

# Procedura di accreditamento ai servizi di Interoperabilità

25/11/2010



MINISTERO DELL'AMBIENTE  
E DELLA TUTELA DEL TERRITORIO E DEL MARE



## Sommario

|     |   |    |
|-----|---|----|
| -   | Limitazioni di responsabilità e uso del manuale .....             | 3  |
| 1.  | Glossario.....  | 3  |
| 2.  | Presentazione .....   | 4  |
| 2.1 | <i>Note sulla sicurezza</i> .....                                 | 4  |
| 2.2 | <i>Modalità Operative</i> .....                                   | 5  |
| 2.3 | <i>Generazione della coppia di chiavi</i> .....                   | 6  |
| 2.4 | <i>Esempio generazione coppia di chiavi</i> .....                 | 7  |
| 2.5 | <i>Procedura Operativa per la richiesta del certificato</i> ..... | 9  |
| 2.6 | <i>Trasferire la richiesta di certificato al SISTRI</i> .....     | 10 |
| 2.7 | <i>Attendere la risposta dal SISTRI</i> .....                     | 10 |
| 2.8 | <i>Scaricare il certificato</i> .....                             | 11 |
| 3.  | Test funzionalità.....  | 12 |
| 3.1 | <i>Import del file formato PKCS#12</i> .....                      | 13 |
| 3.2 | <i>Import del certificato della Root CA SISTRI</i> .....          | 14 |
| 3.3 | <i>Test di funzionalità sistema sisssl.sistri.it</i> .....        | 15 |
|     | Allegati: Scheda richiesta certificato .....                      | 17 |



## - Limitazioni di responsabilità e uso del manuale

I contenuti della presente pubblicazione sono protetti ai sensi della normativa in tema di opere dell'ingegno. La riproduzione, anche parziale, per ragioni commerciali e non commerciali, è consentita a titolo gratuito purché nella pubblicazione, in qualunque forma realizzata e diffusa, sia citata la fonte "SISTR – Procedura di accreditamento ai servizi di Interoperabilità – Versione del xx.xx.xxxx - www.sistri.it (inserire la data della versione utilizzata)".

SISTR si riserva il diritto di apportare, ogni qualvolta lo ritenga necessario, modifiche ed integrazioni al presente manuale.

## 1. Glossario

In ordine alfabetico

|   |  |
|---|--|
| <b>Affiliazione:</b>  | Processo di accoppiamento tra la Black Box e il dispositivo USB.<br>Dopo questa fase la Black Box accetterà solo tale dispositivo e rifiuterà ogni altro.        |
| <b>Attivazione:</b>   | Processo che rende la Black Box abilitata a gestire il servizio SISTR  |
| <b>Black Box:</b>   | Terminale di bordo utilizzato nel sistema SISTR per la tracciabilità dei trasporti dei rifiuti speciali. E' costituito da una gamma di accessori elettronici.    |
| <b>Call Center:</b>   | Struttura che fornisce supporto telefonico per le installazioni  |
| <b>Dispositivo USB:</b><br>(altrimenti detto <b>TOKEN</b> ) | Elemento di autenticazione e di memorizzazione, da utilizzare in accoppiamento alla Black Box.   |
| <b>SISTR:</b>   | <b>S</b> istema di controllo della <b>T</b> racciabilità dei <b>R</b> ifiuti<br>Iniziativa del Ministero dell'Ambiente e della Tutela del Territorio e del Mare. |
| <b>Unità Centrale</b>                                       | Identifica fisicamente la scatola che contiene tutta l'elettronica.  |
| <b>RA</b>   | Registration Authority   |
| <b>CA</b>   | Certification Authority  |



## 2. Presentazione

Questo servizio è ad uso di tutte le aziende che possiedono un software gestionale compatibile con le interfacce di gestione previste dal SISTRI per il sistema di Interoperabilità.

L'utente potrà accedere dalla zona riservata alla richiesta di firma del certificato, inviando la richiesta alla procedura di "Registration Authority" prevista nel sistema SISTRI e disponibile nel Desktop Profile di ogni singolo utente.

Il SISTRI ha stabilito che l'accesso da parte di applicazioni gestionali di terze parti al sistema di interoperabilità debba avvenire tramite una modalità di autenticazione basata su certificati digitali.

Il protocollo scelto per questo obiettivo è il SSL "Secure Socket Layer" in combinazione con la modalità TLS che prevede un modello di autenticazione forte.

Tutte le procedure che avranno la necessità di interfacciarsi con il sistema SISTRI dovranno farlo attraverso la modalità di mutua autenticazione tra applicazioni (Application-TO-Application).

Il meccanismo di autenticazione dovrà avvenire mediante l'uso di certificato x509.v3 rilasciati dalla PKI interna al SISTRI.

I certificati saranno rilasciati dalla PKI del sistema SISTRI secondo le modalità standard previste e descritte in questo documento.

### 2.1 Note sulla sicurezza

La sicurezza della comunicazione tra il gestionale e il sistema di interoperabilità viene garantita dalle modalità con cui si custodiscono queste informazioni che devono rispettare i seguenti requisiti minimi:

- 1) La chiave privata deve essere protetta con una passphrase realizzata in modo sicuro  
(La passphrase deve essere composta da lettere maiuscole, minuscole, numeri e segni d'interpunzione);
- 2) La passphrase deve essere custodita adeguatamente;
- 3) Tutti i file dovranno essere rimossi dal sistema dopo averne effettuato una copia sicura;
- 4) Il certificato in formato "p12" deve essere utilizzato prestando la massima attenzione;
- 5) Deve essere attivato un processo di gestione della sicurezza sui sistemi di interoperabilità.



## 2.2 Modalità Operative

### A cosa serve il certificato

Per poter richiedere l'accesso ai servizi d'interoperabilità, gli utenti iscritti al SISTRI possono accedere alla procedura di richiesta dal Portale riservato. In particolare per accedere al Portale riservato gli utenti dovranno:

1. inserire il dispositivo USB nel proprio computer
2. eseguire l'applicazione
3. accedere al sistema inserendo le proprie credenziali (PIN, userid e password)
4. cliccare sulla voce di menù "interoperabilità"

Per richiedere il certificato, l'utente deve operare in quattro fasi distinte:

- ◇ La prima prevede il download del "Modulo di richiesta di autorizzazione all'utilizzo dei servizi di interoperabilità del sistri per le attività di predisposizione del sistema gestionale".
- ◇ La seconda fase prevede la generazione della CSR (Certificate Signing Request) secondo quanto previsto nel presente documento.
- ◇ La terza fase sarà quella di inserire la richiesta di certificato preparata dall'azienda all'interno della RA (Registration Authority) del SISTRI per chiederne l'approvazione e la firma della richiesta.
- ◇ La quarta fase consentirà di ottenere il certificato di firma emesso dalla CA (Certification Authority) SISTRI.

Nel seguente documento sono descritte le operazioni per richiedere il certificato.

Riportiamo un elenco delle azioni necessarie da eseguire:

#### **Fase 1)**

1. Scaricare il "Modulo di richiesta di autorizzazione all'utilizzo dei servizi di interoperabilità del sistri per le attività di predisposizione del sistema gestionale" dal Portale SISTRI nella Sezione Documenti – Modulistica.
2. Compilare il suddetto Modulo in tutte le sue parti.

#### **Fase 2)**

1. Effettuare la generazione della coppia di chiavi nel proprio ambiente, (in caso di difficoltà seguire l'esempio nell'allegato di questo documento).
2. Eseguire la richiesta di certificato sotto forma di file formato "PEM (PKCS7)".
3. Compilare la scheda riportata al paragrafo 0 in allegato.

#### **Fase 3)**

1. Collegarsi al sito SISTRI (<https://secure.sistri.it>) e cliccare sul link predisposto.
2. Trasferire la richiesta di certificato al SISTRI.
3. Attendere la risposta dal centro SISTRI.



#### **Fase 4)**

1. Effettuare nuovamente l'accesso al sito SISTRI (<https://secure.sistri.it>) e cliccare sul link predisposto RA (Registration Authority).
2. Creare la richiesta di certificato.
3. Scaricare il certificato nel proprio sistema.

Dopo aver scaricato il certificato dal sistema SISTRI, questo potrà essere caricato nei propri sistemi gestionali con i quali sarà possibile realizzare l'accesso al sistema di interoperabilità .

Nel presente documento, sono descritte alcune modalità con cui è possibile verificare il funzionamento del certificato rilasciato al di fuori dei sistemi mediante l'utilizzo di Firefox.

Questa procedura potrà essere sostituita con qualsiasi altra soluzione tecnologica che si riterrà opportuna.

### **2.3 Generazione della coppia di chiavi**

Per la generazione della coppia di chiavi, [pubblica e privata] è possibile utilizzare numerosi strumenti. Nel nostro esempio proponiamo l'utilizzo del software OpenSSL, soluzione affidabile selezionata da DigitPA (ex CNIPA), su sistema operativo Linux.

Non escludiamo la possibilità che possano essere utilizzate altre soluzioni ritenute affidabili su sistemi operativi alternativi a Linux.

La tecnologia utilizzata è chiamata "*Public Key Cryptography*". La tecnologia utilizza chiavi pubbliche e private. La chiave privata, generata tramite lo strumento prescelto, rimarrà nel server senza mai essere resa pubblica.

L'integrità della chiave privata dipende strettamente dalla riservatezza con cui viene trattata.

L'operazione di CSR, (Certificate Signing Request) [richiesta di firma del certificato digitale] consiste nella generazione di una chiave pubblica sul server personale che contiene informazioni specifiche dell'utente [organizzazione, sito etc.]. La chiave deve essere inviata tramite una procedura definita alla CA del SISTRI per la firma.



## 2.4 Esempio generazione coppia di chiavi

Generare una coppia di chiavi con OpenSSL. Collegarsi ad un sistema operativo Linux che abbia installato Open SSL. Posizionarsi nella directory in cui si vuole generare la coppia di chiavi:

Eeguire il comando:

```
openssl req -new -newkey rsa:2048-nodes -keyout private.key -out public.csr
```

Opensll porrà una serie di domande a cui si dovrà rispondere [le risposte sono riportate in **grassetto**]. Assicurarsi che le informazioni inserite siano corrette.

```
Using configuration from /etc/ssl/openssl.cnf
```

```
Generating a 1024 bit RSA private key
```

```
.++++++
```

```
.....++++++
```

```
writing new private key to 'private.key'
```

```
-----
```

```
You are about to be asked to enter information that will be  
incorporated
```

```
into your certificate request.
```

```
what you are about to enter is what is called a Distinguished Name or  
a ID.
```

```
There are a quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
```

```
-----
```

```
Country Name (2 letter code) [AU]:IT
```

```
State or province Name (full name) [Some-State]:Milano
```

```
Locality Name (eg, city) []:Milano
```

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]: acme spa
```

```
Organization Unit Name (eg, section) []:Information Technology
```

```
Common Name (eg, YOUR name) []:www.acme.com
```

```
Email Address []:info@acme.com
```

```
Please enter the following 'extra' attributes  
to be sent with your certificate request
```

```
A challenge password []:acmepassword
```

```
An optional company name []:
```

**NOTA:** Nell'esempio la chiave privata è stata chiamata "private.key" e la chiave pubblica (CSR) "public.csr"



Una volta generato il CSR (e sicuri che i dati inseriti siano corretti) aprire il file con un editor di testo per vederne i contenuti (“notepad” se operate con il sistema operativo Windows o “vi” se operate con il sistema operativo Linux).

```
-----BEGIN NEW CERTIFICATE REQUEST-----  
MIIBJTCB0AIBADBtMQswCQYDVQQGEwJVUzEQMA4GA1UEChs4lBMHQ  
XJpem9uYTENA1UEBxMETWVzYTEfMBOGA1UEChMWTWVs3XbnzYSBDb  
  
.....  
  
DLTAutULTsZKDcLAgEDoAAwDQYJKoZIhvcNAQEEBQADQQAjIFpTLg  
fmBVhc9Sqaip5SFNXtzAmhYzvJkt5JJ4X2r7VJYG3J0vauJ5VkjXz  
9aevJ8dZX37ir3P4XpZ+NFxK1R=  
-----END NEW CERTIFICATE REQUEST-----
```



## 2.5 Procedura Operativa per la richiesta del certificato

All'interno del Desktop di portale riservato ad ogni utente del SISTRI, è presente un link per l'accesso alla procedura di richiesta del certificato di interoperabilità.

Di seguito riportiamo il form con il quale sarà possibile effettuare la richiesta di certificato.

Sistema di controllo  
della Tracciabilità dei Rifiuti **SISTRI**

Per richiedere il certificato completate con le informazioni mancanti in questi form

| DATI AZIENDA             |                        |                           |
|--------------------------|------------------------|---------------------------|
| Codice Pratica: WEB_AP_1 | Ragione Sociale: FARMA | Cod Fiscale Azienda: null |

| DATI DEL LEGALE RAPPRESENTANTE<br>Tutti i campi sono obbligatori compreso e-mail e recapito telefonico |                         |  |
|--|-------------------------|--|
| Cognome: RO  | Nome: BR                | Cod. Fisc:   |
| Luogo Nascita:   | Provincia Nascita:      | Stato:   |
| Data di nascita: 10  | Cittadinanza:           | Sesso: M <input type="radio"/> F <input type="radio"/> |
| Indirizzo:   | Nr:                     | CAP:   |
| Comune di Residenza:   | Provincia di Residenza: |  |
| Indirizzo email:   | Recapito telefonico:    |  |

| DOCUMENTO IDENTITA' DEL RICHIEDENTE<br>Tutti i campi sono obbligatori |                       |         |
|---|-----------------------|---------|
| Tipo: Carta d'identità  | Autorità di rilascio: |         |
| Data rilascio: 10   | Valida sino al: 10    | Numero: |

| SCOPO D'UTILIZZO |                 |          |
|------------------|-----------------|----------|
| Applicazione:    | Modalità d'uso: | Formato: |

| TIPO CERTIFICATO  |  |
|---|--|
| X509: PEM <input type="radio"/> DER <input type="radio"/> | Durata: <input type="radio"/> 1 anno <input type="radio"/> 2 anni <input type="radio"/> 3 anni <input type="radio"/> 4 anni <input type="radio"/> 5 anni |

Alcuni campi vengono riempiti in automatico dalla procedura, mentre gli altri debbono essere inseriti dall'utente.

Una volta che l'utente ha completato la compilazione del modulo, la procedura genera un file PDF che l'utente deve scaricare, stampare e far firmare dal legale rappresentante. Il documento firmato deve essere quindi acquisito (in formato PDF) così come un documento del legale rappresentante in corso di validità.



## 2.6 Trasferire la richiesta di certificato al SISTRI

Una volta completata la procedura di creazione della coppia di chiavi, inseriti correttamente i dati nell'applicazione e compilata la scheda tecnica *Scheda richiesta certificato [Allegato]*, il passo successivo consiste nell'inviare all'attenzione del centro servizi SISTRI tutto il materiale necessario per il completamento della richiesta di certificazione.

L'utente dovrà collegarsi nuovamente all'applicazione e fare l'upload dei 3 PDF (Modulo di richiesta di autorizzazione all'utilizzo dei servizi di interoperabilità del sistri per le attività di predisposizione del sistema gestionale, Scheda richiesta certificato firmata e documento in corso di validità del legale rappresentante) congiuntamente alla CSR generata.

Tale procedura consente agli utenti di compilare i file richiesti in più riprese. Soltanto quando sarà stata inserita tutta la documentazione necessaria, si potrà procedere all'invio della richiesta di certificato come mostrato nell'immagine seguente.



|  |  |
|--|--|
| Pdf contenente la <b>richiesta di autorizzazione all'utilizzo dell'interoperabilità (modulo vuoto)</b> | <input type="text"/> <input type="button" value="Sfoglia..."/> |
| Pdf contenente la Carta di Identità del <b>Legale Rappresentante</b>                                   | <input type="text"/> <input type="button" value="Sfoglia..."/> |
| Pdf contenente il modulo di richiesta <b>firmato</b>   | <input type="text"/> <input type="button" value="Sfoglia..."/> |
| File binario contenente la richiesta di certificato ( <b>CSR</b> )                                     | <input type="text"/> <input type="button" value="Sfoglia..."/> |

## 2.7 Attendere la risposta dal SISTRI

Il centro servizi SISTRI, aprirà una procedura di verifica dei documenti e procederà al rilascio dei certificati richiesti, in continua relazione con l'utente.



## 2.8 Scaricare il certificato

Una volta che il certificato sarà rilasciato, l'utente potrà scaricarlo dalla stessa pagina, come mostrato nell'immagine seguente.

Nella stessa pagina sarà presente anche il certificato di chiave pubblica della CA del SISTRI che deve essere scaricato congiuntamente.



Il certificato va scaricato e conservato nella zona del disco dove sono state archiviate le chiavi precedentemente generate.

**N.B.** Qualora le chiavi andassero perse il certificato non è più valido e la procedura va eseguita nuovamente dall'inizio.



### 3. Test funzionalità

Il test di funzionalità proposto prevede l'utilizzo Mozilla Firefox per verificare il certificato appena scaricato dopo la firma da parte della CA del SISTRI.

Tale funzionalità è utilizzabile dagli utenti in maniera opzionale, al fine di poter verificare in autonomia il corretto funzionamento del sistema. Si evidenzia che, per motivi di sicurezza, al termine della verifica, il certificato va rimosso dal 'key store' di Mozilla.

Per essere importato all'interno di Mozilla Firefox, il certificato deve avere un formato PKCS#12.

Questo formato prevede che le chiavi ed il certificato nel formato PKCS#7, fornito dalla PKI SISTRI siano contenute all'interno di un file unico.

Nel capitolo dedicato alla generazione delle chiavi ed alla richiesta di certificato sono stati generati i seguenti file:

- 1) 'private.key' (contiene la chiave privata);
- 2) 'public.csr' (contiene la richiesta PKCS#10 inviata alla CA SISTRI);
- 3) 'file\_csr\_firmata\_da\_SISTRI.cer' (File con certificato rilasciato dalla CA SISTRI).

Di seguito le istruzioni necessarie per realizzare il file nel formato PKCS#12.

#### Convert P7 to P12

Per ottenere il formato p12, che racchiude entrambe le chiavi e il certificato di firma, eseguire il seguente comando:

```
Senza l'utilizzo del certificato di RootCA SISTRI
```

```
openssl pkcs12 -export -in [file_csr_firmata_da_SISTRI].cer -inkey  
privateKey.key -out certificate.p12
```

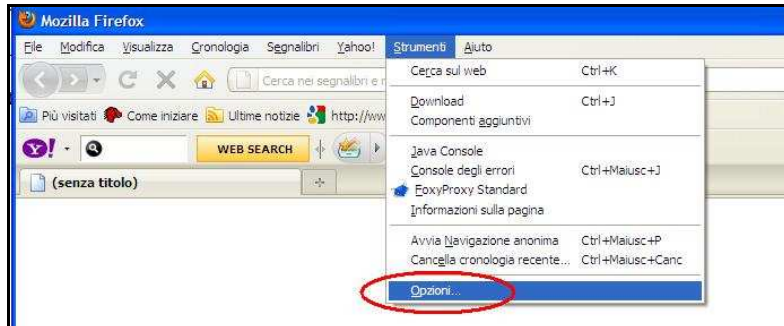
```
Con l'uso del certificato di RootCA SISTRI
```

```
openssl pkcs12 -export -in [file_csr_firmata_da_SISTRI].cer -inkey  
privateKey.key -out certificate.p12 -certfile [file_Root_CA_di_SISTRI].cer
```

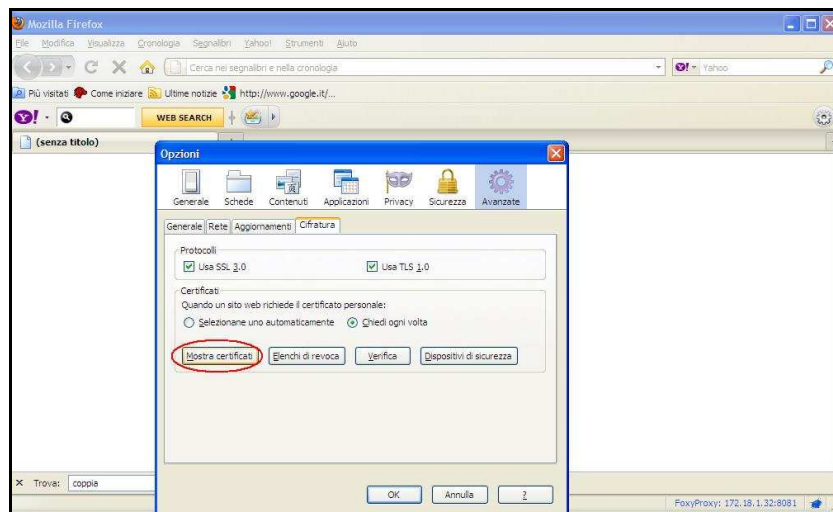
**N.B.** Tutti i file utilizzati come per queste operazioni devono essere rimossi e conservati in modo sicuro.

### 3.1 Import del file formato PKCS#12

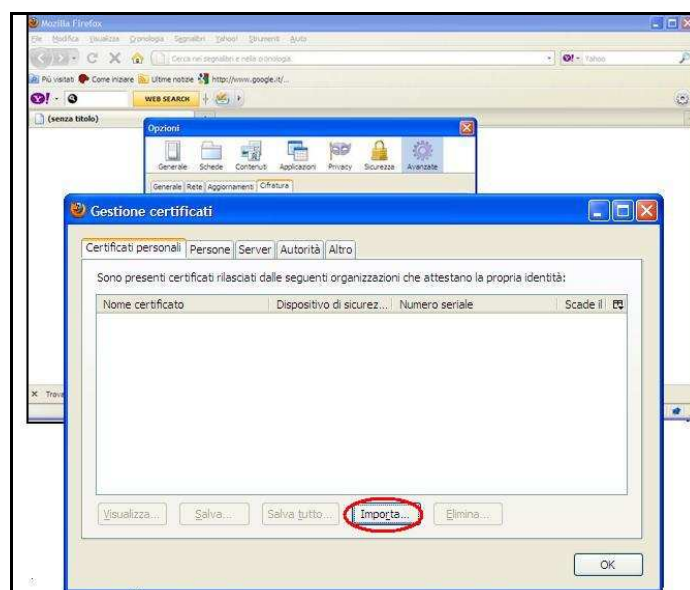
Il test che segue aiuta a verificare che il sistema di chiavi sia stato realizzato correttamente. Per procedere con il test, aprire “Mozilla Firefox”. Nella colonna degli strumenti, cliccare sulle “opzioni” .



All’apertura della finestra opzioni, cliccare sulle funzioni avanzate e sul bottone “mostra certificati” :

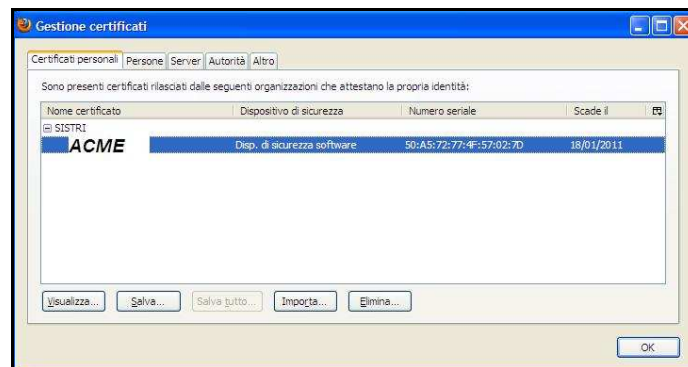


All’apertura della finestra di gestione dei certificati, nella sezione “certificati personali”, selezionare il bottone “Importa”





Selezionando il file con estensione “.p12” navigando nella directory in cui è stato salvato il certificato, digitare la password inserita in sede di creazione del certificato. La gestione dei certificati fornirà in output la seguente schermata :

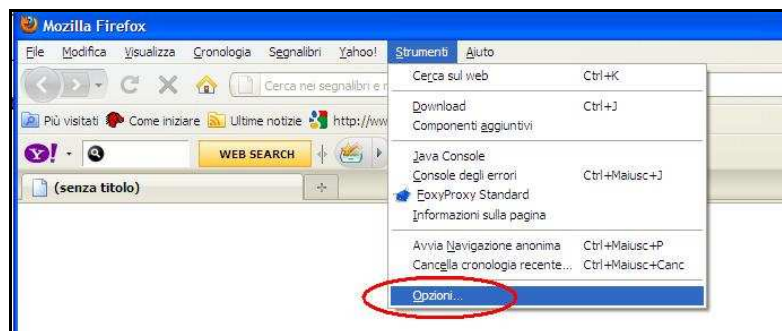


A questo punto il certificato è creato con successo.

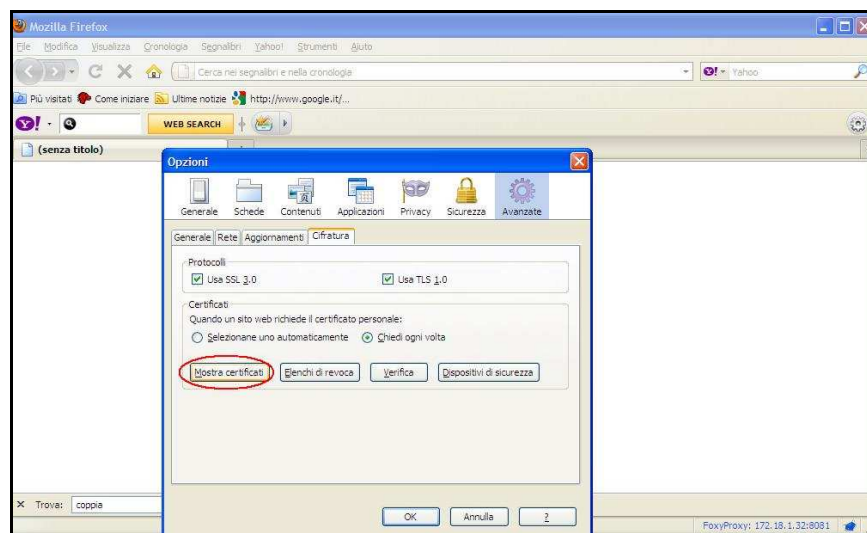
### 3.2 Import del certificato della Root CA SISTRI

Alla risposta di SISTRI, per la consegna della firma del certificato, verrà rilasciato il certificato SISTRI “\*.crt”.

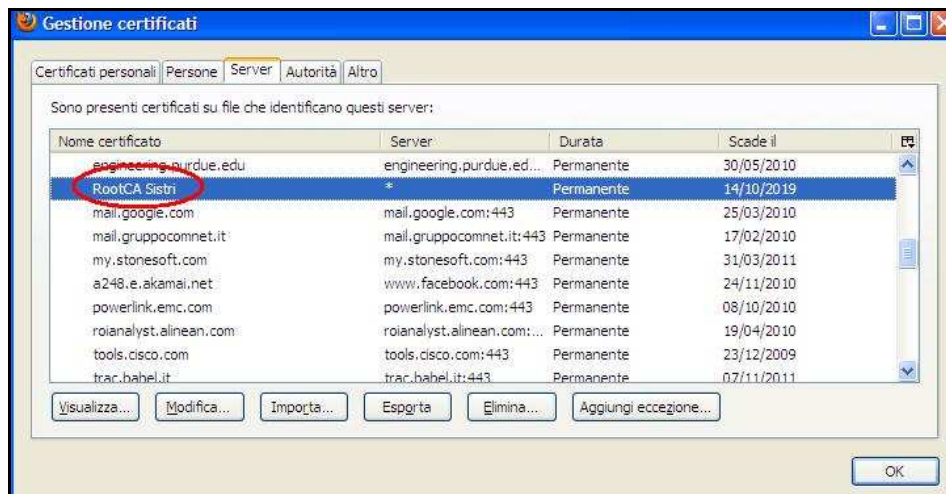
Se si desidera importare il certificato occorre seguire la seguente procedura. Per procedere con il test, aprire “Mozilla Firefox”. Nella colonna degli strumenti, cliccare sulle “opzioni” .



All’apertura della finestra opzioni, cliccare sulle funzioni avanzate e sul bottone “mostra certificati” :



All'apertura della finestra di gestione dei certificati, nella sezione "server", selezionare il bottone "Importa". Navigare nella directory in cui è posizionata il certificato di chiave pubblica SISTRI (RootCASistri.crt).



Il certificato di interoperabilità è stato installato con successo.

Al termine dell'import dei certificati sarà possibile effettuare dei test di connettività che possono essere svolti con semplicità mediante l'utilizzo del browser Mozilla Firefox utilizzato per installare i certificati stessi come visto nei paragrafi precedenti.

### **3.3 Test di funzionalità sistema sisssl.sistri.it**

Dopo aver importato il certificato all'interno di Mozilla Firefox collegarsi al sito SISTRI dove è disponibile l'interrogazione del servizio WSDL. Si tratta di una risorsa esposta all'esterno che si interfaccia con i servizi di interoperabilità interni al SISTRI.

La URL di riferimento è:

<https://sisssl.sistri.it/SIS/services/SIS?wsdl>



Il risultato ottenuto dall'interrogazione del servizio è il seguente:

```
- <wsdl:definitions name="SIS_WSDL" targetNamespace="http://www.sistri.it/SIS_WSDL/">
- <wsdl:types>
- <xsd:schema targetNamespace="http://www.sistri.it/SIS_WSDL/">
- <xsd:complexType name="SISException">
- <xsd:sequence>
  <xsd:element name="errorCode" nillable="false" type="xsd:string"/> </xsd:element>
  <xsd:element name="errorMessage" nillable="true" type="xsd:string"/>
  </xsd:sequence>
</xsd:complexType>
- <xsd:complexType name="Catalogo">
- <xsd:sequence>
  <xsd:element name="idCatalogo" type="xsd:string"/>
  <xsd:element minOccurs="0" name="description" nillable="true" type="xsd:string"/>
  </xsd:sequence>
</xsd:complexType>
- <xsd:complexType name="DescrittoreCatalogo">
- <xsd:sequence>
  <xsd:element name="catalogo" type="xsd:string"/> </xsd:element>
  <xsd:element name="versione" nillable="true" type="xsd:string"/>
  <xsd:element name="descrizione" nillable="true" type="xsd:string"/>
  </xsd:sequence>
</xsd:complexType>
- <xsd:element name="GetElencoCataloghiRequest">
- <xsd:complexType>
- <xsd:sequence>
  <xsd:element name="identity" type="xsd:string"/> </xsd:element>
  </xsd:sequence>
</xsd:complexType>
</xsd:element>
- <xsd:element name="GetElencoCataloghiResponse">
- <xsd:complexType>
- <xsd:sequence>
  <xsd:element minOccurs="0" maxOccurs="unbounded" name="out" nillable="true" type="tns:DescrittoreCatalogo"/>
  </xsd:sequence>
</xsd:complexType>
</xsd:element>
<xsd:element name="GetElencoCataloghi_fault" type="tns:SISException"/>
</xsd:element name="GetVersioneCatalogoRequest">
```



## Allegato: Scheda richiesta certificato

Per la richiesta del CSR, compilare la seguente scheda fornendo i documenti richiesti

| <b>DATI DEL RICHIEDENTE</b>   |                         |  |
|---|-------------------------|--|
| Tutti i campi sono obbligatori compreso e-mail e recapito telefonico  |                         |  |
| Codice Pratica:   | Ragione Sociale:        | Cod Fiscale Azienda:   |
| Cognome:  | Nome:                   | Cod. Fisc:   |
| Luogo Nascita:  | Provincia Nascita       | Stato:   |
| Data di Nascita:  | Cittadinanza:           | Sesso: M <input type="checkbox"/> F <input type="checkbox"/> |
| Indirizzo residenza::   | Nr:                     | CAP:   |
| Comune di Residenza:  | Provincia di residenza: |  |
| Indirizzo e-mail:   | Recapito Telefonico:    |  |
| <b>DOCUMENTO IDENTITÀ DEL RICHIEDENTE</b>   |                         |  |
| Tutti i campi sono obbligatori  |                         |  |
| Tipo:   | Autorità di rilascio:   |  |
| Data rilascio:  | Valida sino al:         | Numero:  |
| N.B.: Ai fini di una valida identificazione del richiedente possono essere accettati solo i seguenti documenti d'identità, in corso di validità: <ul style="list-style-type: none"><li>• Carta d'identità;</li><li>• Passaporto;</li><li>• Patente auto;</li><li>• Tesserino di riconoscimento del personale delle amministrazioni statali.</li></ul> |                         |  |
| <b>DICHIARAZIONE SOSTITUTIVA CODICE FISCALE</b>   |                         |  |
| Il sottoscritto richiedente, consapevole che chiunque rilascia dichiarazioni mendaci è punito ai sensi del codice penale e delle leggi speciali in materia, ai sensi e per gli effetti di cui art.46 del D.P.R. n. 445/2000   |                         |  |
| di essere in possesso del seguente Codice Fiscale _____   |                         |  |
| <b>SCOPO D'UTILIZZO</b>   |                         |  |
| Applicazione:   |                         |  |
| Modalità d'uso:   |                         |  |
| Formato:  |                         |  |
| <b>TIPO CERTIFICATO</b>   |                         |  |
| X509: PEM <input type="checkbox"/> DER <input type="checkbox"/>   |                         |  |