



21/02/2013

MANUALE DI ISTRUZIONI DELL'APPLICAZIONE SID – GENERAZIONE CERTIFICATI

VERSIONE 1.0

INDICE

1. PREMESSA	4
2. INSTALLAZIONE	5
3. ESECUZIONE	6
4. STRUTTURA DELLE CARTELLE	7
5. CARATTERISTICHE GENERALI DELL'APPLICAZIONE	9
6. GENERAZIONE AMBIENTE DI SICUREZZA	10
6.1 FUNZIONE IMPOSTA AMBIENTE	12
7. FUNZIONI DI AUSILIO ALL'AMBIENTE DI SICUREZZA	26
7.1 FUNZIONE IMPORTA CERTIFICATO	26
7.2 FUNZIONE VISUALIZZA CERTIFICATI UTENTE	27
7.3 FUNZIONE COPIA AMBIENTE	28
7.4 FUNZIONE CAMBIA PASSWORD DI PROTEZIONE	28
8. ALTRE FUNZIONALITA' DELL'APPLICAZIONE	29
8.1 FUNZIONI DI CONFIGURAZIONE	29
8.2 FUNZIONI DI CONSULTAZIONE	30
8.3 FUNZIONI DI GUIDA	31
9. PROCEDURA MANUALE PER IL COMPLETAMENTO DELLA GENERAZIONE DELL'AMBIENTE DI SICUREZZA	33
9.1 INVIO DELLA RICHIESTA DI CERTIFICATO	33

9.2	DOWNLOAD DEL CERTIFICATO	34
9.3	IMPORTAZIONE DEL CERTIFICATO	36
10.	REVOCA DELL'AMBIENTE DI SICUREZZA	38

1. **PREMESSA**

Il presente documento è una guida per l'installazione e l'utilizzo dell'applicazione "**SID - Generazione certificati**", distribuita dall'Agenzia delle Entrate per consentire a particolari utenti (società, enti, ditte individuali), abilitati al **Servizio telematico Fisconline**, di poter ottenere dei certificati di firma e di cifra rilasciati dall'Agenzia delle Entrate mediante i quali è possibile operare nell'ambito del nuovo sistema di interscambio dati (SID).

2. INSTALLAZIONE

L'applicazione "**SID – Generazione certificati**" viene installata in una directory ("directory di installazione") che dovrà essere indicata dall'utente in fase di installazione dell'applicazione stessa. La directory iniziale dell'applicazione sarà comunque "**SID-GenerazioneCertificati**".

Per la sua esecuzione l'applicazione necessita della **JVM versione 1.6. o successive** integrata con le **policy java** indispensabili per la crittografia dei file.

In particolare per i sistemi operativi Windows l'applicazione durante l'installazione si aggancia all'ultima JVM disponibile sulla postazione di lavoro dell'utente (a partire dalla JVM 1.6 e superiori, quindi JVM 6 e JVM 7): nel "wizard" di installazione è presente una schermata che indica dove verranno installati i file di policy.

Inoltre in fase di installazione vengono salvate all'interno della cartella "...\\prog\\policy java" le policy di java relative alla JVM 1.6 e 1.7 che l'utente in caso di necessità (ad esempio in caso di aggiornamento automatico della JVM o di reinstallazione della stessa) potrà copiare manualmente all'interno della directory della JVM utilizzata "...\\Java\\jre6(jre7)\\lib\\security" senza dover reinstallare il pacchetto dell'applicazione.

3. ESECUZIONE

Al termine dell'operazione di installazione compare sul desktop della postazione di lavoro l'icona identificata dall'etichetta "**SID – Generazione Certificati**", che consente di attivare l'applicazione con un doppio "click".

4. STRUTTURA DELLE CARTELLE

All'interno della directory di installazione è prevista una struttura di cartelle nelle quali si trovano i diversi componenti dell'applicazione ed i file generati dall'applicazione stessa nelle varie fasi di utilizzo da parte dell'utente.

L'applicazione si installa nella cartella "**SID-GenerazioneCertificati**" all'interno della directory di installazione scelta dall'utente.

Le sotto-cartelle che vengono create sono le seguenti:

- cartella "**invio**" contenente i file da inviare all'Amministrazione finanziaria: in tale cartella viene salvato il file contenente la richiesta di certificati generata dall'applicazione che deve essere inviato all'Amministrazione finanziaria (file "**req.ccc**");
- cartella "**ricezione**" contenente i file di risposta predisposti dall'Amministrazione finanziaria: in tale cartella deve essere salvato il file contenente la risposta relativa alla richiesta di certificati inviata all'Amministrazione finanziaria (file "**certif.in**");
- cartella "**prog**" contenente tutte le componenti necessarie per l'esecuzione dell'applicazione. Tale cartella ha al suo interno le seguenti sotto-cartelle create in fase di installazione dell'applicazione:
 - cartella "**help**" contenente i file di help dell'applicazione in formato "pdf";
 - cartella "**img**" contenente le immagini utilizzate all'interno dell'applicazione;
 - cartella "**certstore**" contenente i certificati del servizio e della CA;

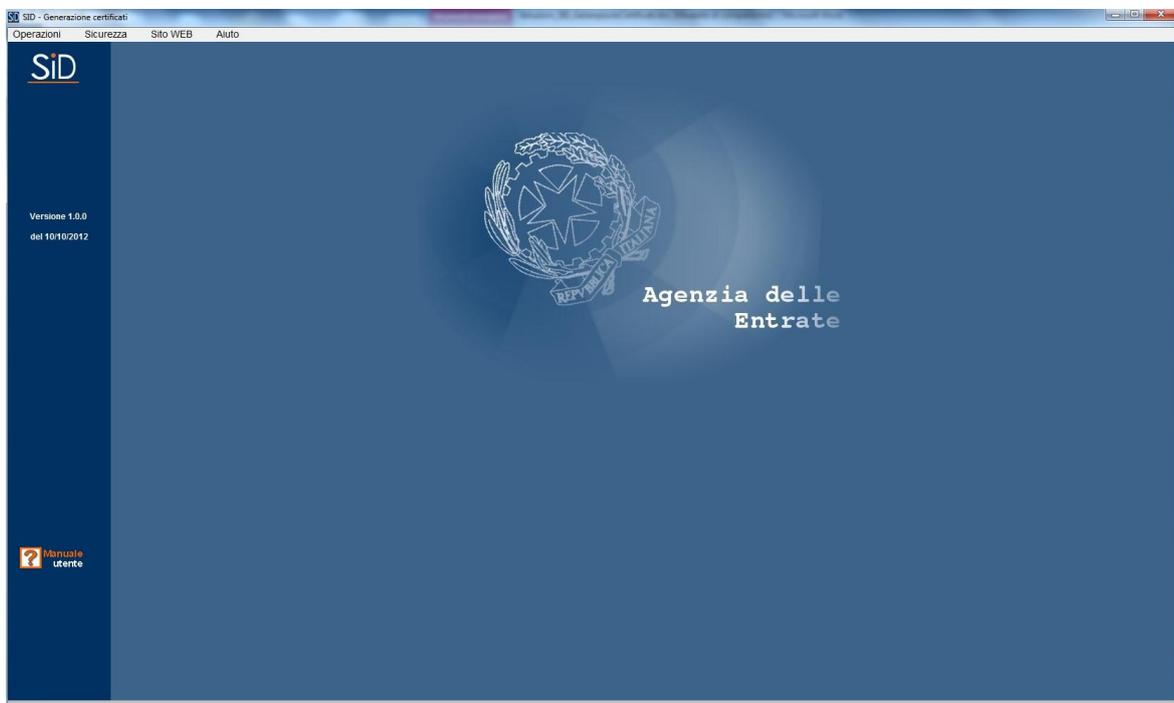
- cartella “**policy java**” contenente i file di policy relative alle versioni della JVM 1.6 e 1.7;
- cartella “**cfg**” contenente i file di configurazione dell'applicazione.

5. CARATTERISTICHE GENERALI DELL'APPLICAZIONE

L'applicazione contiene al suo interno le funzioni per la generazione e la gestione dell'ambiente di sicurezza ed altre funzioni di ausilio all'applicazione (funzioni di consultazione, funzioni di configurazione e funzioni guida).

Tali funzioni sono raggruppate nei seguenti menù:

- menù **“Operazioni”** per la gestione delle funzionalità di configurazione;
- menù **“Sicurezza”** per la gestione delle funzionalità relative all'ambiente di sicurezza;
- menù **“Sito WEB”** per la gestione delle funzionalità di consultazione;
- menù **“Aiuto”** per la gestione delle funzionalità di guida.



6. GENERAZIONE AMBIENTE DI SICUREZZA

Le funzioni descritte nei paragrafi che seguono sono relative alla generazione **dell'Ambiente di sicurezza**, cioè alla creazione delle credenziali di cui ciascun utente deve essere dotato per garantire l'identità di colui che effettua una determinata operazione, l'integrità dei dati trasmessi e la loro riservatezza.



Per generare l'ambiente di sicurezza è necessario selezionare la funzione **"Imposta ambiente"** nell'ambito del menù **"Sicurezza"**.

Tale funzione consente, in particolare, la generazione delle coppie di chiavi asimmetriche: una coppia di chiavi per la firma di cui una pubblica, nota a tutti per definizione, ed una privata nota solo all'utente; una coppia di chiavi per la cifra di cui una pubblica, nota a tutti per definizione, ed una privata nota solo all'utente.

La funzione prevede l'utilizzo di un supporto fisico (floppy, USB, etc.) su cui registrare le coppie di chiavi che dovrà essere successivamente custodito in luogo sicuro.

I dati richiesti all'utente in fase di generazione sono i seguenti:

- il codice PIN (formato da 10 caratteri) ottenuto mediante la procedura di abilitazione al servizio Fisconline;
- il codice fiscale dell'utente abilitato al servizio Fisconline;
- il PIN di revoca che rappresenta un codice scelto a piacere dall'utente costituito da un minimo di 15 e da un massimo di 20 caratteri (di cui solo numeri e/o lettere non accentate) da utilizzare nel caso in cui l'utente debba revocare il proprio ambiente di sicurezza mediante un'apposita funzione di "Ripristino" disponibile sul sito web del servizio Fisconline. Nel caso in cui l'utente, invece, non sia in possesso di tale codice nel momento della revoca potrà recarsi presso un ufficio finanziario per richiedere il ripristino dei codici di autenticazione;
- la password di protezione del supporto che rappresenta un codice scelto a piacere dall'utente costituito da un minimo di 8 e da un massimo di 15 caratteri (di cui solo numeri e/o lettere non accentate - almeno una lettera e almeno un numero);
- la conferma della password che prevede l'indicazione dello stesso valore specificato nel campo relativo alla password di protezione.

Al termine dell'inserimento da parte dell'utente di tali informazioni l'applicazione procede alla generazione delle coppie di chiavi ed alla creazione della richiesta di registrazione contenuta in un apposito file "req.ccc" salvato nella cartella "Invio" della directory di installazione dell'applicazione. Tale file, contenente le chiavi pubbliche (di cifratura e di firma), deve essere trasmesso in via telematica all'Agenzia delle Entrate tramite il servizio Fisconline.

Il certificato ha una validità di 3 anni. E' cura dell'utente verificarne la scadenza e provvedere al suo rinnovo mediante la revoca del proprio ambiente di sicurezza e la generazione del nuovo ambiente.

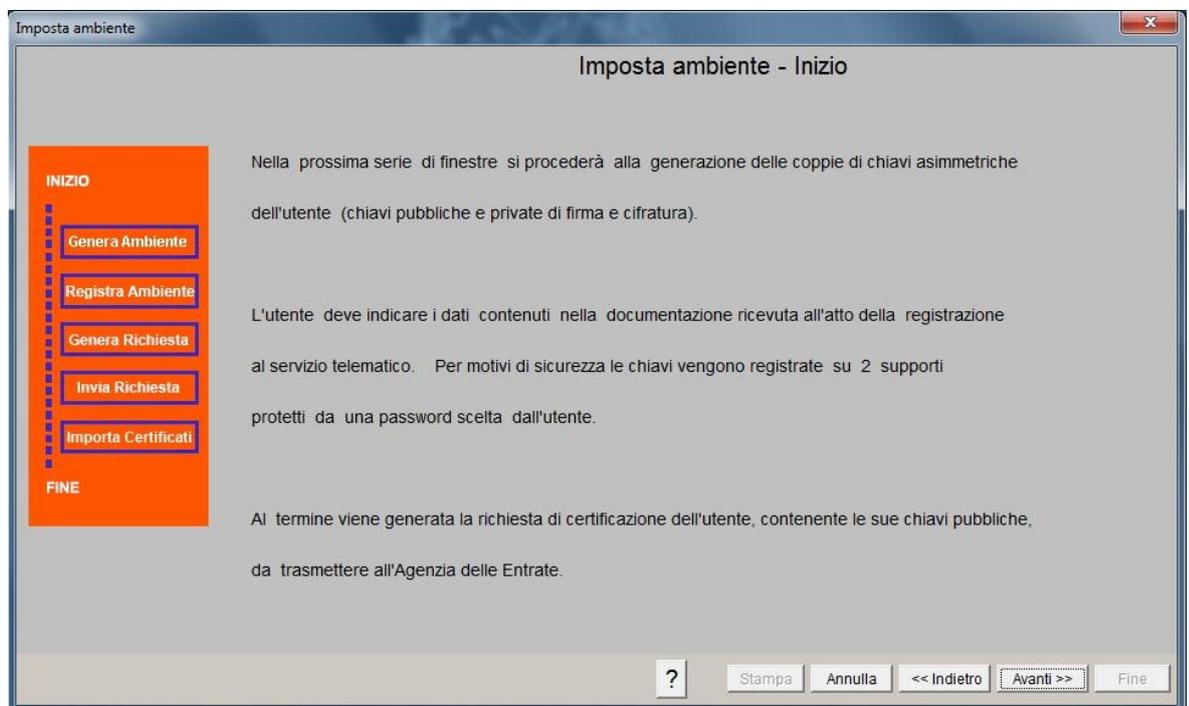
6.1 FUNZIONE IMPOSTA AMBIENTE

La funzione “**Imposta ambiente**” prevede una sequenza di schermate di tipo “wizard” in modo da facilitare l'utente nella procedura di generazione delle coppie di chiavi asimmetriche.

I passi da seguire sono di seguito descritti:

Imposta ambiente – Inizio

In questa fase vengono fornite all'utente alcune informazioni di carattere generale.



Imposta ambiente – Genera ambiente (passo 1 di 4)

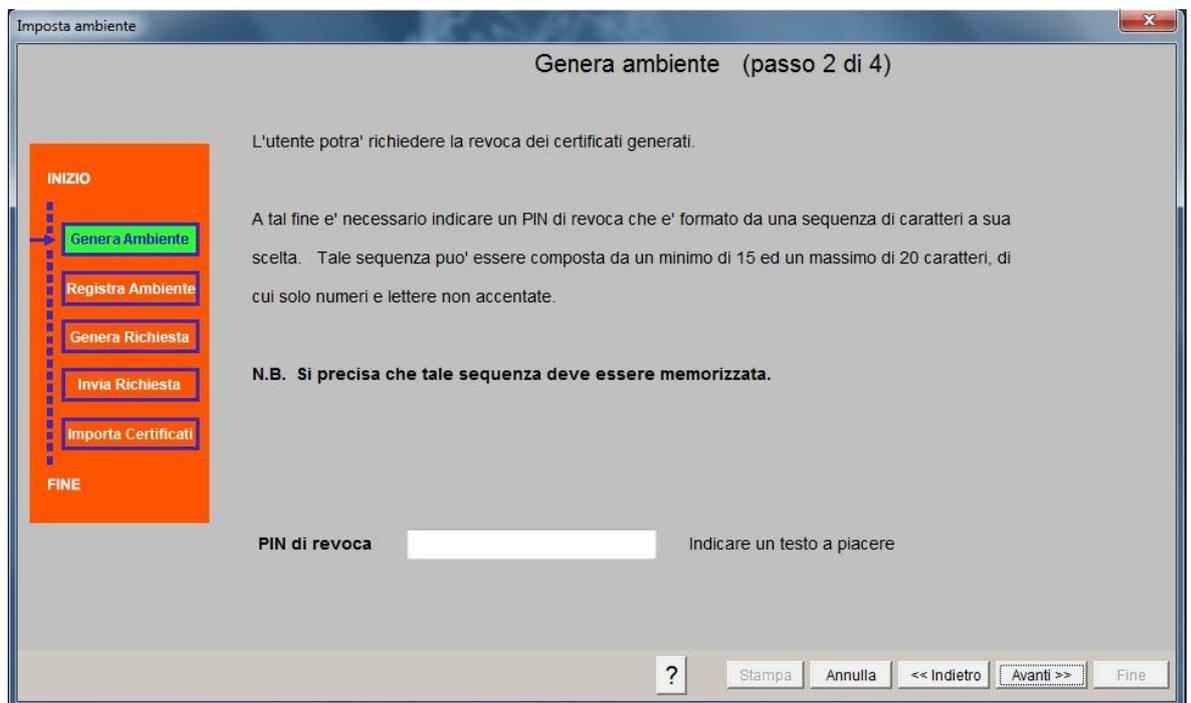
In questa fase viene richiesto all'utente di inserire il proprio codice fiscale ed il codice PIN (composto da 10 numeri) ottenuto mediante la registrazione al servizio Fisconline.

The screenshot shows a software window titled "Imposta ambiente" with a sub-header "Genera ambiente (passo 1 di 4)". On the left side, there is a vertical orange navigation bar containing the following items: "INIZIO", "Genera Ambiente" (highlighted in green), "Registra Ambiente", "Genera Richiesta", "Invia Richiesta", "Importa Certificati", and "FINE". The main content area contains the instruction: "Inserire il codice fiscale dell'utente ed il codice PIN ottenuto all'atto della registrazione al servizio telematico." Below this instruction are two input fields: "Codice fiscale" and "Codice PIN". At the bottom of the window, there is a row of buttons: a question mark icon, "Stampa", "Annulla", "<< Indietro", "Avanti >>", and "Fine".

Imposta ambiente – Genera ambiente (passo 2 di 4)

In questa fase viene richiesto all'utente di inserire il PIN di revoca: l'utente deve indicare una sequenza di caratteri a sua scelta. Tale sequenza può essere composta da un minimo di 15 caratteri fino ad un massimo di 20 caratteri, di cui solo numeri e lettere non accentate.

Il PIN di revoca deve essere memorizzato dall'utente in quanto potrà essere utilizzato per revocare il proprio ambiente di sicurezza. Si consiglia, pertanto, di scrivere il codice prescelto archiviandolo in luogo non accessibile da parte di altre persone.



Imposta ambiente – Genera ambiente (passo 3 di 4)

In questa fase viene richiesto all'utente di inserire il supporto di registrazione e di indicare la password di protezione del proprio ambiente di sicurezza con la relativa conferma: l'utente deve indicare una sequenza di caratteri a sua scelta. Tale sequenza può essere composta da un minimo di 8 caratteri fino ad un massimo di 20 caratteri, di cui solo numeri e lettere non accentate. Inoltre devono essere presenti almeno una lettera ed almeno un numero.

La password di protezione dell'ambiente di sicurezza deve essere memorizzata dall'utente in quanto dovrà essere utilizzata sia per la predisposizione dei flussi da trasmettere all'Agenzia che per l'elaborazione delle ricevute nel caso in cui queste siano state predisposte in formato cifrato. Si consiglia, pertanto, di scrivere il codice prescelto archiviandolo in luogo non accessibile da parte di altre persone. La password di protezione, infatti, è nota soltanto all'utente e, quindi, in caso di smarrimento o di dimenticanza, non è in alcun modo recuperabile e sarà necessario procedere alla revoca del proprio ambiente di sicurezza ed alla successiva generazione.

Imposta ambiente

Genera ambiente (passo 3 di 4)

INIZIO

- Genera Ambiente
- Registra Ambiente
- Genera Richiesta
- Invia Richiesta
- Importa Certificati

FINE

Le chiavi devono essere registrate su un supporto precedentemente formattato e devono essere protette da una password, scelta dall'utente, formata da non meno di 8 e non più di 20 caratteri, di cui solo numeri e lettere non accentate. Devono essere presenti almeno una lettera ed almeno un numero.

Inserire il supporto ed indicare la password di protezione. La password deve essere ripetuta nella casella "Conferma Password".

N.B. Si ricorda che la password deve essere memorizzata.

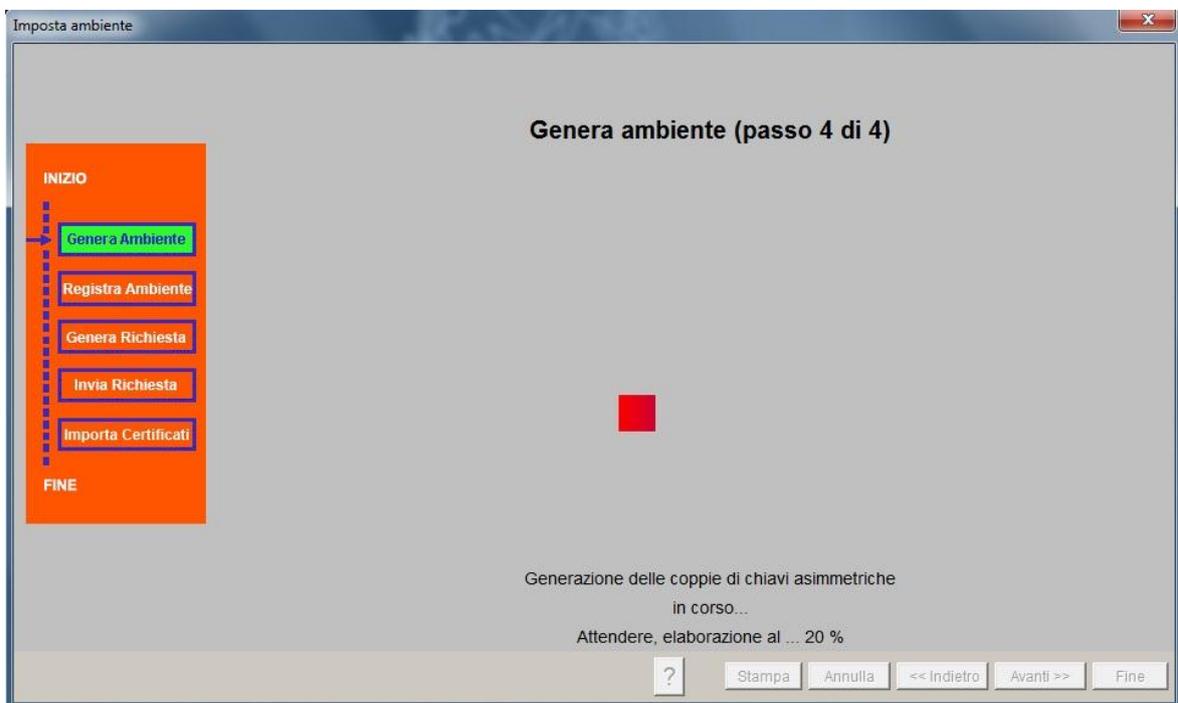
Password di protezione

Conferma Password

? Stampa Annulla << Indietro Avanti >> Fine

Imposta ambiente – Genera ambiente (passo 4 di 4)

In questa fase avviene la generazione delle coppie di chiavi asimmetriche: una coppia di chiavi (di cui una pubblica ed una privata) per la firma dei file ed una coppia di chiavi (di cui una pubblica ed una privata) per la decifrazione delle ricevute.



Imposta ambiente – Registra ambiente

Il risultato della generazione delle coppie di chiavi comporta il salvataggio sul supporto indicato dall'utente del file:

- UTENTE.KS – file “repository” contenente i certificati di firma e di cifra.



Imposta ambiente – Genera richiesta

In questa fase avviene la generazione della richiesta di certificato che dovrà essere inviata telematicamente all'Amministrazione per essere validata.

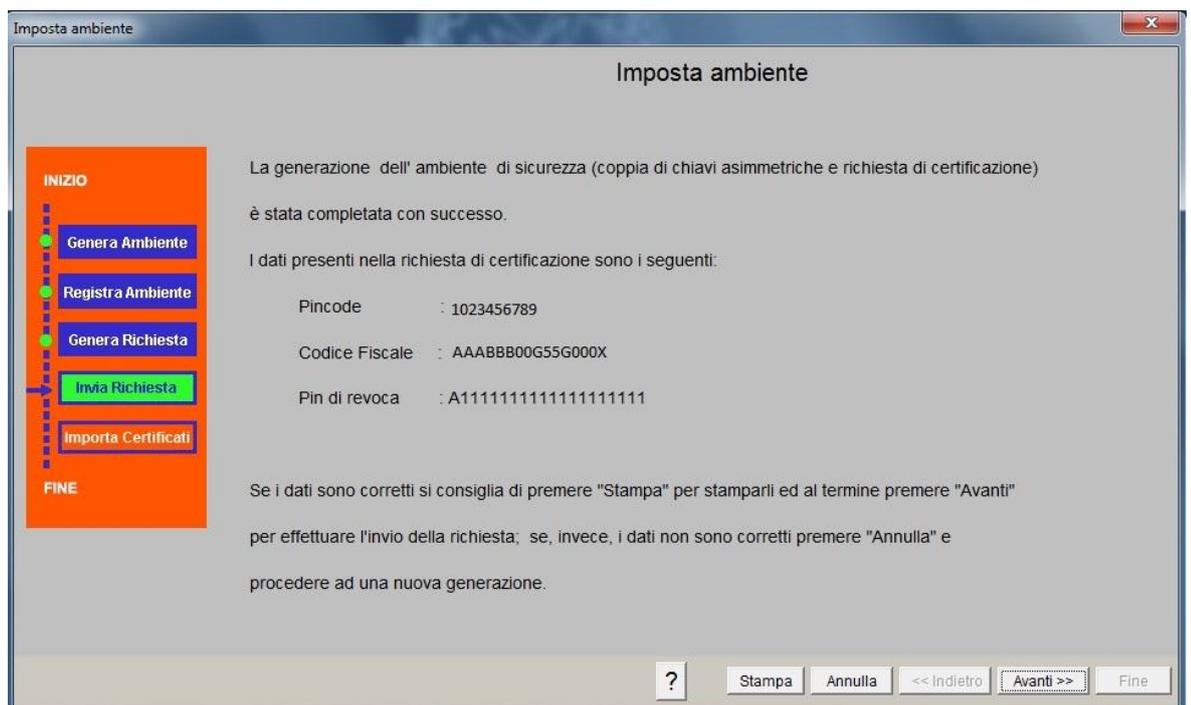
Al termine di questa fase, infatti, l'applicazione scrive nell'apposita cartella "Invio" della directory di installazione il file "REQ.CCC" contenente le chiavi pubbliche (di cifratura e di firma) da trasmettere in via telematica all'Agenzia delle Entrate mediante il servizio Fisconline.



Imposta ambiente – Dettaglio richiesta

In questa fase vengono fornite le informazioni di dettaglio contenute all'interno della richiesta in modo tale che possano essere verificate dall'utente prima che la richiesta sia inviata all'Amministrazione.

Si raccomanda, pertanto, di controllare che le informazioni indicate siano esattamente quelle presenti nella documentazione rilasciata al momento dell'abilitazione, in quanto se non dovessero coincidere, la richiesta sarà scartata dal sistema.



Imposta ambiente – Invio richiesta (passo 1 di 2)

In questa fase viene richiesto all'utente di inserire le proprie credenziali di accesso al servizio telematico (nome utente e password).

Inoltre l'utente deve specificare l'opzione "Invio da effettuare per proprio conto" se sta effettuando la trasmissione di un proprio file, oppure deve selezionare l'opzione "Invio da effettuare per conto di un altro soggetto dal quale si è stati incaricati" nel caso in cui l'utente stia effettuando l'operazione di invio della richiesta per conto di un altro soggetto abilitato al servizio Fisconline. Se la trasmissione, pertanto, viene effettuata da un "gestore incaricato", che può essere abilitato indifferentemente al servizio Entratel oppure al servizio Fisconline, è necessario indicare anche il codice fiscale del soggetto per cui si sta effettuando la trasmissione.

Imposta ambiente

Invia richiesta (passo 1 di 2)

Prima di effettuare l'invio della richiesta verificare che la connessione sia attiva.

Indicare il nome utente e la password per accedere al servizio telematico.

Specificare se si sta effettuando una trasmissione per proprio conto oppure per conto di altri.

NOME UTENTE

PASSWORD

Invio da effettuare per proprio conto

Invio da effettuare per conto di un altro soggetto dal quale si è stati incaricati

CODICE FISCALE

INIZIO

Genera Ambiente

Registra Ambiente

Genera Richiesta

Invia Richiesta

Importa Certificati

FINE

? Stampa Annulla << Indietro Avanti >> Fine

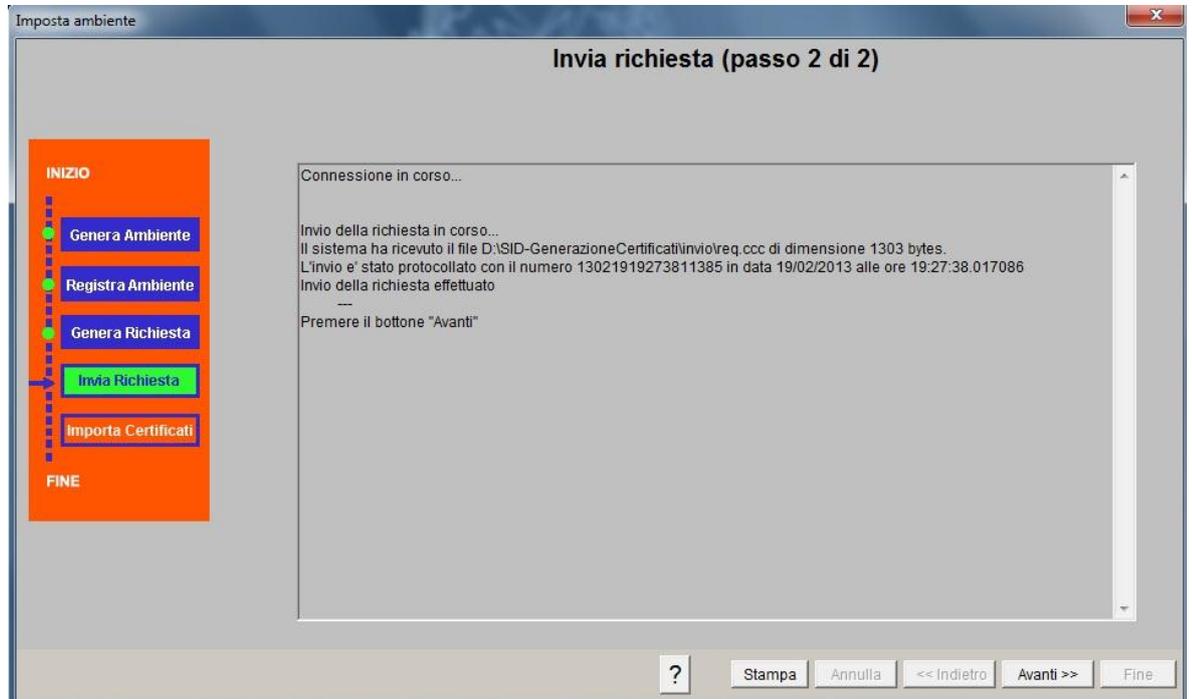
Imposta ambiente – Invio richiesta (passo 2 di 2)

In questa fase viene effettuato l'invio della richiesta di certificato all'Amministrazione.

A tal proposito l'applicazione esegue automaticamente l'invio della richiesta di certificato contenuta nel file "**req.ccc**". Pertanto è necessario assicurarsi che la postazione di lavoro sia correttamente configurata e collegata per eseguire la connessione (modem collegato, linea libera, connessione ADSL attivata, etc.).

A seguito dell'invio il sistema rilascia un protocollo di ricezione che attesta l'avvenuta ricezione del file. La richiesta di certificato viene elaborata e viene prodotta una ricevuta di accoglimento o di scarto in funzione dell'esito dell'elaborazione.

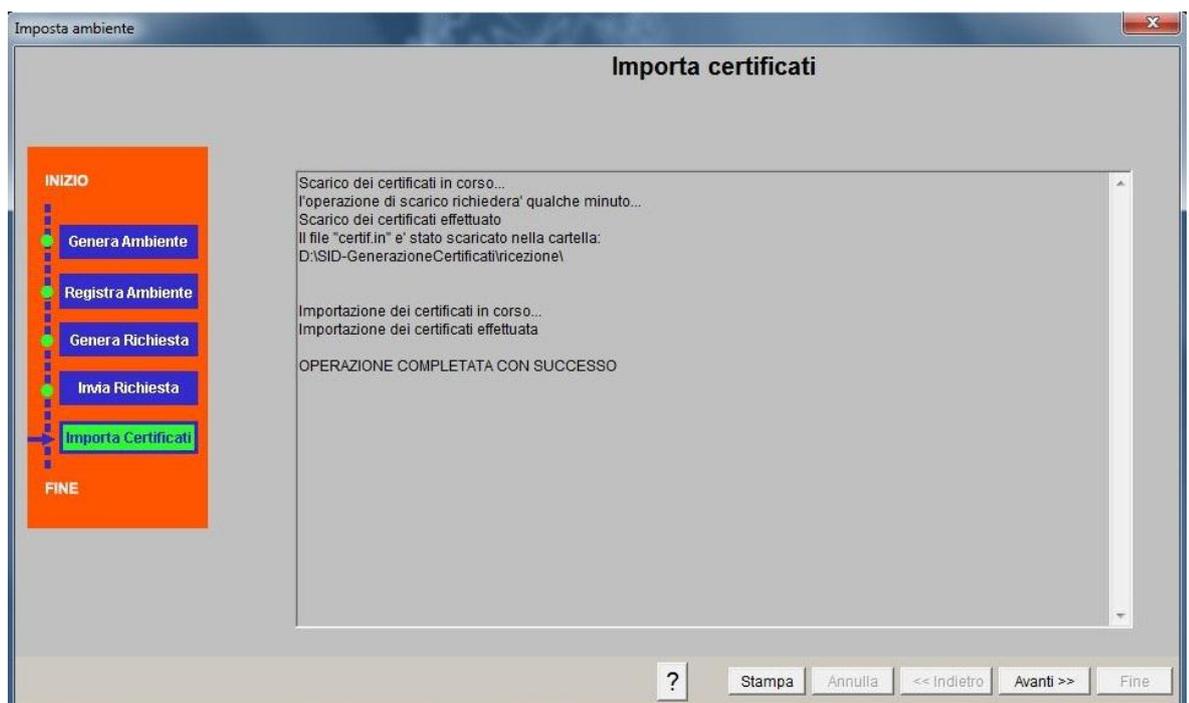
Nel caso in cui la richiesta venga rifiutata dal sistema la procedura si interrompe, altrimenti è possibile procedere alla fase successiva di importazione del certificato.



Imposta ambiente – Importa certificato

A seguito dell'invio della richiesta di certificato il sistema procede alla sua elaborazione verificando la correttezza delle informazioni in essa contenute.

Se la risposta del sistema avviene entro l'intervallo "di attesa" previsto, l'applicazione prosegue con il "download" del file che contiene le chiavi pubbliche dell'utente (file "**CERTIF.IN**") all'interno della cartella "Ricezione" dell'applicazione e successivamente con l'importazione nel "repository" dei certificati della componente pubblica validata dall'Amministrazione.



Al termine di tale operazione verranno creati i certificati di firma e di cifra all'interno della cartella scelta dall'utente:

- UTEF.P12 (certificato di firma),

- UTEC.P12 (certificato di cifra).

Se, invece, la ricevuta non è disponibile nel tempo “prefissato” dall'applicazione, l'utente dovrà procedere “manualmente” al “download” del file ed alla importazione delle informazioni nel “repository” delle chiavi mediante l'apposita funzione “Importa certificato” presente all'interno del menù “Sicurezza” dell'applicazione stessa.

7. FUNZIONI DI AUSILIO ALL'AMBIENTE DI SICUREZZA

Le funzioni di ausilio alla gestione dell'ambiente di sicurezza sono le seguenti:

1. “**Importa certificato**” per completare l'ambiente di sicurezza nel caso in cui la procedura automatica si interrompa durante la fase di invio della richiesta di certificato;
2. “**Visualizza certificati utente**” per visualizzare i dati presenti nel certificato di cifratura e nel certificato utilizzato per calcolare i codici di autenticazione;
3. “**Copia ambiente**” per copiare l'ambiente di sicurezza da un supporto ad un altro;
4. “**Cambia password di protezione**” per modificare la password di protezione del supporto che contiene l'ambiente di sicurezza dell'utente.

7.1 FUNZIONE IMPORTA CERTIFICATO

La funzione consente di importare nel “repository” dei certificati la componente pubblica validata dall'Amministrazione.

Per l'importazione dei certificati è necessario eseguire i seguenti passi:

- accedere all'apposita pagina dei servizi del Sito Telematico Fisconline per verificare che il file contenente la richiesta di certificato (REQ.CCC) sia stato elaborato con esito positivo dal sistema,
- verificare che il file corrispondente alla richiesta di certificato inviata (REQ.CCC) sia stato correttamente creato (CERTIF.IN);

- copiare il file CERTIF.IN in locale specificando come cartella di destinazione la cartella “Ricezione” dell'applicazione,
- inserire il supporto di memorizzazione che contiene l'ambiente di sicurezza (file “UTENTE.KS”) in precedenza generato, indicare la relativa password di protezione e procedere con l'elaborazione,
- verificare il buon esito dell'operazione eseguita.

I supporti sui quali è registrato l'ambiente di sicurezza devono essere conservati in luogo sicuro, al fine di evitarne un uso indebito da parte di terzi; è opportuno, inoltre, conservare in luogo diverso la password di protezione della chiave privata.

E' consigliabile infine, proteggere i supporti da ulteriori operazioni di scrittura.

7.2 FUNZIONE VISUALIZZA CERTIFICATI UTENTE

La funzione permette di visualizzare i dati presenti nel certificato di cifratura e di firma. A tal fine è necessario inserire il supporto di memorizzazione che contiene l'ambiente di sicurezza in precedenza generato ed indicare la relativa password di protezione.

In particolare i dati visualizzati per ciascun certificato sono i seguenti:

- il codice fiscale ed il progressivo sede dell'utente,
- la data di inizio e quella di fine validità,
- lo stato del certificato (valido, non ancora valido, scaduto, in scadenza),

- il tipo di utilizzo cui è destinato il certificato (certificato di firma o certificato di cifra).

Inoltre mediante la selezione del “Dettaglio” di ciascun certificato si ottengono ulteriori informazioni.

7.3 FUNZIONE COPIA AMBIENTE

La funzione consente di copiare il contenuto del supporto di memorizzazione dell'ambiente di sicurezza su un altro supporto in modo da avere più copie.

In tal caso è necessario inserire il supporto di origine che contiene l'ambiente di sicurezza dell'utente e successivamente quello di destinazione.

7.4 FUNZIONE CAMBIA PASSWORD DI PROTEZIONE

La funzione consente di modificare la password di protezione del supporto di memorizzazione che contiene l'ambiente di sicurezza dell'utente.

In tal caso è necessario inserire il supporto che contiene l'ambiente di sicurezza dell'utente indicare i seguenti dati:

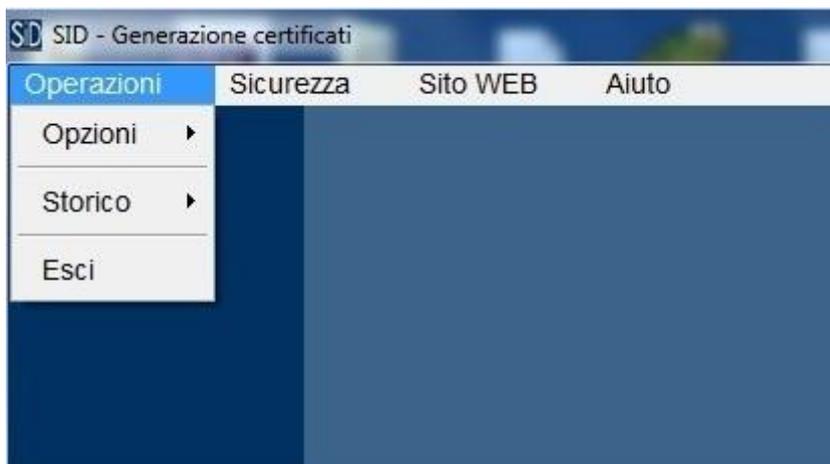
- la “vecchia” password di protezione;
- la nuova password di protezione;
- la conferma della nuova password di protezione.

8. ALTRE FUNZIONALITA' DELL'APPLICAZIONE

Oltre alle funzioni base che riguardano la generazione e la gestione dell'ambiente di sicurezza l'applicazione prevede una serie di funzionalità che ne ottimizzano la gestione.

8.1 FUNZIONI DI CONFIGURAZIONE

Le funzioni di configurazione sono inserite nel menù **Operazioni** che consente l'accesso alle seguenti funzioni di utilità:



- **Opzioni** per modificare alcune impostazioni di “default” dell'applicazione;
- **Storico**, per consultare il riepilogo delle operazioni eseguite, per ciò che riguarda la generazione dell'ambiente di sicurezza. Le operazioni di generazione, infatti, vengono registrate in un apposito file. A tal proposito le informazioni riportate sono le seguenti:
 - data ed ora in cui è stata eseguita l'operazione generazione dell'ambiente di sicurezza,

- nome del file creato dall'operazione di generazione dell'ambiente di sicurezza (comprensivo di tutto il percorso,
- codice fiscale e progressivo sede inseriti nella richiesta di certificato;
- **Esci**, per chiudere l'applicazione.

8.2 FUNZIONI DI CONSULTAZIONE

Le funzioni di consultazione sono inserite nel menu **"Sito Web"** che consente all'utente sia di attivare la connessione e di accedere alla "home page" del sito dei servizi telematici. Tale menù prevede le seguenti sotto-funzioni:

- **"Servizio telematico"** per accedere alla pagina iniziale del sito dei servizi telematici;
- **"Assistenza"** per accedere alla pagina iniziale del sito dell'assistenza (<http://assistenza.agenziaentrate.gov.it>) che fornisce informazioni utili relative all'utilizzo del Servizio Telematico Fisconline.



8.3 FUNZIONI DI GUIDA

Le funzioni di guida sono contenute nel menu “**Aiuto**”. Tale menù, infatti, contiene al suo interno alcune funzioni il cui scopo è quello di guidare l'utente nell'utilizzo dell'applicazione e di fornire informazioni dettagliate relativamente all'applicazione stessa.



Tale menù prevede le seguenti sotto-funzioni:

- “**Novità**” per visualizzare le novità relative alla versione installata dell'applicazione;
- “**Guida**” per visualizzare le pagine di help dell'applicazione;
- “**Versione**” per visualizzare le seguenti informazioni:
 - la versione e la data dell'applicazione;
 - la versione del Run Time Java;

- il sistema operativo su cui risulta installata l'applicazione con la relativa versione;
- la directory di installazione dell'applicazione.



9. PROCEDURA MANUALE PER IL COMPLETAMENTO DELLA GENERAZIONE DELL'AMBIENTE DI SICUREZZA

Nel caso in cui l'utente non sia riuscito a completare la generazione dell'ambiente di sicurezza mediante l'apposita funzione "Imposta ambiente" del menù "Sicurezza" (connessione non attiva, credenziale indicate errate, tempo di risposta superiore a quello "atteso" dall'applicazione, etc.) è necessario procedere "manualmente" alla esecuzione delle operazioni successive a quella di creazione della richiesta di certificato contenuta nel file "**REQ.CCC**".

Tali operazioni vengono di seguito descritte.

9.1 INVIO DELLA RICHIESTA DI CERTIFICATO

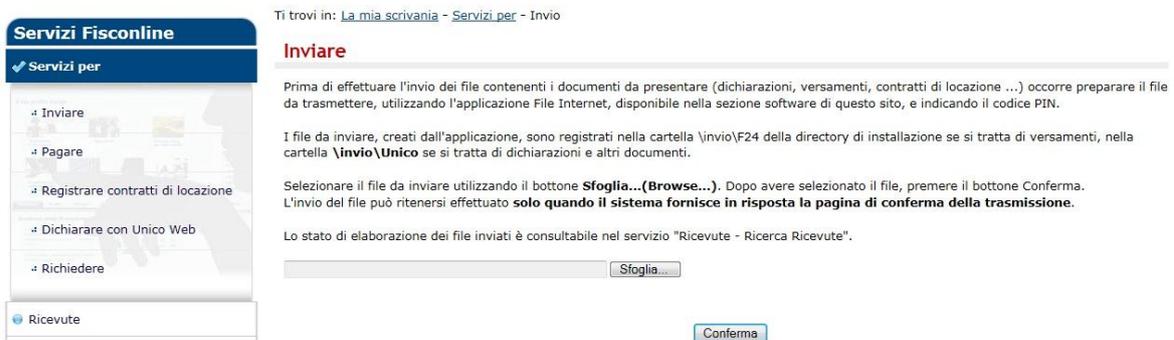
Nel caso in cui l'utente non sia riuscito ad effettuare l'invio della richiesta di certificato mediante l'apposita funzione "Imposta ambiente" del menù "Sicurezza" (connessione non attiva, credenziale indicate errate, etc.) è necessario effettuare "manualmente" la trasmissione del file "**REQ.CCC**".

A tal proposito la procedura da seguire è:

- accedere alla pagina iniziale del sito web dei servizi telematici (<http://telematici.agenziaentrategov.it>)
- inserire le proprie credenziali;
- selezionare l'utenza di lavoro (cioè il codice fiscale corrispondente all'utenza con la quale si intende operare) con la quale interagire con il sistema nel caso in cui si svolgano le funzioni di "Gestore Incaricati" o di "Incaricato", a

seguito di una precisa delega in tal senso ricevuta in base all'organizzazione interna della struttura per la quale si opera;

- accedere alla funzione “Servizi per -> Inviare” del sito;
- selezionare il file da inviare utilizzando il bottone Sfoglia...(Browse...) e, dopo avere selezionato il file “REQ.CCC” dalla cartella “Invio” della directory di installazione dell'applicazione, confermare l'invio.



L'invio del file può ritenersi effettuato solo quando il sistema fornisce in risposta la pagina di conferma della trasmissione contenente il protocollo telematico assegnato dal sistema.

La richiesta di certificato viene identificata dal codice documento “**PKS10**”.

9.2 DOWNLOAD DEL CERTIFICATO

Nel caso in cui l'utente non sia riuscito ad effettuare il download della risposta relativa alla trasmissione della richiesta di certificato mediante l'apposita funzione “Imposta ambiente” del menù “Sicurezza” (connessione non attiva,

tempo di risposta superiore a quello “atteso” dall'applicazione, etc.) è necessario effettuare “manualmente” il download del file di risposta.

A tal proposito la procedura da seguire è:

- accedere alla pagina iniziale del sito web dei servizi telematici (<http://telematici.agenziaentrate.gov.it>)
- inserire le proprie credenziali;
- selezionare l'utenza di lavoro (cioè il codice fiscale corrispondente all'utenza con la quale si intende operare) con la quale interagire con il sistema nel caso in cui si svolgano le funzioni di “Gestore Incaricati” o di “Incaricato”, a seguito di una precisa delega in tal senso ricevuta in base all'organizzazione interna della struttura per la quale si opera;
- accedere alla funzione “Profilo utente > Stato richiesta certificato” del sito web;
- inserire il codice PIN dell'utente;
- controllare che la richiesta di certificato sia stata elaborata e che il file di risposta “**CERTIF.IN**”, associato al documento identificato dal codice “**PKS10**”, sia stato creato (in tal caso viene evidenziata una cartellina gialla chiusa);
- selezionare la cartellina gialla in corrispondenza del file inviato “**PKS10**” e copiare il file in locale specificando come cartella di destinazione la cartella “Ricezione” dell'applicazione. Nel caso in cui la richiesta di certificato sia stata rifiutata dal sistema in quanto errata non sarà possibile scaricare alcun file di ricezione poiché la risposta sarà visualizzabile e stampabile direttamente dal sito web.



Ti trovi in: [La mia scrivania](#) - [Profilo Utente](#) - [Stato Richiesta Certificati](#) - [Elenco Certificati](#)

Elenco certificati

Di seguito viene riportata la lista delle attestazioni di avvenuto ricevimento relative alle richieste di certificato che sono state trasmesse per via telematica all'Agenzia delle Entrate.

Dopo aver verificato lo stato di validità della richiesta di certificato è necessario cliccare sul simbolo  corrispondente alla riga nella quale viene indicato il protocollo attribuito alla richiesta inviata a salvare sulla propria postazione di lavoro il file di ricevuta denominato "CERTIF.IN" nella cartella "Ricezione" dell'applicazione "Generazione certificati".

Il simbolo  indica che la ricevuta non è disponibile in quanto la richiesta di certificato, pur essendo stata inviata dall'utente in sessione, contiene dati relativi ad altro utente.

Protocollo	Modello Ricevuta	Stato	Nome file	Data inizio validità	Data fine validità	Inviante	Motivo di scarto
13030535392711422	PKS10	 elaborato	req.ccc	05/03/2013	05/03/2016		

9.3 IMPORTAZIONE DEL CERTIFICATO

Nel caso in cui l'utente non sia riuscito ad effettuare il download della risposta relativa alla trasmissione della richiesta di certificato mediante l'apposita funzione "Imposta ambiente" del menù "Sicurezza" (connessione non attiva, tempo di risposta superiore a quello "atteso" dall'applicazione, etc.) è necessario completare "manualmente" la procedura di creazione dell'ambiente di sicurezza effettuando l'importazione, all'interno del "repository" dei certificati dell'utente, della componente pubblica validata dall'Amministrazione.

A tal proposito deve essere utilizzata l'apposita funzione "Importa certificato" presente sotto il menù "Sicurezza" dell'applicazione.



La procedura da seguire viene descritta al paragrafo “7.1 - FUNZIONE IMPORTA CERTIFICATO” di tale documento.

Al termine dell'operazione di importazione del certificato è consigliabile effettuare la copia dell'ambiente di sicurezza mediante la funzione “Copia ambiente” presente sotto il menù “Sicurezza” dell'applicazione.

Il supporto protetto da password contenente le coppie di chiavi asimmetriche, deve essere conservato con cura dall'utente in quanto dovrà essere utilizzato sia per firmare i file da inviare telematicamente all'Amministrazione, sia per elaborare le ricevute restituite dall'Agenzia delle Entrate.

10. REVOCA DELL'AMBIENTE DI SICUREZZA

Per richiedere la revoca del proprio ambiente di sicurezza qualora non fosse più integro o non più utilizzabile è necessario:

- accedere alla pagina iniziale del sito web dei servizi telematici (<http://telematici.agenziaentrate.gov.it>)
- inserire le proprie credenziali;
- selezionare l'utenza di lavoro (cioè il codice fiscale corrispondente all'utenza con la quale si intende operare) con la quale interagire con il sistema nel caso in cui si svolgano le funzioni di “Gestore Incaricati” o di “Incaricato”, a seguito di una precisa delega in tal senso ricevuta in base all'organizzazione interna della struttura per la quale si opera;
- accedere alla funzione “Profilo utente > Ripristina Ambiente” del sito web;
- indicare i seguenti dati:
 - il numero della richiesta di registrazione al servizio Fisconline presente nella lettera ricevuta al proprio domicilio ovvero, per gli utenti registrati mediante CNS, contenuto nella pagina visualizzata al termine della procedura di registrazione;
 - il PIN di revoca indicato in fase di generazione dell'ambiente di sicurezza;
- procedere nella conferma.



Ti trovi in: [La mia scrivania](#) - [Profilo Utente](#) - Ripristina Ambiente

Ripristina Ambiente

Questa funzione permette di richiedere la revoca del proprio ambiente di sicurezza qualora non fosse più integro o non più utilizzabile. Tale richiesta non è annullabile e, se viene completata con successo, l'utente dovrà generare nuovamente l'ambiente di sicurezza.

Per poter effettuare il "ripristino dei codici di autenticazione" è necessario indicare:

- il numero della richiesta di registrazione al servizio Fisconline presente nella lettera ricevuta al proprio domicilio ovvero, per gli utenti registrati mediante CNS, contenuto nella pagina visualizzata al termine della procedura di registrazione
- il PIN di revoca indicato in fase di generazione dell'ambiente di sicurezza;

Il sistema non tiene conto della differenza tra maiuscole e minuscole.

Numero Registrazione:

PIN di Revoca:

Il ripristino dell'ambiente di sicurezza non è un'operazione annullabile. Pertanto se l'operazione di ripristino viene completata con successo, l'utente dovrà generare nuovamente il proprio ambiente di sicurezza.

Infine, se l'utente non è in possesso dei dati necessari per effettuare il ripristino del proprio ambiente di sicurezza mediante la funzionalità presente nel sito web, deve presentare, presso un qualunque ufficio dell'Agenzia delle Entrate, la richiesta di ripristino delle chiavi per il calcolo dei codici di autenticazione.