

GENERA AMBIENTE

MANUALE PER L'UTENTE

Indice

1	Introduzione	3
2	Requisiti software	4
3	Genera chiavi	5
4	Copia dispositivo di firma.....	9
5	Blocco chiavi	11
6	Errore imprevisto dalla CA	13
7	Connection refused: no further information	14

1 Introduzione

Il Servizio Telematico Territorio gestisce l'invio dei documenti di aggiornamento per la Banca Dati dell'Agenzia del Territorio (sia Reparto di Pubblicità Immobiliare che Catasto).

Per i documenti trasmessi è necessario apporre le credenziali di firma. L'utente è libero di avvalersi di certificati emessi da enti accreditati tra i certificatori elencati dal CNIPA o avvalersi delle credenziali fornite dall'Agenzia del Territorio.

In quest'ultimo caso per la generazione del proprio certificato può avvalersi dell'applicazione web 'Genera ambiente' accedendo al servizio <https://generaambiente.agenziaterritorio.it/>.

Di seguito viene rappresentata l'home page del Servizio:

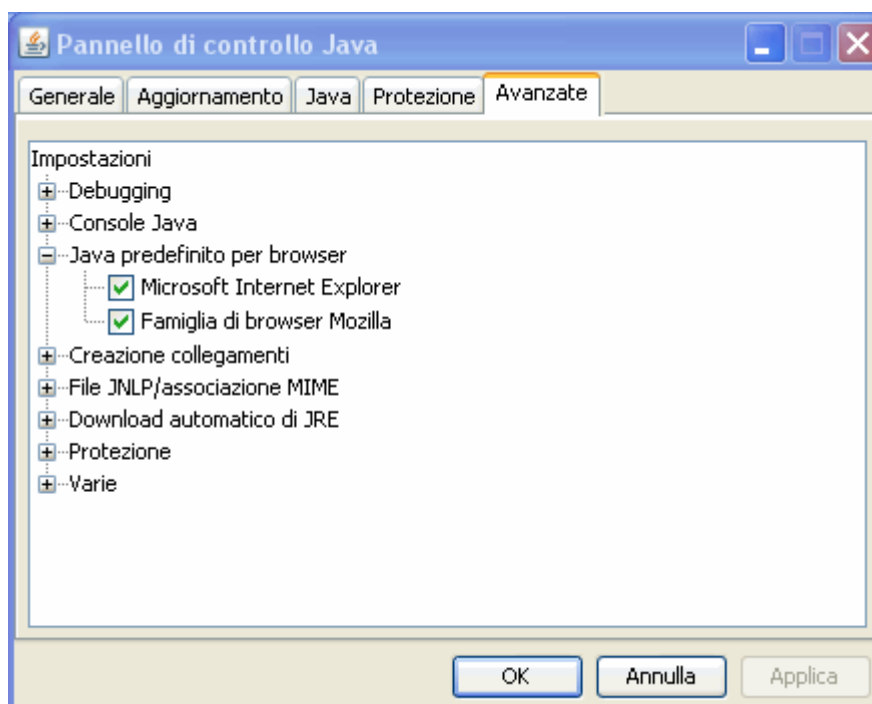


2 Requisiti software

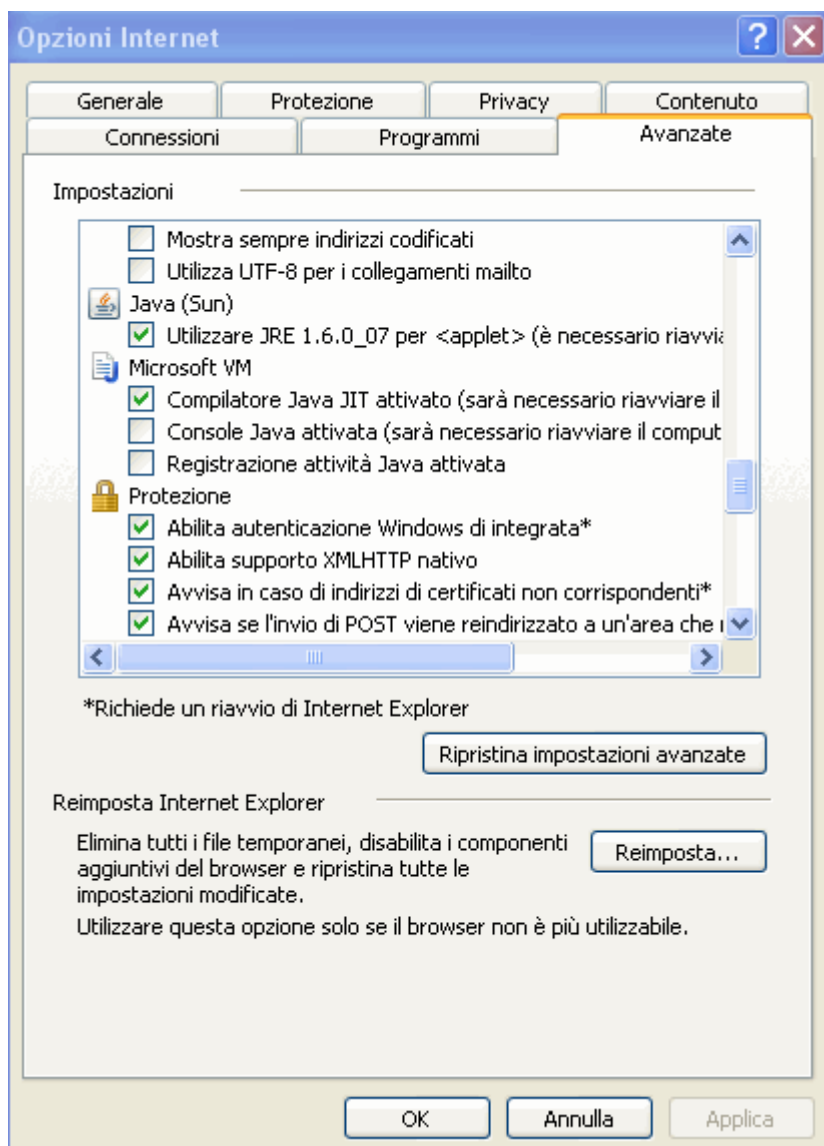
Per poter utilizzare correttamente l'applicazione web Genera Ambiente è necessario verificare il rispetto dei seguenti requisiti:

- **JRE 5.0 o successiva:** è necessario che sul computer dell'utente sia installata una versione del Java Runtime Environment di versione 5.0 o successiva;
- **Java predefinito per browser:** è necessario che il Java sia predefinito per il browser utilizzato dall'utente per accedere all'applicazione.

Per verificare questo requisito è necessario accedere al pannello di controllo Java dal pannello di controllo di Windows (Start / Impostazioni / Pannello di controllo / Java), verificando che sia selezionata la propria tipologia di browser (Internet Explorer e/o famiglia di browser Mozilla) nella tab "Avanzate", come evidenziato nella seguente immagine.



- **Abilitazione applet Java:** dalle opzioni del browser utilizzato è necessario abilitare le applet Java come evidenziato nella seguente immagine (browser Internet Explorer 7).



3 Genera chiavi

La funzione consente la generazione della coppia di chiavi dell'utente, pubblica e privata, che saranno successivamente utilizzate per il calcolo dei codici di autenticazione.

I passi che l'utente deve eseguire sono i seguenti:

Selezionare la funzione 'Genera chiavi', visualizzata sulla home page e fornire i dati richiesti:

- codice fiscale: codice fiscale del soggetto titolare del certificato
- PIN: numero del pin contenuto nella busta consegnata dall'ufficio al momento del censimento
- Numero postazione (o progressivo sede): 001
- Numero di autorizzazione: numero di registrazione attribuito durante la procedura di censimento dell'utente visualizzato sulla stampa dell'autorizzazione rilasciata dall'ufficio del territorio.

Genera Chiavi

Codice fiscale

PIN

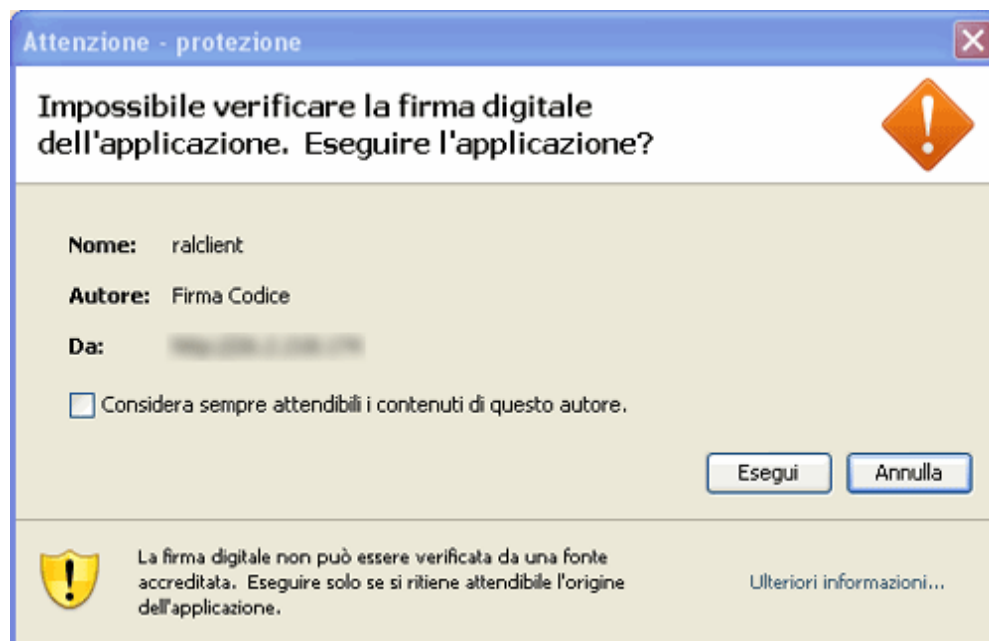
Postazione
numero

Autorizzazione
numero

Esegui

Ripristina

Alla richiesta di eseguire l'applicazione "ralclient" premere "Esegui" .



L'applicazione si connette automaticamente con il server di registrazione dell'Amministrazione finanziaria (RA centrale), che verifica i dati e ne invia un riscontro in risposta.

L'applicazione visualizza alcuni dati generali mostrati nella figura che segue :

Dati utente			
Codice fiscale	[redacted]	CommonName	[redacted]
Sede	001	Country	IT
Organization	Agenzia del Territorio	Organization Unit	Servizi Telematici

Genera Certificato

Qualora i dati visualizzati non dovessero coincidere con quelli noti all'utente, è necessario contattare l'Amministrazione finanziaria.

Nel caso in cui l'utente verifichi la coerenza dei dati, potrà selezionare il bottone 'Genera Certificato'.

Proseguendo nell'operazione, viene richiesto di indicare il dispositivo in cui dovrà essere registrato il certificato:



L'utente dovrà quindi scegliere e digitare una password di protezione del certificato che può avere un lunghezza da un minimo di 4 ad un massimo di 8 caratteri alfanumerici.



Tale password è quella che dovrà essere fornita all'applicazione 'Firma e Verifica ' ogni volta si dovrà procedere alla firma di un file da inviare al servizio telematico territorio.

L'applicazione in questa fase provvederà a:

- generare la chiave pubblica e privata dell'utente;
- registrare la chiave privata sul dispositivo scelto;
- comporre con la chiave pubblica la richiesta di iscrizione che viene trasmessa al server di certificazione (CA - Certification Authority) il quale:
 - controlla che l'utente non sia già titolare di un altro certificato ancora valido;
 - controlla che la stessa chiave pubblica non risulti già assegnata ad un altro utente;
 - genera e registra il certificato dell'utente;
 - restituisce il certificato all'applicazione.

Al termine l'applicazione provvederà a registrare sul dispositivo prescelto il certificato, creando un unico file di nome keystore.ks.



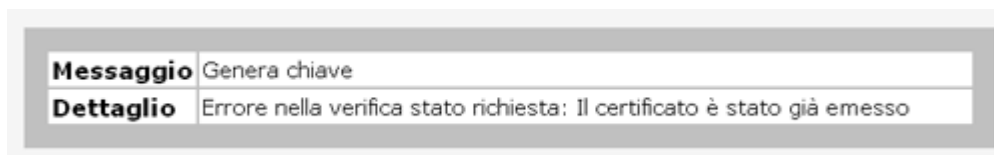
Dopo aver registrato il certificato di firma l'applicazione visualizza l'avvenuta conclusione dell'operazione nella figura che segue :

GENERAZIONE CHIAVE EFFETTUATA CON SUCCESSO!

Si evidenzia la necessità di eseguire immediatamente una copia del dispositivo di firma, e di conservarlo accuratamente.

In caso di smarrimento del certificato è necessario procedere come descritto al successivo paragrafo (Blocco chiave).

Nel caso in cui, in fase di generazione delle chiavi, venga emesso il seguente messaggio:



L'operazione di generazione del certificato si interrompe immediatamente poiché l'utente risulta già titolare di un certificato.

4 Copia dispositivo di firma

La funzione "Copia dispositivo di firma" consente di eseguire una o più copie del certificato di firma che contiene le chiavi dell'utente, protetti dalla medesima password. Si consiglia di effettuare le copie subito dopo l'avvenuta generazione.

Per eseguire l'operazione, selezionare nella seguente schermata il bottone "SI"

Copia Dispositivo di Firma

Eeguire una copia del dispositivo di firma ?

Si **No**

Per eseguire l'operazione, selezionare nella schermata il bottone "SI"

Copia Dispositivo di Firma

Avvio procedura copia dispositivo di firma

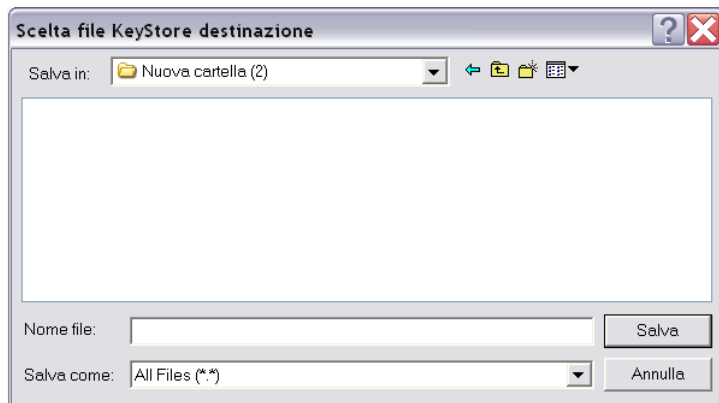
Procedi

Selezionare il bottone "Procedi"

Selezionare dalla finestra presentata il dispositivo su cui è registrato il certificato di firma, quindi selezionare "Apri".



Selezionare il percorso completo su cui si intende fare una copia del certificato e selezionare "Salva".



Viene quindi visualizzato il messaggio di operazione effettuata correttamente.

COPIA DEL DISPOSITIVO DI FIRMA
ESEGUITA CORRETTAMENTE

5 Blocco chiavi

La funzione ha lo scopo di bloccare l'utilizzo della chiave pubblica quando l'utente titolare non è più in grado di utilizzare il dispositivo di firma oppure teme che lo stesso venga indebitamente utilizzato da altri. A tal fine occorre selezionare la funzione dall'home page del servizio, ed inserire i dati richiesti:

- codice fiscale: codice fiscale del soggetto titolare del certificato
- PIN di revoca: numero del pin di revoca contenuto nella busta consegnata dall'ufficio al momento del censimento
- Numero postazione (o progressivo sede): 001
- Numero di autorizzazione: numero di registrazione attribuito durante la procedura di censimento dell'utente visualizzato sulla stampa dell'autorizzazione rilasciata dall'ufficio del territorio.

Blocco Chiavi

Codice fiscale	<input type="text"/>
PIN di revoca	<input type="text"/>
Postazione numero	<input type="text"/>
Autorizzazione numero	<input type="text"/>

Esegui **Ripristina**

Selezionare quindi il bottone “Esegui”.

Sulla base dei dati indicati, l'applicazione si connette automaticamente con il server di registrazione e controlla la congruenza dei dati da voi indicati con quanto memorizzato in fase di censimento dell'utente.

Nel caso in cui i controlli di verifica della congruenza dei dati forniti risultino negativi, viene emessa la segnalazione di errore seguente:

Messaggio	Blocco Chiavi
Dettaglio	Utente non autorizzato, verificare i parametri inseriti!

Nel caso in cui i controlli di verifica della congruenza dei dati forniti risultino positivi, viene emessa la schermata contenente i “dati utente” e i “dati certificato”:

Dati utente			
Codice fiscale		CommonName	
Organization	Agenzia del Territorio	Organization Unit	Servizi Telematici

Dati certificato			
Seriale Certificato		Authority Key Identifier	
Stato	EVASO	Data Emissione Certificato	29/09/2008

Blocco chiavi

Per confermare l'operazione di blocco delle chiavi è necessario che l'utente selezioni il bottone "Blocco chiavi".

Tale operazione non è "annullabile" va quindi eseguita esclusivamente in caso di effettiva necessità.

Successivamente viene emessa la schermata di conferma dell'avvenuto blocco delle chiavi:

BLOCCO CHIAVI EFFETTUATA CON SUCCESSO!

6 Errore imprevisto dalla CA

Nel caso in cui si dovessero verificare problemi di comunicazione tra il server dell'Amministrazione che contiene i dati di registrazione (RA Centrale) e il server che certifica la chiave pubblica (CA) potrebbe verificarsi l'emissione del 'Errore imprevisto dalla CA'.

Si consiglia in questo caso di ritentare più tardi la stessa operazione perché nel frattempo potrebbe essere stato risolto il problema; se il problema persiste sarà necessario segnalare il problema al servizio di assistenza.

7 Connection refused: no further information

Nel caso in cui si verificassero problemi di comunicazione con il sistema di certificazione dell'Amministrazione potrebbe essere emesso il messaggio d'errore "Connection refused: no further information". Il problema può dipendere dal fatto che l'accesso ad internet non è stato configurato correttamente

Si consiglia in questo caso di verificare la configurazione della connessione.