

Procedura di accreditamento ai servizi di Interoperabilità

10/12/2010



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
3. Procedura Operativa	5
3.1. <i>Richiesta del certificato</i>	6
3.2. <i>Trasferimento della richiesta di certificato al SISTRI</i>	7
3.3. <i>Attesa della risposta dal SISTRI</i>	8
3.4. <i>Rilascio del certificato</i>	12
4. Test funzionalità.....	13
4.1. <i>Import del file formato PKCS#12</i>	14
4.2. <i>Import del certificato della Root CA SISTRI</i>	15
4.3. <i>Test di funzionalità sistema sisssl.sistri.it</i>	16
Allegati	18
A. <i>Modulo per la richiesta del certificato</i>	18
B. <i>Modulo per la richiesta di autorizzazione all'utilizzo dei servizi di interoperabilità</i>	19
C. <i>Procedura di generazione CSR</i>	20



- 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 "SISTRI – Procedura di accreditamento ai servizi di Interoperabilità – Versione del xx.xx.xxxx - www.sistri.it (inserire la data della versione utilizzata)".

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

1. Glossario

In ordine alfabetico

Affiliazione:	Processo di accoppiamento tra la Black Box e il dispositivo USB. Dopo questa fase la Black Box accetterà solo tale dispositivo e rifiuterà ogni altro.
Attivazione:	Processo che rende la Black Box abilitata a gestire il servizio SISTRI
Black Box:	Terminale di bordo utilizzato nel sistema SISTRI per la tracciabilità dei trasporti dei rifiuti speciali. E' costituito da una gamma di accessori elettronici.
Call Center:	Struttura che fornisce supporto telefonico per le installazioni
Dispositivo USB: (altrimenti detto TOKEN)	Elemento di autenticazione e di memorizzazione, da utilizzare in accoppiamento alla Black Box.
SISTRI:	SIST ema di controllo della Tr acciabilità dei R ifiuti Iniziativa del Ministero dell'Ambiente e della Tutela del Territorio e del Mare.
Unità Centrale	Identifica fisicamente la scatola che contiene tutta l'elettronica.
RA	Registration Authority
CA	Certification Authority



2. Presentazione

Il presente documento si propone quale strumento di supporto alla richiesta di accesso ai servizi d'interoperabilità 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.



3. Procedura Operativa

Per richiedere il certificato l'utente deve provvedere, nel proprio ambiente informatico, alla generazione della CSR (Certificate Sign Request) secondo quanto descritto nell'*Allegato C - Procedura di generazione CSR*.

Per poter richiedere l'accesso ai servizi d'interoperabilità, gli utenti iscritti al SISTRI devono accedere alla procedura di richiesta autorizzazione sul Portale riservato.

In particolare per accedere al Portale riservato gli utenti dovranno:

1. inserire il dispositivo USB nel proprio computer;
2. eseguire l'applicazione residente sul dispositivo e cliccare "Accedi al sistema";
3. inserire le proprie credenziali (PIN, user-id e password) seguendo le istruzioni sul portale;
4. cliccare sulla voce di menù "Interoperabilità";
5. Il portale visualizza all'utente una maschera per l'inserimento dei dati;
6. Inserire i dati richiesti;
7. selezionare e scaricare i moduli pdf generati dall'applicazione;
8. Stampare e firmare entrambi i moduli;
9. effettuare la scansione dei moduli firmati in formato pdf;
10. effettuare l'upload della CSR e dei moduli in formato pdf nel portale utilizzando l'applicazione interoperabilità in uso.

Le maschere di dettaglio dell'applicazione sono riportate nelle successive sezioni.

L'utente può eseguire i passi descritti precedentemente anche in modalità asincrona.

L'utente potrà collegarsi in più fasi per verificare che il certificato sia stato rilasciato ed effettuare il download per utilizzarlo.

L'utente sarà comunque avvisato dal sistema che il certificato potrà essere scaricato. L'avviso avverrà tramite un messaggio di posta elettronica all'indirizzo mail indicato in fase di inserimento dati richiesti dall'applicazione.

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.



3.1. 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 generato e mostrato dall'applicazione.

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

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

DATI AZIENDA		
Codice Pratica	Ragione Sociale:	Cod Fiscale Azienda: null

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

DOCUMENTO IDENTITA' DEL RICHIEDENTE		
Tutti i campi sono obbligatori		
Tipo: Carta d'identità	Autorità di rilascio:	
Data rilascio:	Valida sino al:	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 devono essere inseriti dall'utente.

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



3.2. Trasferimento della 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.



Stampate i 2 PDF seguenti, fateli firmare dal rappresentante legale e caricateli nell'apposita pagina insieme al PDF della carta di identità del legale rappresentante

Dichiarazione	Autorizzazione

Correggi i dati

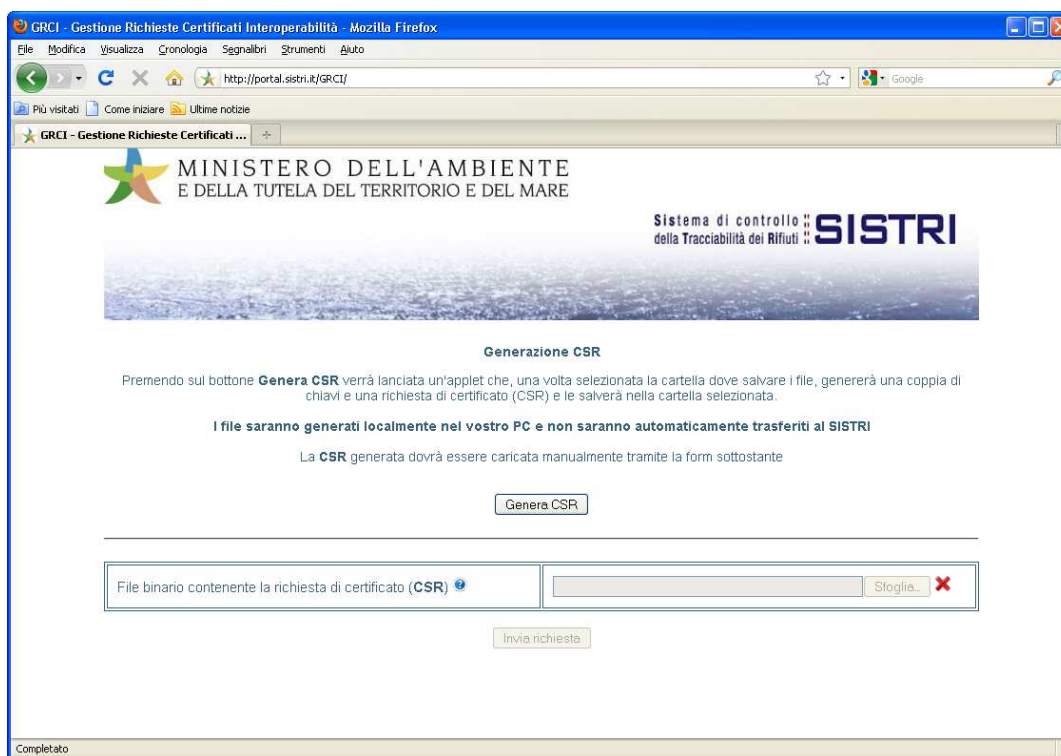
Pdf contenente la richiesta di autorizzazione all'utilizzo dell'interoperabilità	<input type="text"/> Sfoglia... ✖
Pdf contenente la Carta di Identità del Legale Rappresentante	<input type="text"/> Sfoglia... ✖
Pdf contenente il modulo di richiesta firmato	<input type="text"/> Sfoglia... ✖

Invia richiesta

3.3. Attesa della risposta dal SISTRI

Il centro servizi SISTRI aprirà una procedura di verifica dei documenti e procederà al rilascio dei certificati richiesti.

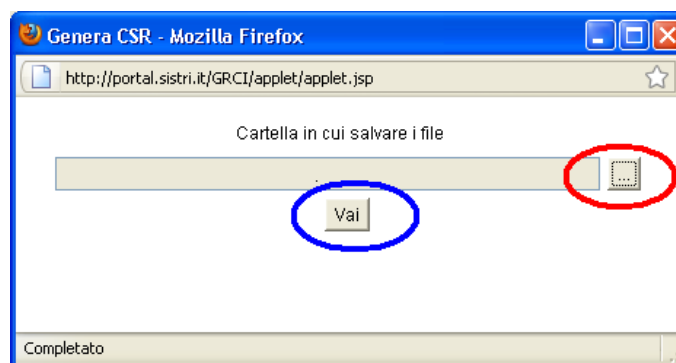
Per procedere con la fase di rilascio del certificato ed il successivo prelievo dal centro, si dovrà rientrare nella parte relativa all'interoperabilità. Una volta cliccato sul link interoperabilità apparirà la figura seguente:



In questa sezione della procedura di interoperabilità il sistema prevede lo svolgimento di tre fasi distinte:

1. la prima prevede la generazione della CSR;
2. la seconda prevede l'inoltro della richiesta di certificato al centro;
3. la terza si conclude con la firma della richiesta ed il rilascio del certificato.

Per procedere con la generazione della richiesta del certificato si dovrà cliccare sul bottone genera CSR, la procedura in automatico presenterà la seguente maschera:

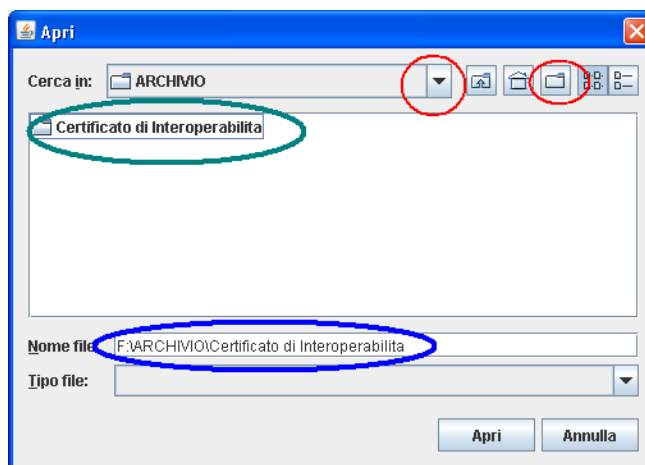


Questa fase prevede che l'utente utilizzi una zona del disco del proprio computer.

Su questa maschera:

Se si conosce già la zona del disco da utilizzare per il salvataggio dei file con la coppia di chiavi e la CSR basterà scriverla (es. *C:\Nomecartella*). Successivamente si potrà cliccare sul bottone (Vai).

Se non si conosce la cartella all'interno della quale salvare i file occorrerà selezionare con il mouse, sul simbolo cerchiato in rosso. In questo caso apparirà la maschera seguente:



La figura sopra riportata, mostra la finestra di navigazione dove (mediante l'utilizzo dei bottoni cerchiati in rosso) sarà possibile selezionare o creare la cartella (nell'esempio cerchiata in verde) all'interno della quale sarà possibile effettuare la generazione della coppia di chiavi e la richiesta del certificato.

Se si conosce già la cartella sarà possibile digitare direttamente il percorso (nell'esempio cerchiato in blu).

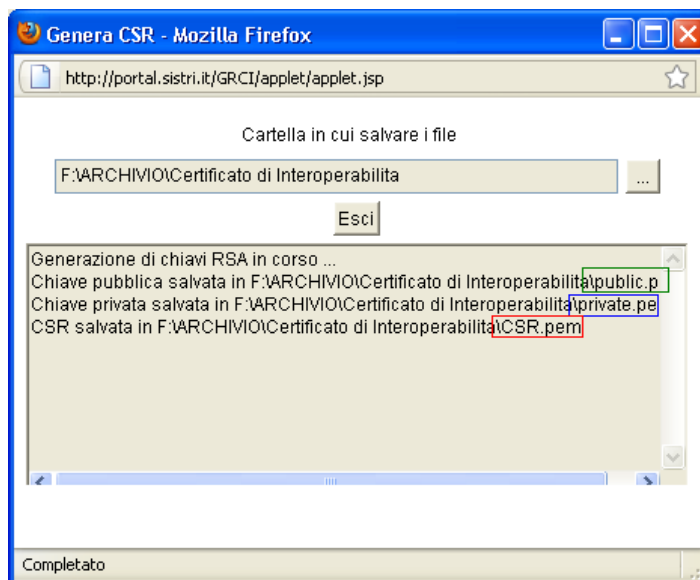
N.B. nel presente esempio i file sono stati archiviati sul dispositivo USB ma potranno essere salvati e generati su una zona qualsiasi del disco del vostro computer. Sarà importante ricordarsi dove questi sono stati generati.

N.B. Queste informazioni devono essere conservate in luogo sicuro e protetto. La loro perdita comporta la richiesta di revoca del certificato al centro SISTRI e la emissione di un nuovo certificato.

Al termine della selezione appare nuovamente la maschera seguente con il nome della Cartella selezionata nel campo “Cartella in cui salvare i file”.



Per procedere con la generazione della coppia di chiavi e della richiesta di certificato occorrerà cliccare sul bottone “Vai”. La maschera seguente riporta il risultato dell’esecuzione del comando “Vai”.



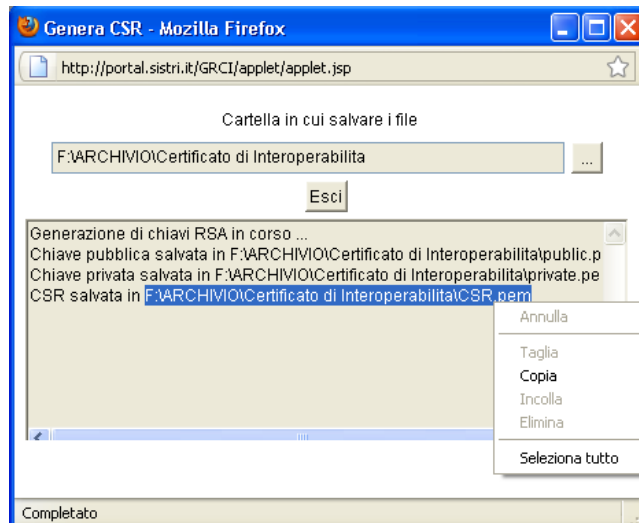
In questo step vengono generati tre file fondamentali:

1. public.pem
2. private.pem
3. CSR.pem

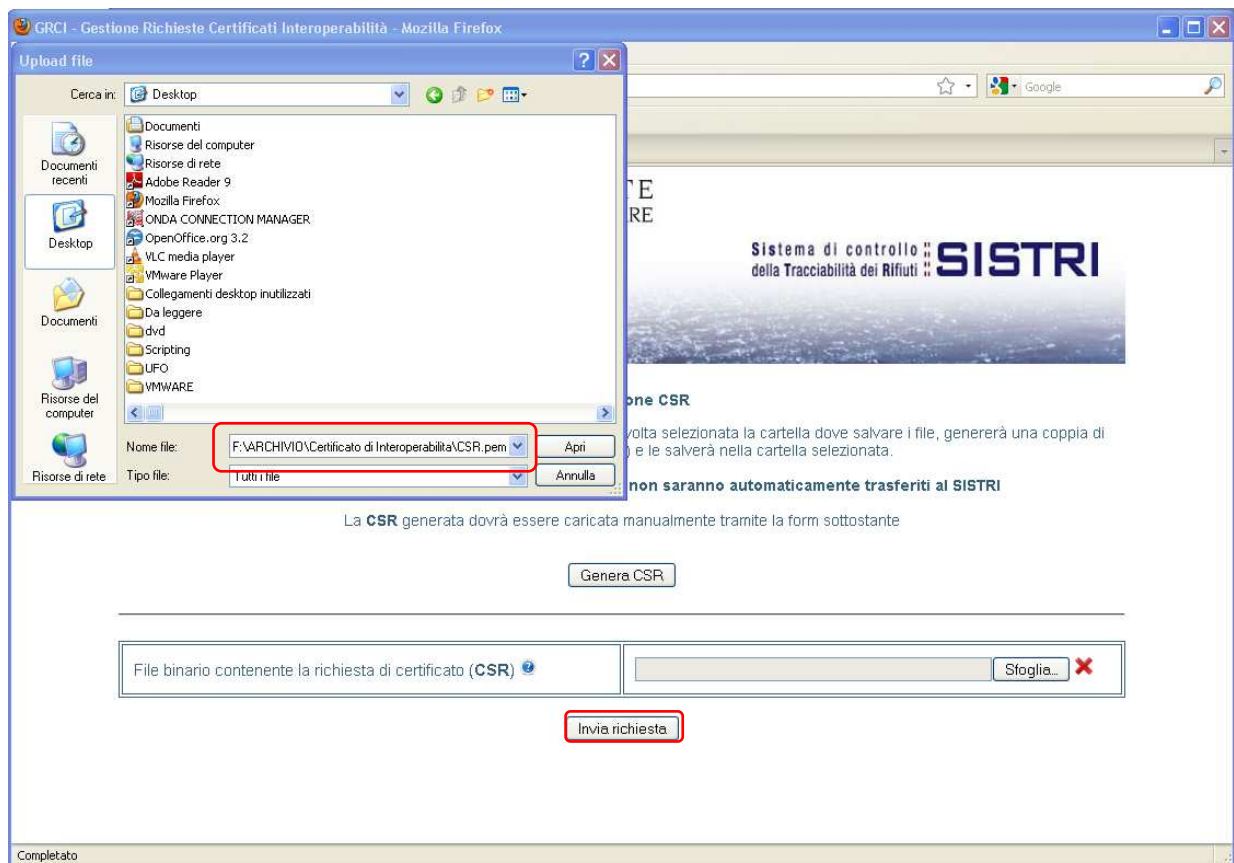
Il file necessario per ottenere la firma da parte del sistema SISTRI è il file “CSR.pem” che andrà caricato al centro SISTRI per il rilascio automatico della firma del certificato.



Per caricare il certificato al centro SISTRI occorre eseguire i seguenti passi:



Si suggerisce di evidenziare il nome del file dalla form mostrata sopra e di copiarlo all'interno del campo visibile nella figura seguente:



Effettuati questi passaggi, che permettono di indicare dove si trova all'interno del Vostro sistema il file "CSR.pem" occorrerà selezionare il bottone "Invia richiesta" ed attendere che la procedura rilasci la firma del certificato.

N.B. Questa firma può essere associata soltanto ai file precedentemente generati e in nessun caso potrà essere scambiata con altri file.



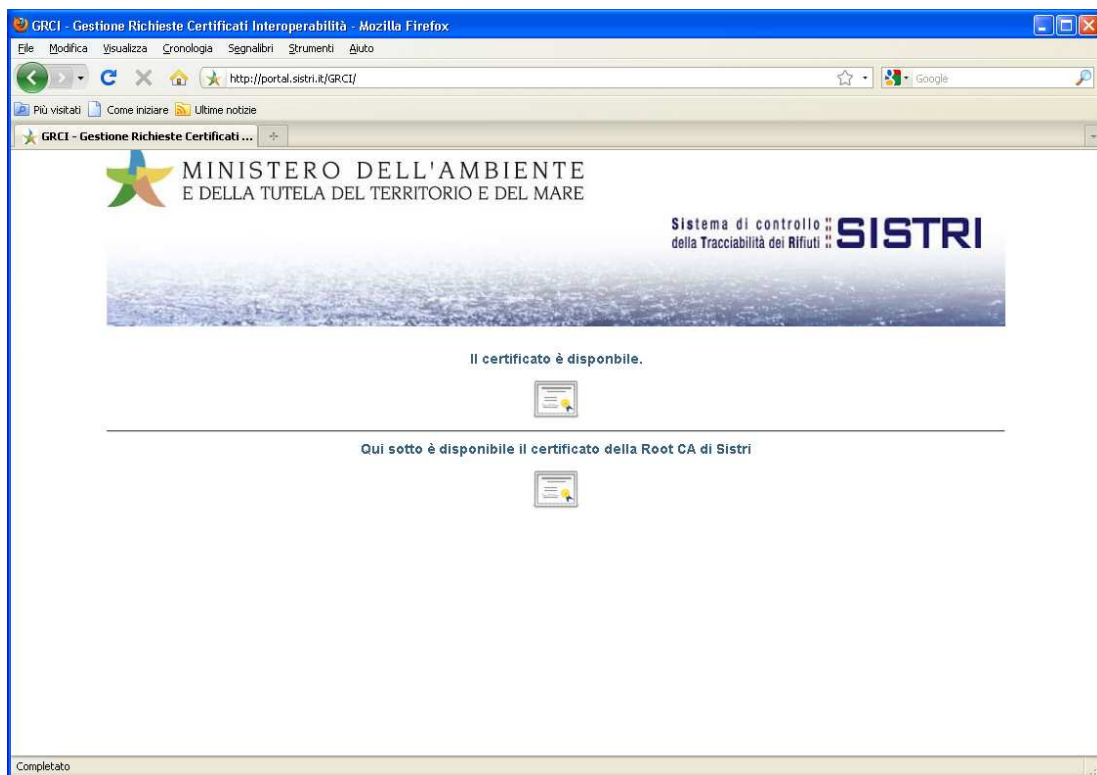
La figura seguente mostra un dettaglio della fase descritta sopra:

File binario contenente la richiesta di certificato (CSR)

F:\ARCHIVIO\Certificato di Interoperabilita\CSR.pem

3.4. Rilascio del 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 deve essere nuovamente eseguita dall'inizio.



4. 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.

Assemblare i file nel formato PKCS#12

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
```

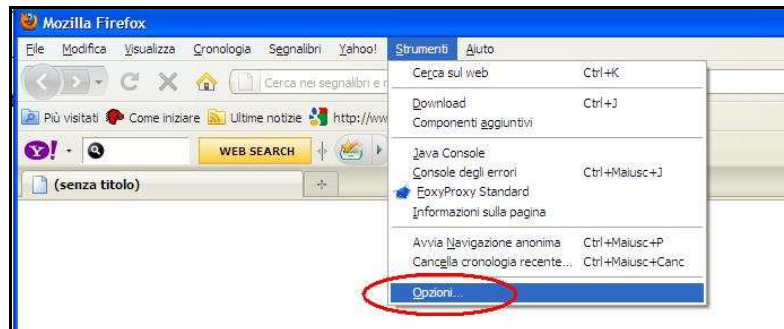
```
Con l'uso del certificato di RootCA SISTRI
```

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

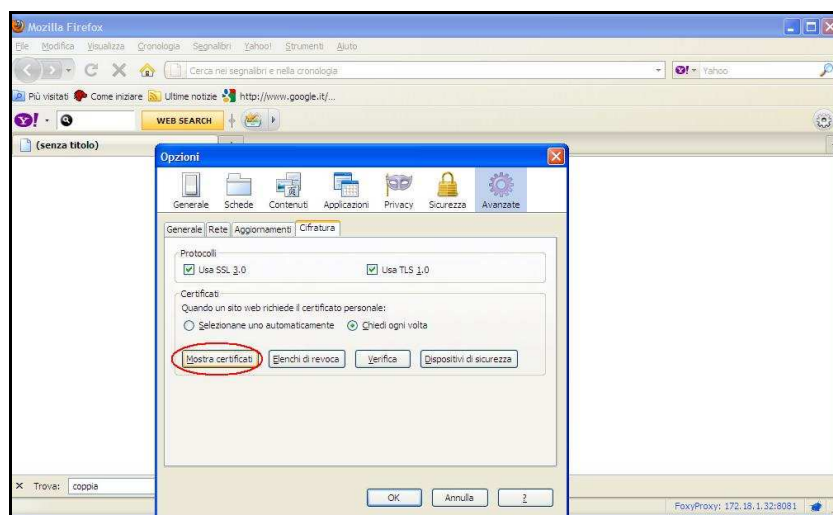
N.B. Tutti i file utilizzati come per queste operazioni devono essere rimossi e conservati in modo sicuro.

4.1. Import del file formato PKCS#12

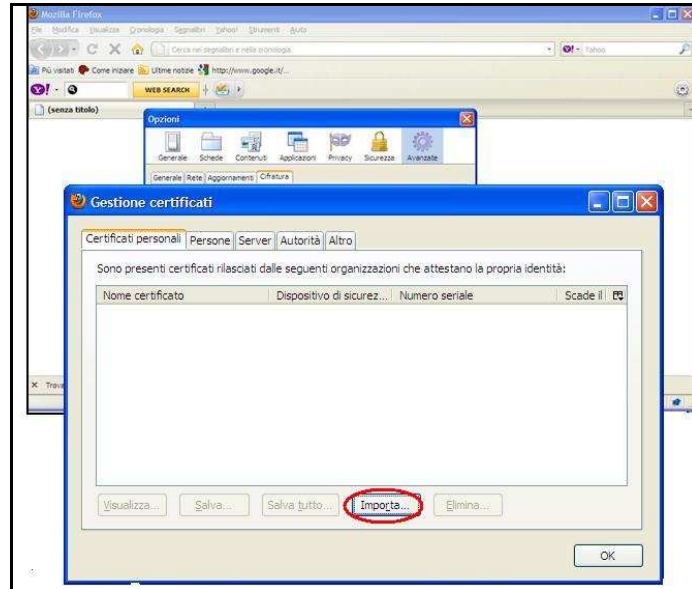
Il test seguente consente di verificare che il sistema di chiavi sia stato realizzato correttamente. Per procedere con il test, aprire “Mozilla Firefox”. Nella colonna degli strumenti, cliccare sulla voce “Opzioni”.



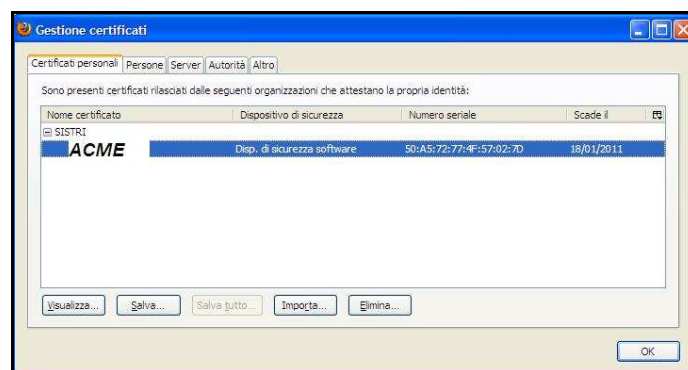
All’apertura della finestra Opzioni, cliccare su “Avanzate”, sezione “Cifratura” e sul bottone “Mostra certificati”.



All’apertura della finestra “Gestione certificati”, nella sezione “Certificati personali”, cliccare 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:

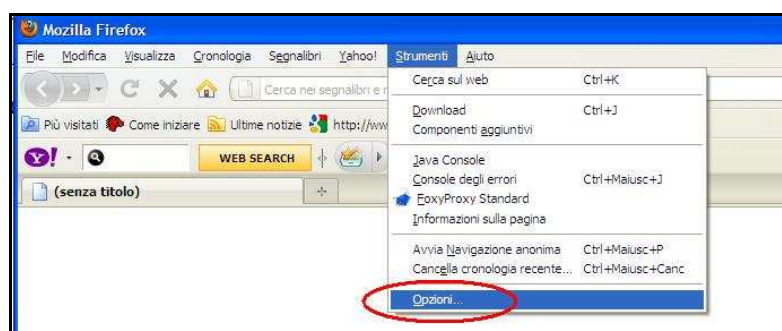


A questo punto il certificato è creato con successo.

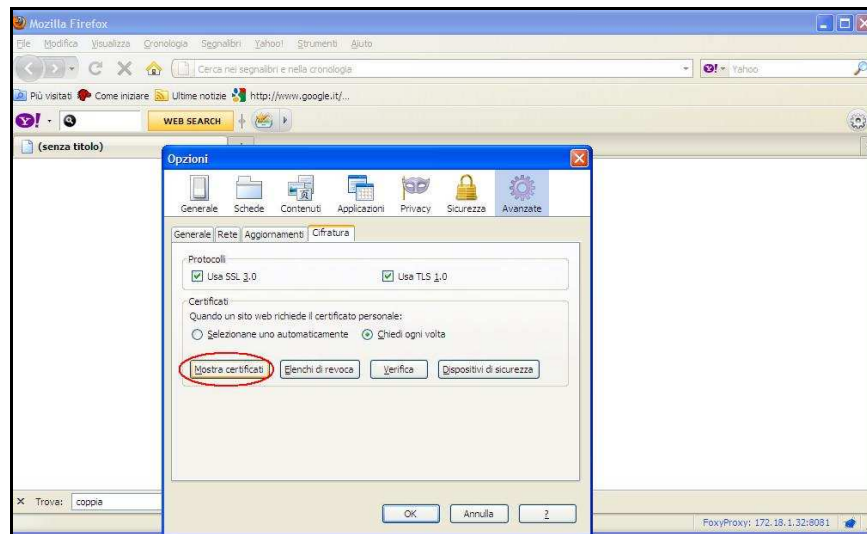
4.2. Import del certificato della Root CA SISTRI

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

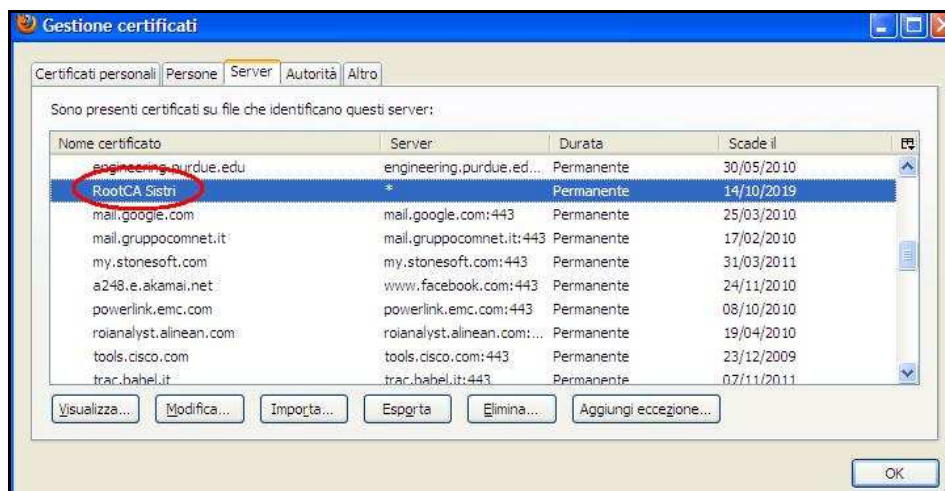
Se si desidera importare il certificato occorre seguire la seguente procedura. Per procedere aprire “Mozilla Firefox”. Nella colonna degli strumenti, cliccare sulla voce “Opzioni”.



All'apertura della finestra Opzioni, cliccare su "Avanzate" e sul bottone "Mostra certificati".



All'apertura della finestra "Gestione certificati", nella sezione "Server", cliccare sul bottone "Importa". Navigare nella directory in cui è posizionato 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.

4.3. 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 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 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:sequence>
      </xsd:complexType>
    </xsd:element>
    -<xsd:element name="GetElencoCataloghiResponse">
      -<xsd:complexType>
        -<xsd:sequence>
          <xsd:element minOccurs="0" maxOccurs="unbounded" name="out" nillable="true" type="ms:DescrittoreCatalogo"/>
        </xsd:sequence>
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="GetElencoCataloghi_fault" type="ms:SISException"/>
  </xsd:schema>
</wsdl:types>
</wsdl:definitions>
```



Allegati

A. Modulo per la richiesta del certificato

Il modulo viene generato automaticamente dall'applicazione.

L'utente deve inserire i dati, stamparlo, firmarlo, scansionarlo in PDF ed eseguire l'upload nel sistema SISTRI fornendo i documenti richiesti.

DATI DEL RICHIEDENTE		
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:	
DOCUMENTO IDENTITÀ DEL RICHIEDENTE		
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">• Carta d'identità;• Passaporto;• Patente auto;• Tesserino di riconoscimento del personale delle amministrazioni statali.		
DICHIARAZIONE SOSTITUTIVA CODICE FISCALE		
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 _____		
SCOPO D'UTILIZZO		
Applicazione:		
Modalità d'uso:		
Formato:		
TIPO CERTIFICATO		
X509: PEM <input type="checkbox"/> DER <input type="checkbox"/>		



B. Modulo per la richiesta di autorizzazione all'utilizzo dei servizi di interoperabilità

Il modulo viene generato automaticamente dall'applicazione. L'utente deve inserire i dati, stamparlo, firmarlo, scansarlo in PDF ed eseguire l'upload nel sistema SISTRI analogamente a quanto previsto per il modulo precedente.

**MODULO DI RICHIESTA DI AUTORIZZAZIONE ALL'UTILIZZO DEI SERVIZI DI INTEROPERABILITÀ
DEL SISTRI PER LE ATTIVITÀ DI PREDISPOSIZIONE DEL SISTEMA GESTIONALE**

Il/La sottoscritto/a _____,

nato/a a _____ il ___ / ___ / _____,

codice fiscale _____, nella sua qualità di _____

e legale rappresentante della _____,

codice pratica SISTRI _____ con sede legale in _____

_____ codice fiscale _____, di seguito "l'Impresa",

RICHIEDE l'autorizzazione all'utilizzo dei servizi di interoperabilità del SISTRI al fine di poter inviare e richiedere i dati relativi alla tracciabilità dei rifiuti di pertinenza dell'Impresa. Certifica, inoltre, che il sistema gestionale sotto indicato e l'organizzazione dell'impresa rispondono ai requisiti di sicurezza previsti dalle disposizioni normative vigenti ed è consapevole che, in caso di mancato soddisfacimento di questi requisiti, è vietato l'utilizzo dei servizi volti all'ottenimento o all'invio dei dati relativi alla tracciabilità dei rifiuti.

Di seguito si riportano i dettagli del sistema in dotazione:

Azienda Produttrice: _____

Nome Sistema: _____

Versione: _____

Numero installazioni: _____

_____ li, ___ / ___ / _____

(firma leggibile)



C. Procedura di generazione CSR

Il primo passo da effettuare è la generazione di una coppia di chiavi (una pubblica ed una privata). Per la generazione della coppia di chiavi, [pubblica e privata] è possibile utilizzare numerosi strumenti. Nel nostro esempio proponiamo l'utilizzo del software OpenSSL, su sistema operativo Linux. L'utente può tuttavia utilizzare soluzioni analoghe su sistemi operativi alternativi che producano una CSR (PKCS#10) conforme agli standard richiesti. L'integrità della chiave privata dipende strettamente dalla riservatezza con cui viene trattata e deve essere custodita secondo gli standard di sicurezza previsti per lo scopo.

Esempio di generazione della CSR

Collegarsi ad un sistema operativo Linux che abbia installato Open SSL. Posizionarsi nella directory in cui si vuole generare la coppia di chiavi ed eseguire la procedura riportata nel riquadro seguente:

Eseguire 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" questi sono presenti nel sistema sotto forma di file di testo. Il file da inviare al SISTRI tramite l'applicazione è [public.csr]