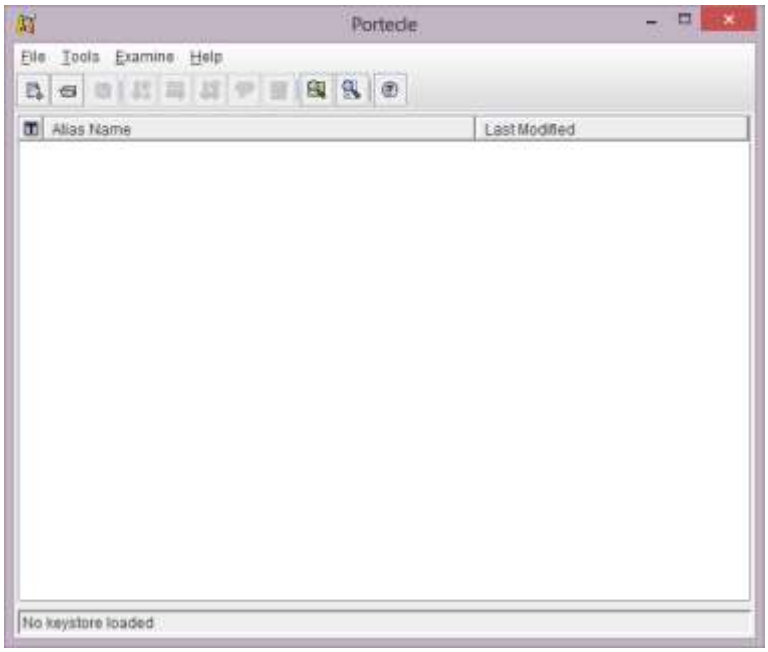
4.2 PORTECLE

Per attivare Portecle effettuare doppio clic sull’icona 

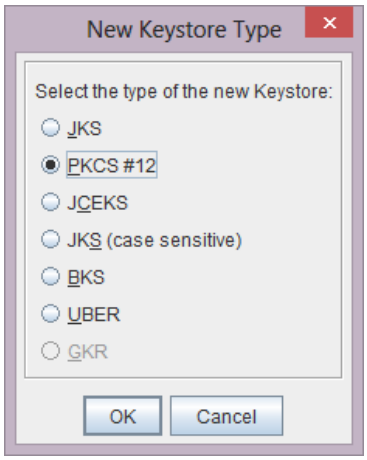
presente sul desktop.

Il primo passo è la definizione di un “Keystore”:

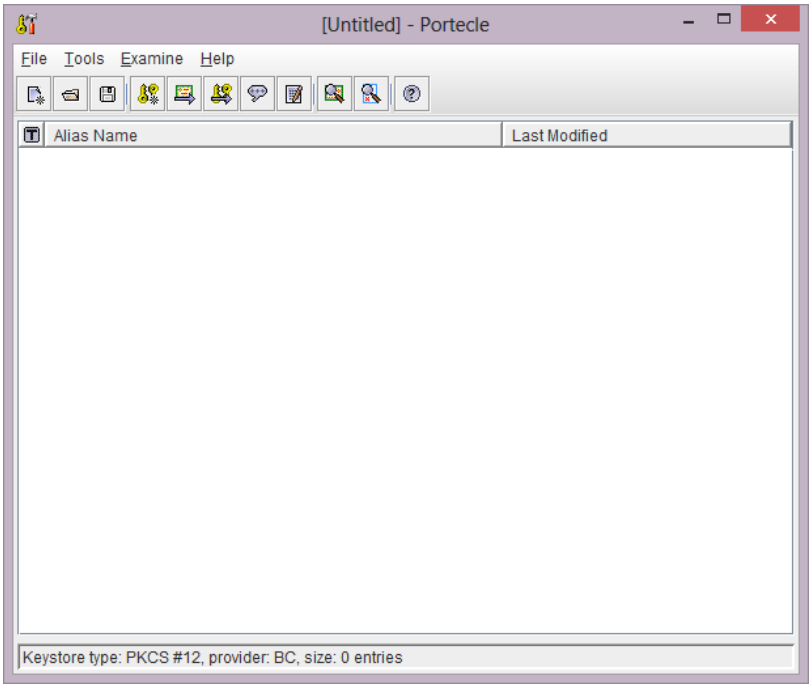
1. Dal menù "**File",** scegliere **"New Keystore".** In alternativa cliccare sul pulsante **"New Keystore"** presente sulla barra degli strumenti:



2. Dal dialogo **"New Keystore Type"** che segue, selezionare PKCS#12, e premere il bottone "OK"

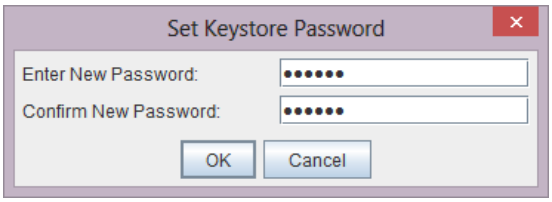


3. La barra del titolo cambierà in **"Untitled"** e la barra di stato mostrerà il tipo di Keystore selezionato.

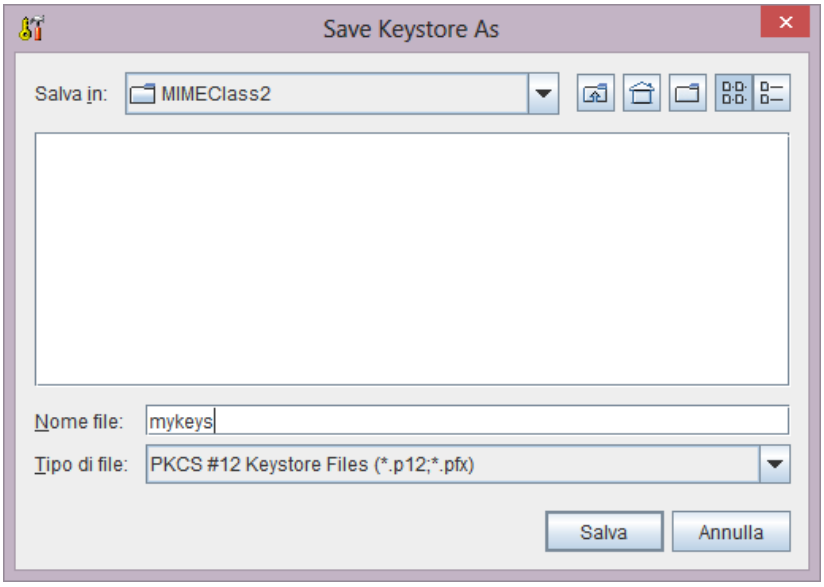


4. Dal menù "**File"**, scegliere **"Save Keystore"**. In alternativa cliccare sul bottone **"Save Keystore"** presente sulla barra degli strumenti:

5. Se è la prima volta verrà richiesto di inserire una password di protezione del keystore:
   - La finestra **"Set Keystore Password"** viene mostrata.
   - Inserire la password di protezione e confermare cliccando sul bottone **"OK".**



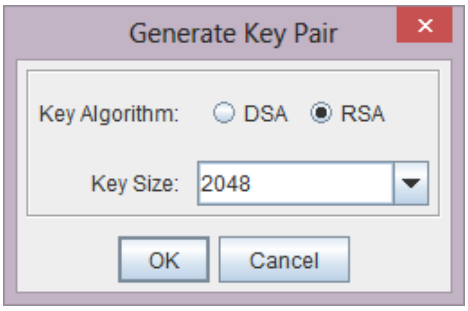
6. Viene mostrata la finestra **"Save Keystore As"**.
7. Selezionare la cartella dove si vuole salvare il file (Nota: verificare che si posseggano i diritti di scrittura su tale cartella).
8. Inserire il nome del file nel campo **"Nome file"**.



9. Cliccare sul bottone **"Salva"**.

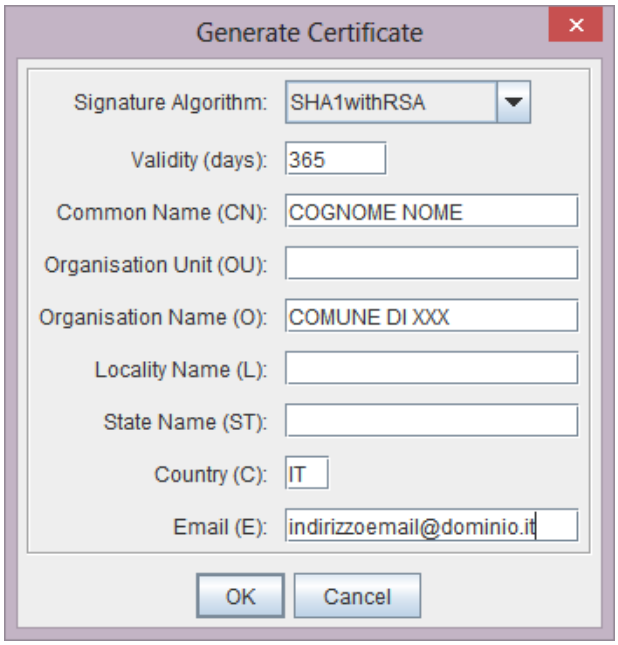
10. Dal menù **"Tools",** scegliere **"Generate Key Pair"**. In alternativa cliccare sul bottone della barra degli strumenti **"Generate Key Pair"**:

11. Viene mostrata la finestra **"Generate Key Pair"**. Selezionare **"RSA"** Key Algorithm and **"2048"** per la **"Key Size"** e cliccare sul bottone **"OK"** per confermare. La generazione della chiave avrà inizio in background.



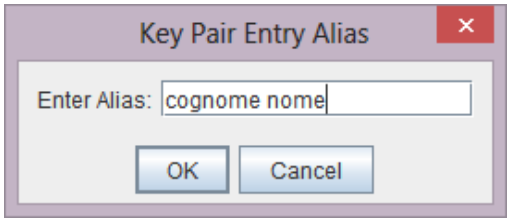
12. Viene mostrata la finestra **"Generate Certificate"**.

13. Inserire i dati da certificare, quindi cliccare sul bottone **"OK"**.

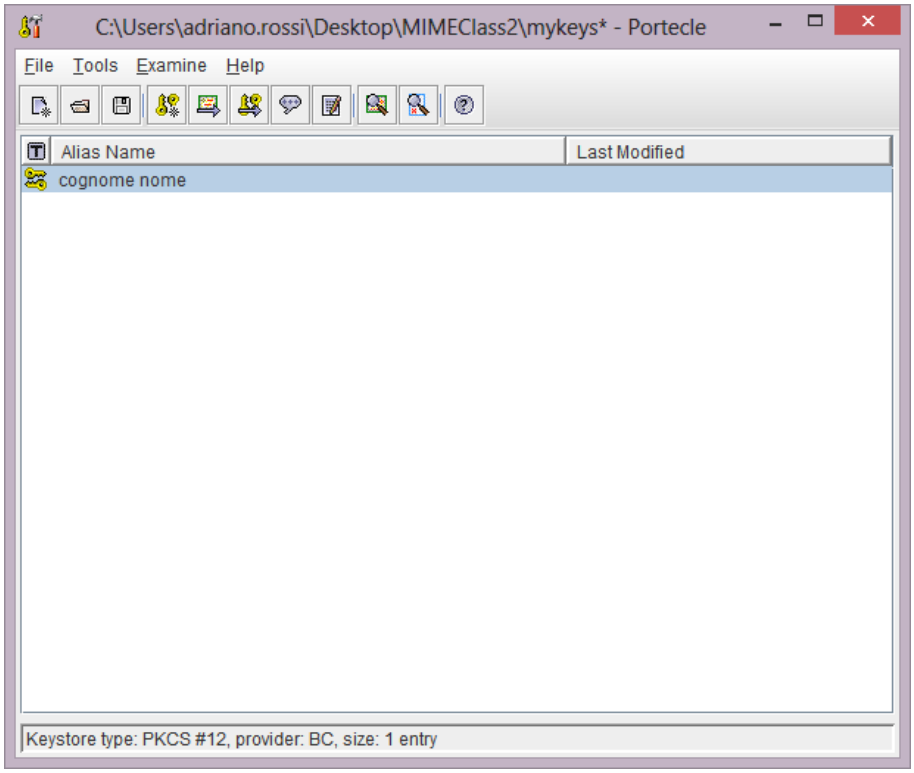


- **Country**: “IT”.
- **Organisation Name**: Nome dell’organizzazione di appartenenza (es. COMUNE DI XXX), scritto in maiuscolo.
- **Common Name**: COGNOME NOME del titolare del certificato scritto in lettere maiuscole
- **E-mail:** indirizzo della casella di posta elettronica dove recapitare il certificato, scritto in lettere minuscole

14. Viene mostrata la finestra **”Key Pair Entry Alias”**.

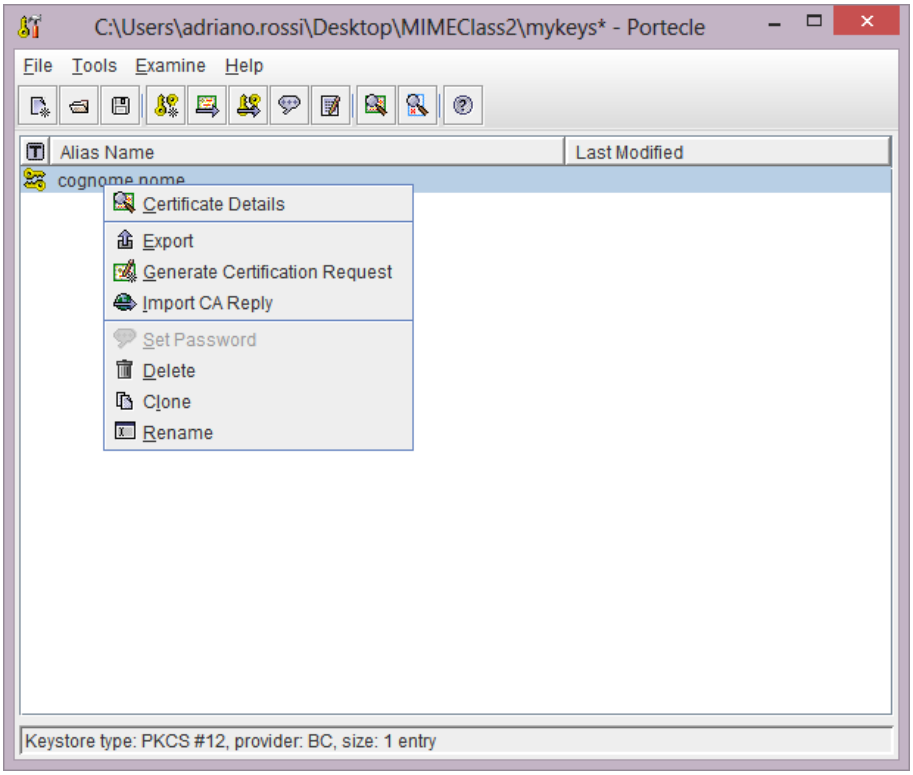


15. Inserire l’alias per le chiavi appena generate e confermare cliccando sul bottone **“OK”**
16. L’alias delle chiavi viene mostrato nella tabella del keystore.

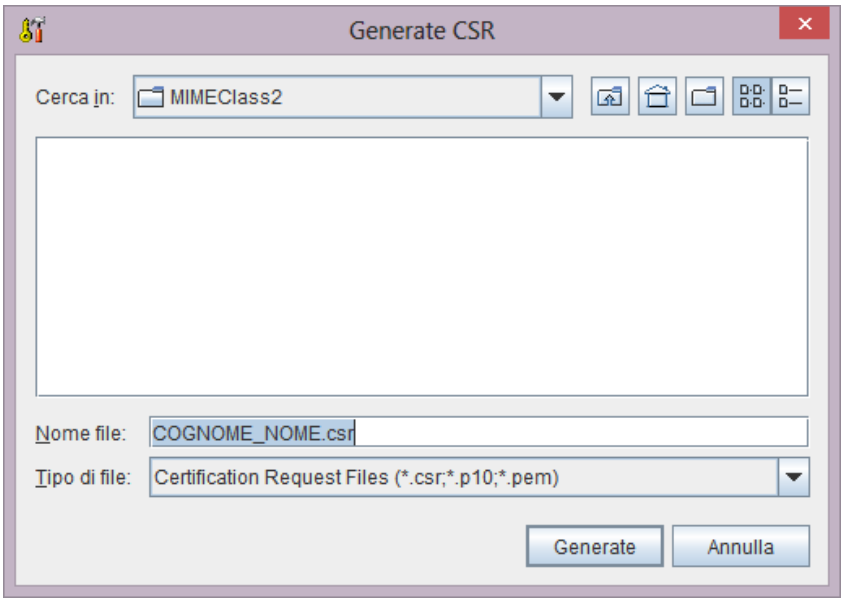


Una volta che le chiavi sono state generate e sono stati definiti i dati da certificare, occorre generare e salvare la richiesta PKCS#10, anche detta Certificate Request.

1. Cliccare sul tasto destro del mouse sull'alias della chiave. Selezionare la funzione **"Generate Certification Request"** dal menù pop-up.



2. Viene mostrata la finesta **"Generate CSR"**. Selezionare la cartella dove salvare la richiesta.



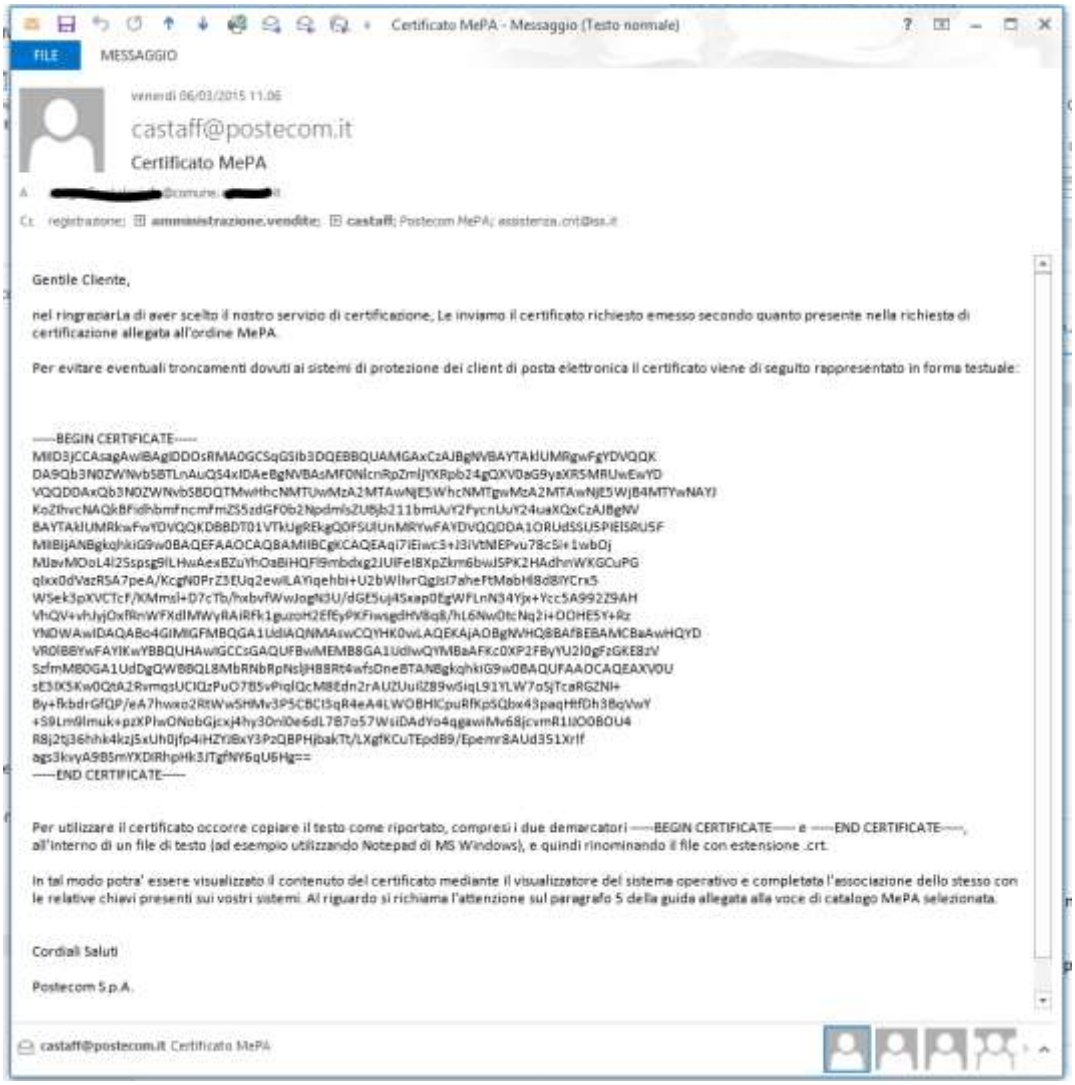
3. Inserire il nome del file nel campo **"Nome file"**.
4. Cliccare sul bottone **"Generate"**.
5. In chiusura del software salvare per conservare la chiave privata generata.
6. **Il file salvato dovrà essere firmato digitalmente e allegato all'ordine MePA.**

Il salvataggio di cui al punto 5 è necessario per la conservazione della chiave privata che sarà associata al certificato emesso dal certificatore, mediante la procedura descritta al par. 6.2.

5 Ricezione del certificato

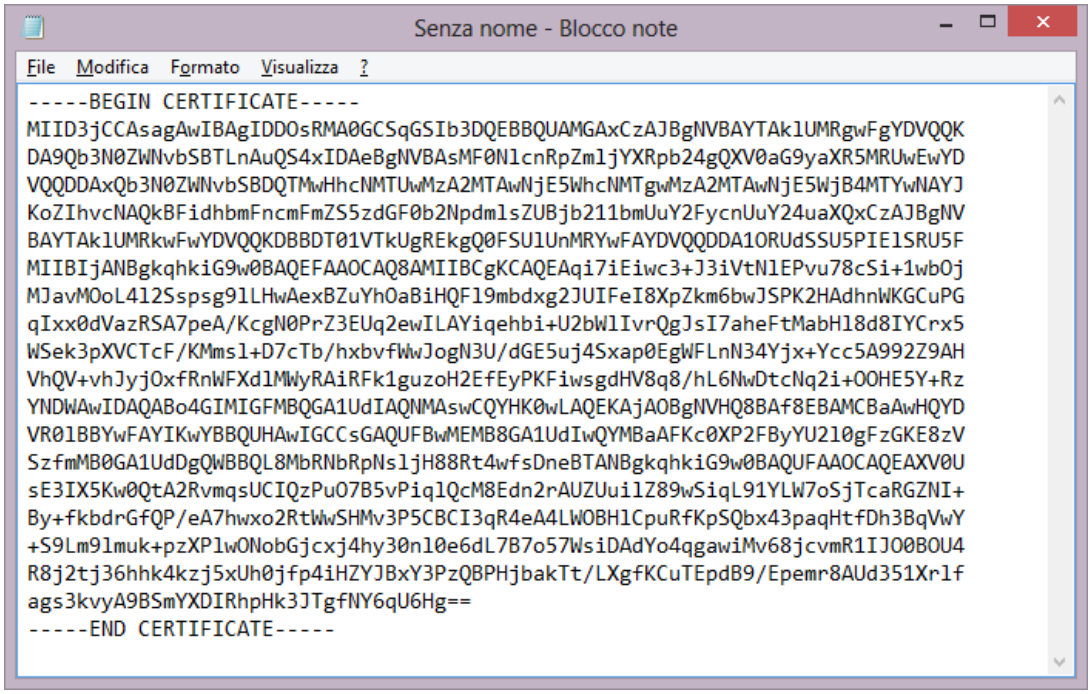
A seguito della ricezione della richiesta PKCS#10 (CSR) da parte del certificatore, verrà generato il certificato, che il certificatore curerà di spedire via mail all'indirizzo indicato all'interno della CSR.

Poiché diversi sistemi di protezione impediscono l'invio di certificati in allegato a messaggi di e-mail, il certificato sarà incorporato nel messaggio stesso.



Come descritto nella stessa mail, per utilizzare il certificato, occorre:

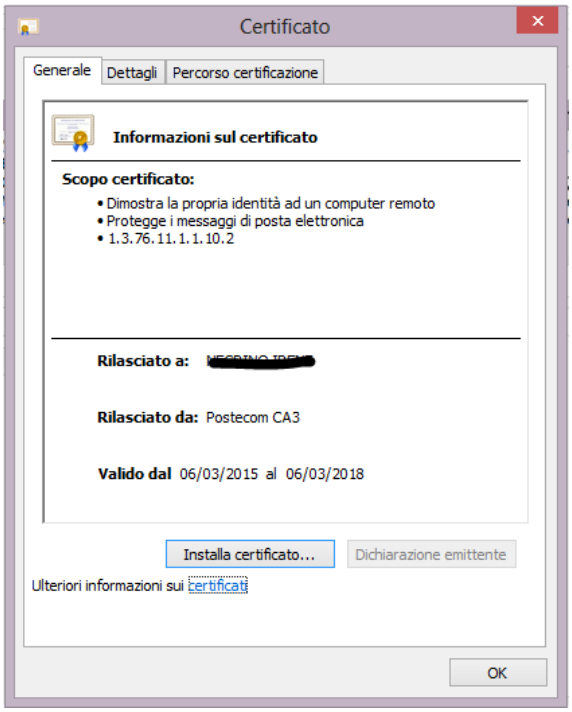
1. Copiare il testo, compresi i delimitatori del certificato all'interno di un file di testo (es. notepad di MS Windows), curando di eliminare tutti gli spazi prima e dopo i delimitatori



2. Salvare il file con estensione .crt (es. COGNOME_NOME.crt).

Per verificare che il file sia funzionante:

3. Effettuare un doppio click sul file COGNOME_NOME.crt appena creato.
4. Se il risultato è equivalente al seguente allora si prosegua con il capitolo successivo, altrimenti verificare che non siano presenti spazi dopo le ultime “-----“ e ripetere le operazioni:



6 IMPORTAZIONE ED ESPORTAZIONE

Una volta ricevuto da Postecom il certificato, è necessario accoppiarlo alla chiave crittografica ed esportare il tutto in un contenitore sicuro protetto da password definito secondo lo standard PKCS#12. Per la generazione del file PKCS#12 è necessario avere a disposizione anche il certificato di CA di Postecom, che è presente come allegato al catalogo Postecom pubblicato sul portale del MePA.

Il file PKCS#12 potrà quindi essere importato nel contesto applicativo che effettuerà l'autenticazione al servizio del Centro Nazionali Trapianti.

Di seguito sono illustrate le procedure di importazione ed esportazione mediante le due soluzioni software alternative. Qualora si incontrassero dei problemi si prega consultare la sezione FAQ della presente guida.

6.1 OPENSSL

Dopo aver salvato il file ricevuto e copiato il certificato di CA (con estensione ".pem") all'interno della sottocartella "bin" di Openssl, aprire una finestra di comando e posizionarsi nella sottocartella "bin"

1. Lanciare il comando "**C:\openssl-0.9.8k_WIN32\bin>openssl pkcs12 -export -inkey private.key -in COGNOME_NOME.crt -CAfile Postecom_CA3.pem -chain -out COGNOME_NOME.p12**"

   Dove *COGNOME_NOME.crt* è il file ricevuto da Postecom, *Postecom_CA3.pem* è il nome del file contenente il certificato di CA e *COGNOME_NOME.p12* è il nome del file PKCS#12 che conterrà chiave e certificati.
2. Se tutto è corretto il tool chiederà di definire (e confermare) una password di protezione (Export Password).

Il file PKCS#12 può essere importato nel contesto applicativo di utilizzo semplicemente effettuando un doppio-click sul file e seguendo le istruzioni del Wizard.

6.2 PORTECLE

Occorre effettuare i tre seguenti passi:

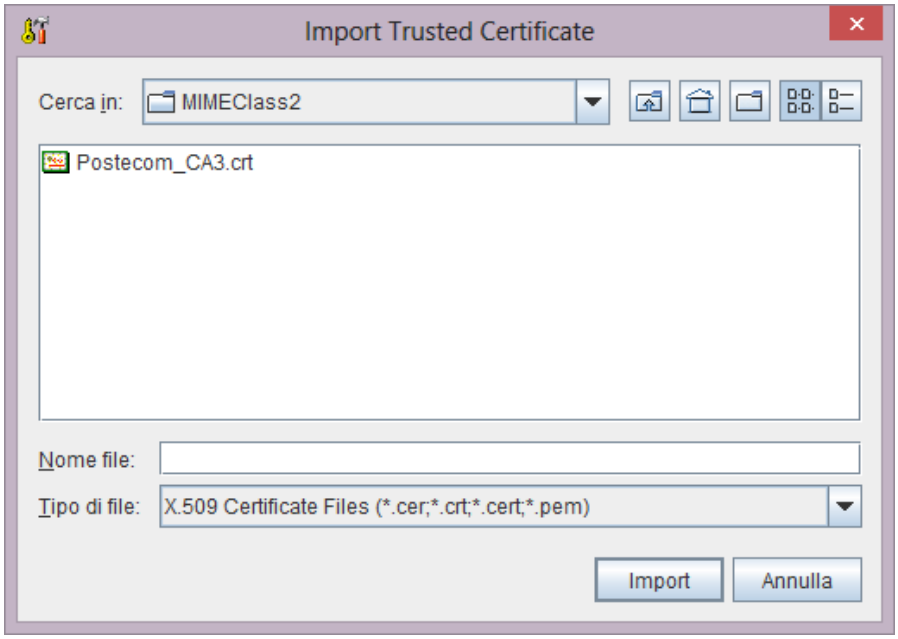
- Importare del certificato di CA di Postecom (in Portecle è chiamato "**Trusted Certificate**") presente in allegato al catalogo Postecom pubblicato sul portale MePA;
- Importare il certificato utente (in Portecle chiamato "**CA Reply**");
- Esportare il file PKCS#12 (in Portecle chiamato "**KeyStore entry**").

Per importare il certificato di CA nel keystore attraverso il file fornito da Postecom:

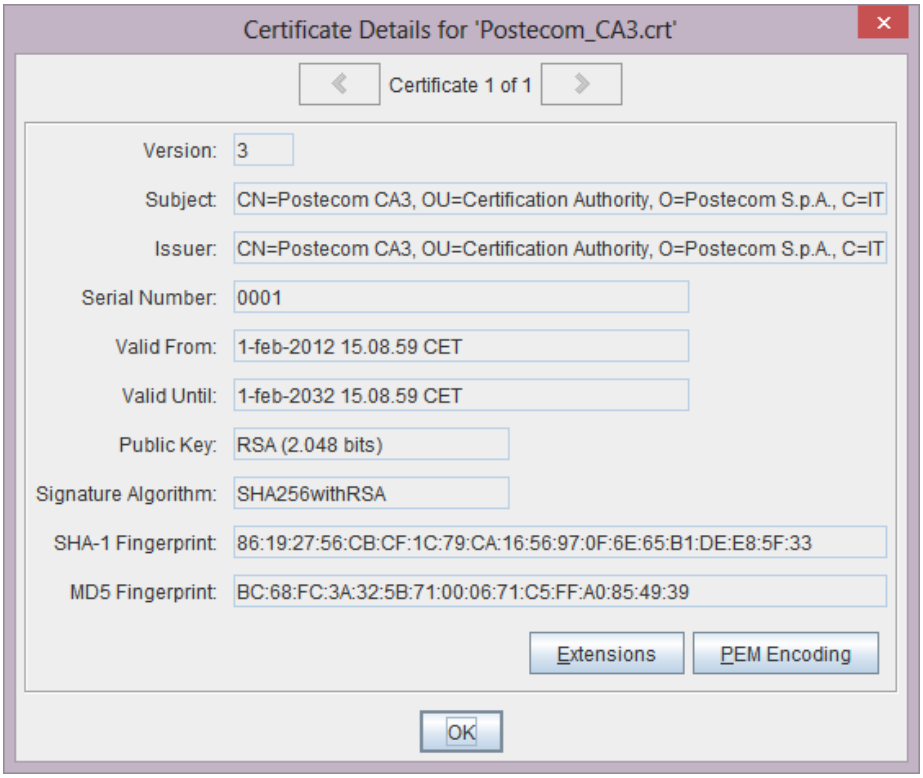
1. Lanciare il software Portecle
2. Aprire il keystore utilizzato in fase di generazione della chiave privata e della CSR di cui al par. 4.2, che nell'esempio è chiamato "mykeys". Dal menù "**File**", scegliere "**Open Keystore File**;
3. Selezionare il file "mykeys" e quindi cliccare sul bottone "**Apri**";
4. Inserire la password di protezione definita al par. 4.2, passo 5.

5. Dal menù “**Tools”**, scegliere “**Import Trusted Certificate”**. In alternativa cliccare sul bottone della barra degli strumenti “**Import Trusted Certificate”**:


6. Viene mostrata la finestra “**Import Trusted Certificate”**.

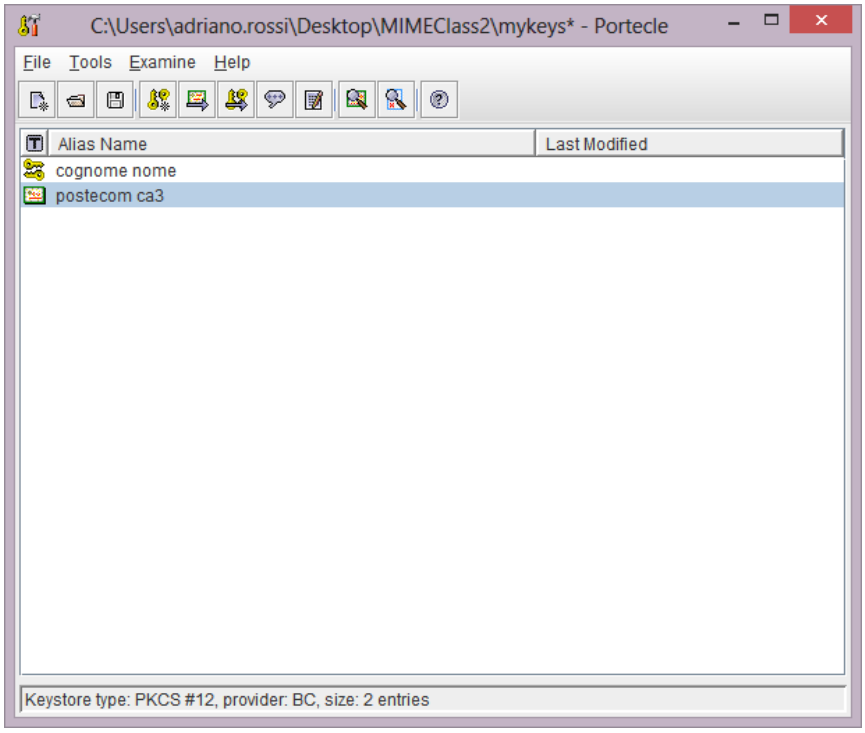


7. Selezionare la cartella dove si trova il file da importare.
8. Cliccare sul file da importare o scriverne il nome nel campo **”Nome file”**.
9. Cliccare sul bottone **“Import”**.
10. Se Portecle non può stabilire la catena di trust mostrerà una finestra per confermare l’importazione:
    - Viene mostrata la finestra **“Certificate Details**”.



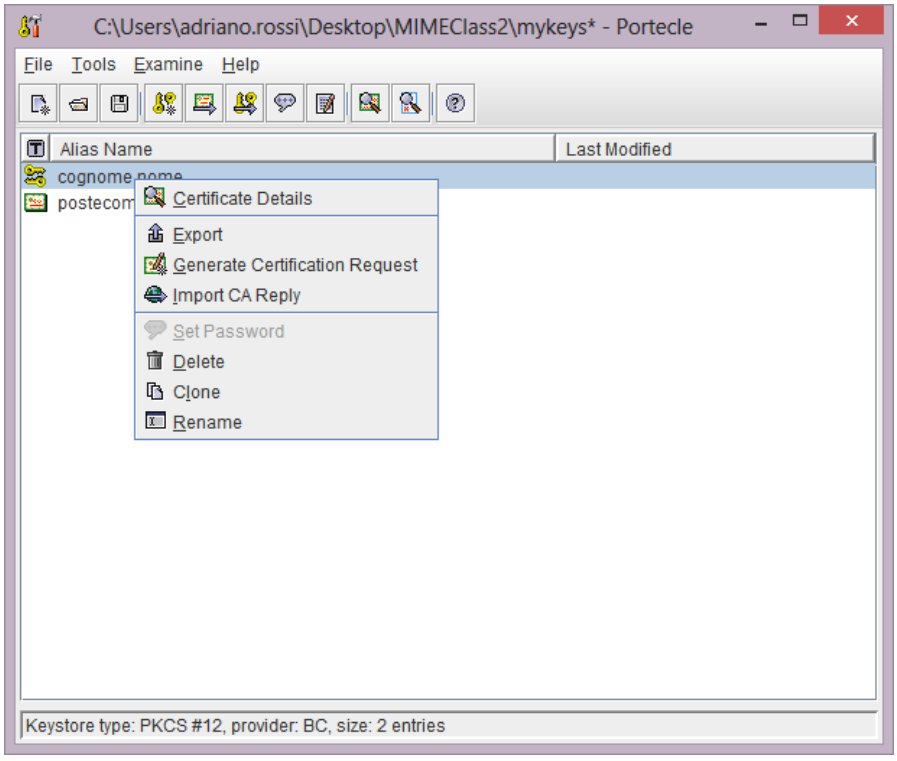
- Dopo aver rivisto i dettagli confermare l'importazione cliccando sul bottone **"OK"**.
- Un ulteriore finestra chiederà di confermare.
- Cliccare sul bottone **"Sì"** per confermare.

11. Viene mostrata la finesta **"Trusted Certificate Alias"**.
12. L'alias del certificato viene mostrato nel keystore.

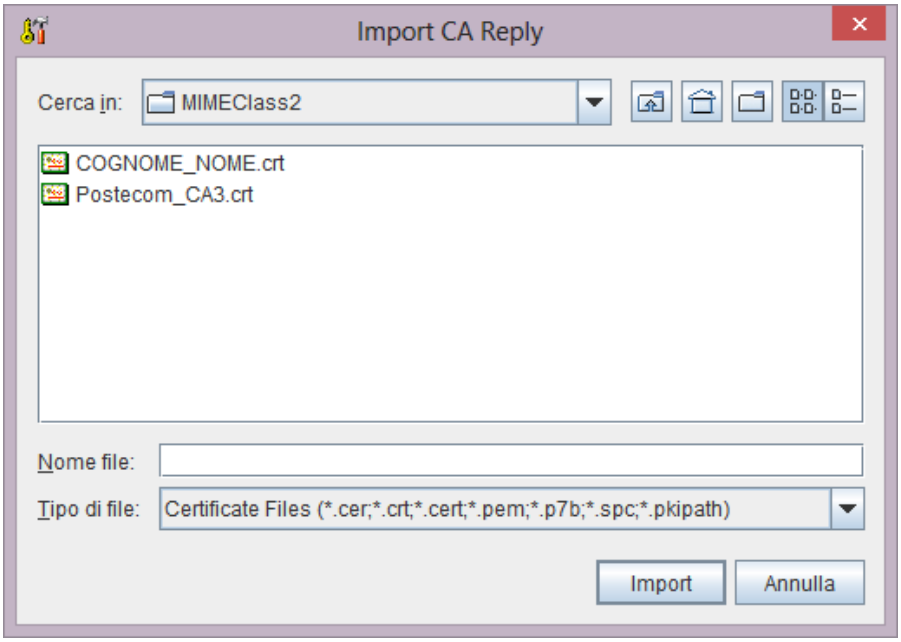


Per importare il certificato utente nel keystore:

1. Cliccare il tasto destro del mouse sull'alias delle chiavi relative al certificato. Selezionare la funzione **"Import CA Reply"** all'interno del menù pop-up.



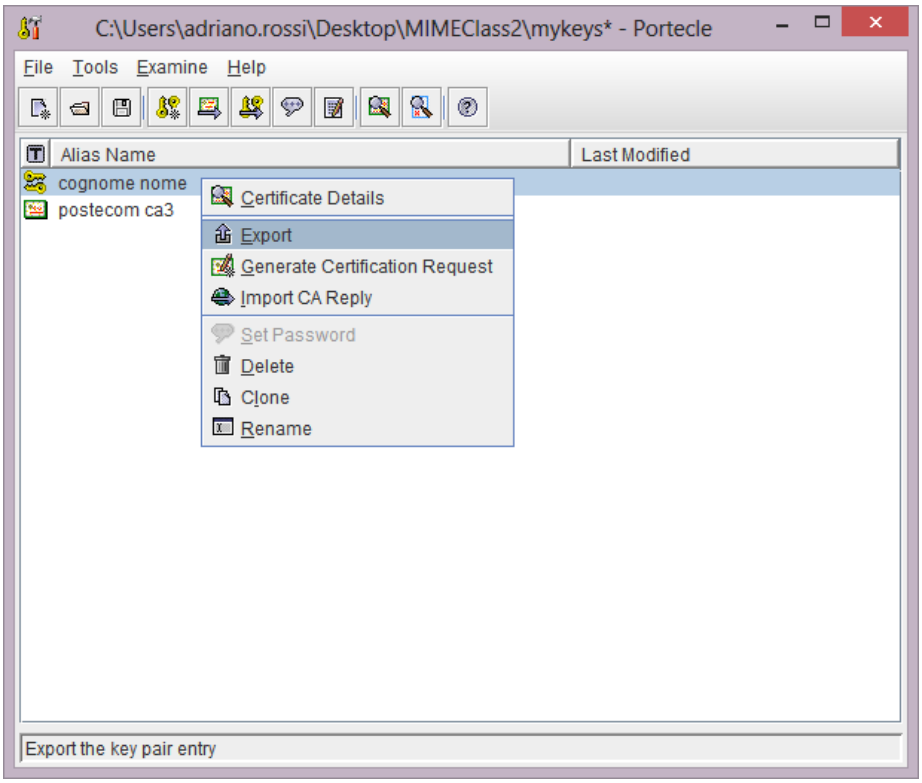
2. Viene mostrata la finestra **"Import CA Reply"**.



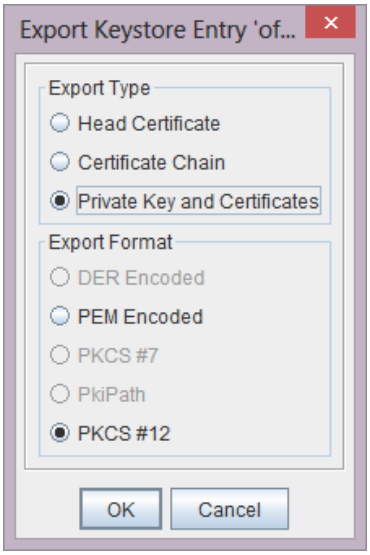
3. Selezionare la cartella dove si trova il certificato da importare.
4. Cliccare sul file del certificato o inserire il nome nel campo **“File Name”**.
5. Cliccare sul bottone **“Import”**.
6. Il keystore viene aggiornato con l’accoppiamento del certificato alla chiave corrispondente.

Per esportare chiave e certificato nel file PKCS#12:

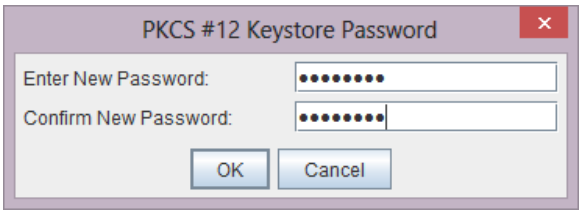
1. Cliccare con il tasto destro del mouse sull’alias del certificato da esportare. Selezionare la funzione **“Export”**dal menù pop-up.



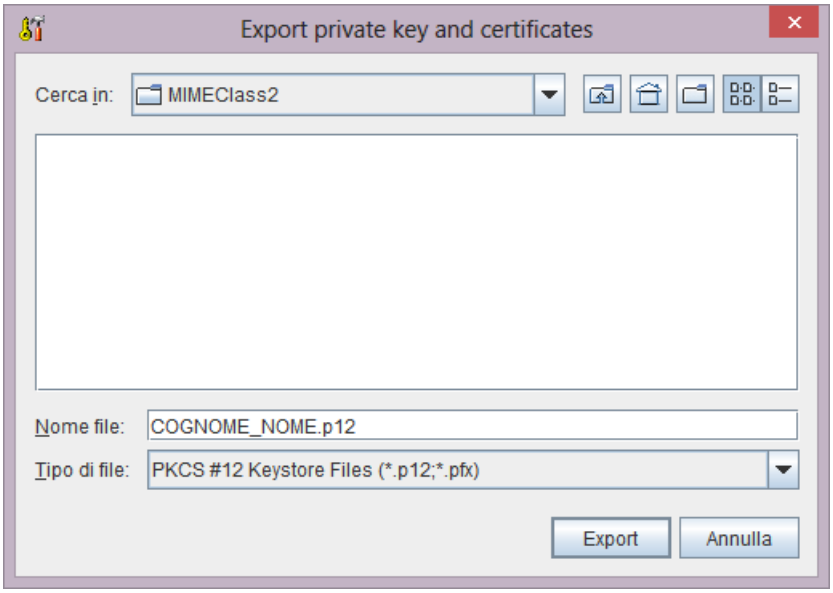
2. Viene mostrata la finestra **"Export Keystore Entry"**.



3. Scegliere **"Private Key and Certificates"** e **"PKCS#12**" quindi cliccare sul bottone **"OK"**.
4. Viene mostrata la finestra **"PKCS #12 Keystore Password"**.
    - Inserire la password di protezione del keystore esportato e confermare cliccando sul bottone **"OK"**.



5. Viene mostrato il dialogo **“Export”**.



6. Selezionare la cartella dove esportare il keystore.
7. Scrivere il nome del file nel campo **“Nome File**”.
8. Cliccare sul bottone **“Export”**.

Il file PKCS#12 può essere importato nel contesto applicativo di utilizzo semplicemente effettuando un doppio-click sul file e seguendo le istruzioni del Wizard.

7 Frequently Asked Questions (FAQ)

Di seguito sono illustrate le principali domande (e risposte) per le problematiche che si sono maggiormente manifestate dal lancio del prodotto.

Domanda – Importazione/Esportazione certificato con Portecle:

Ho ricevuto il certificato SSL MIME Class 2 necessario per l'autenticazione al servizio del Centro Nazionale Trapianti. Seguendo le istruzioni contenute nella guida, utilizzando la soluzione Portecle, sono arrivato all'esportazione della chiave e del certificato nel file PKCS#12. Al comando "Export" è comparso il seguente messaggio di errore:

net.sf.portecle.crypto.CryptoException: Could not save Keystore

One usual suspect for this error is that the unlimited strength jurisdiction policy files for the current JRE may not be installed. Consult the JRE vendor documentation to see if those files are available for it.....

Error Details

net.sf.portecle.crypto.CryptoException: Could not save Keystore

java.io.IOException: exception encrypting data – java.security.invalid Key Exception: illegal key size

Risposta

Il problema è legato alla mancanza delle extension "*Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files*" relative alla istallazione della versione di java. Occorre scaricarle dal fornitore della distribuzione java, es per la versione 8 di Oracle si trovano su:

http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

I due file "local_policy.jar" e "US_export_policy.jar" devono essere copiati, sovrascrivendo eventualmente i precedenti, nella directory "security" dove è installato java (es. Program FIle/Java/Jre/lib/security)

Domanda – Importazione/Esportazione certificato con Openssl

Lancio il comando previsto al par.6.1 al punto 1 ma ottengo il seguente messaggio di errore:

"no certificate matches private key".

Risposta

La chiave presente sul pc nella cartella dove viene eseguito Openssl non corrisponde al certificato restituito dal certificatore. Ciò può dipendere o da una corruzione del file private.key o per un errato file private.key.

Domanda – Importazione/Esportazione certificato con Openssl

Lancio il comando previsto al par.6.1 al punto 1 ma, dopo aver inserito le password, ottengo il seguente messaggio di errore:

"unable to write 'random state'".

Risposta

Occorre lanciare il cmd.exe come amministratore; ciò può essere fatto cliccando con il tasto destro del mouse sul file cmd.exe (presente in \Windows\System32 o \Windows\SysWOW64) e selezionado "Esegui come amministratore".

Domanda – Generazione della chiave privata e della richiesta

Lancio il comando previsto al par. 4.1 punto 1, ma ottengo il seguente errore:

"Unable to load config info from c:/openssl/ssl/openssl.cnf"

Risposta

Copiare il file "openssl.cnf" presente nella cartella principale di openssl e copiarlo nella sottocartella "bin". Aggiungere al comando l'opzione "–config openssl.cnf", es "**openssl req –new –newkey rsa:2048 -nodes -keyout private.key –config openssl.cnf -out public.csr**"

La medesima risoluzione in caso di stesso errore al lancio del comando di cui al par. 6.1 punto 1.