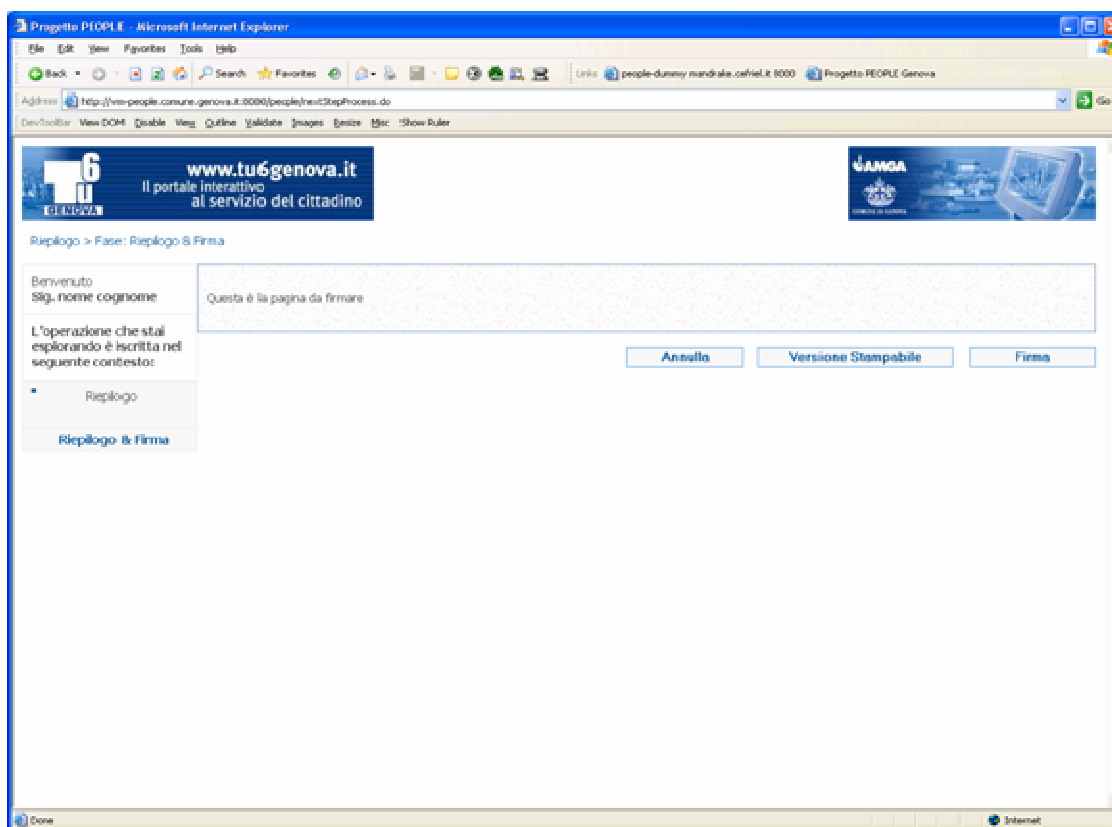
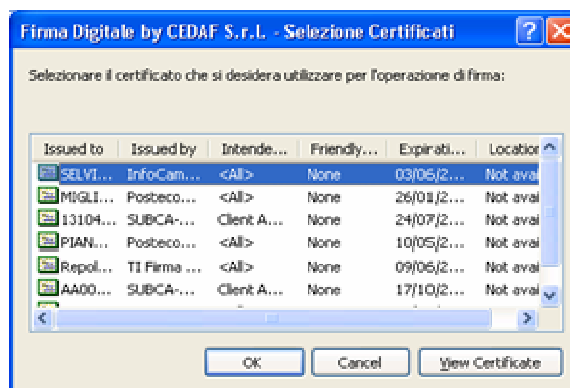


Linee guida per l'utilizzo della funzionalità di firma remota

Il processo di firma viene attivato nella pagina di riepilogo della pratica:

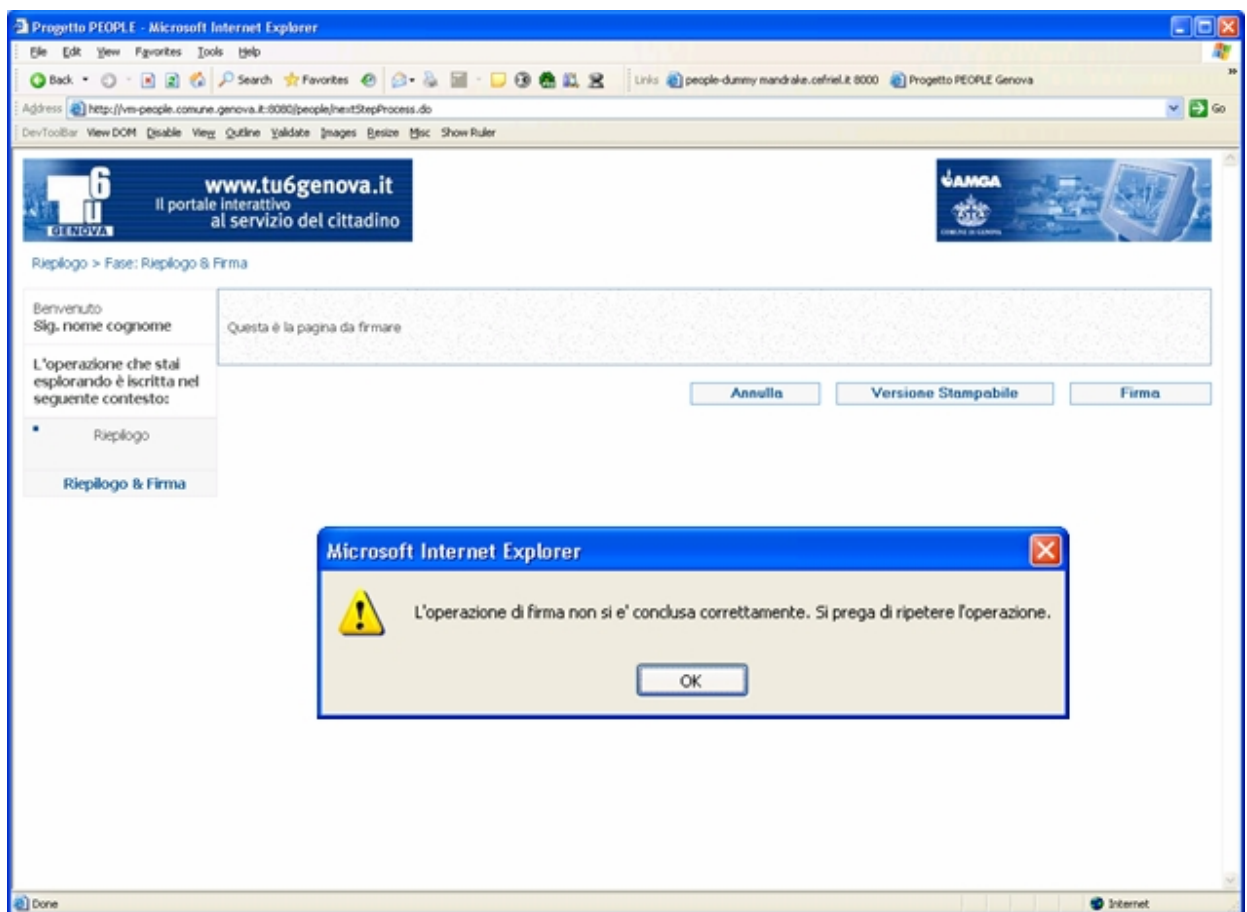


Cliccando sul pulsante 'Firma' viene visualizzato, ad opera del componente ActiveX di Firma Digitale, l'elenco dei certificati utilizzabili per la firma (alla prima esecuzione se il componente ActiveX non è installato all'utente verrà proposta automaticamente l'installazione):

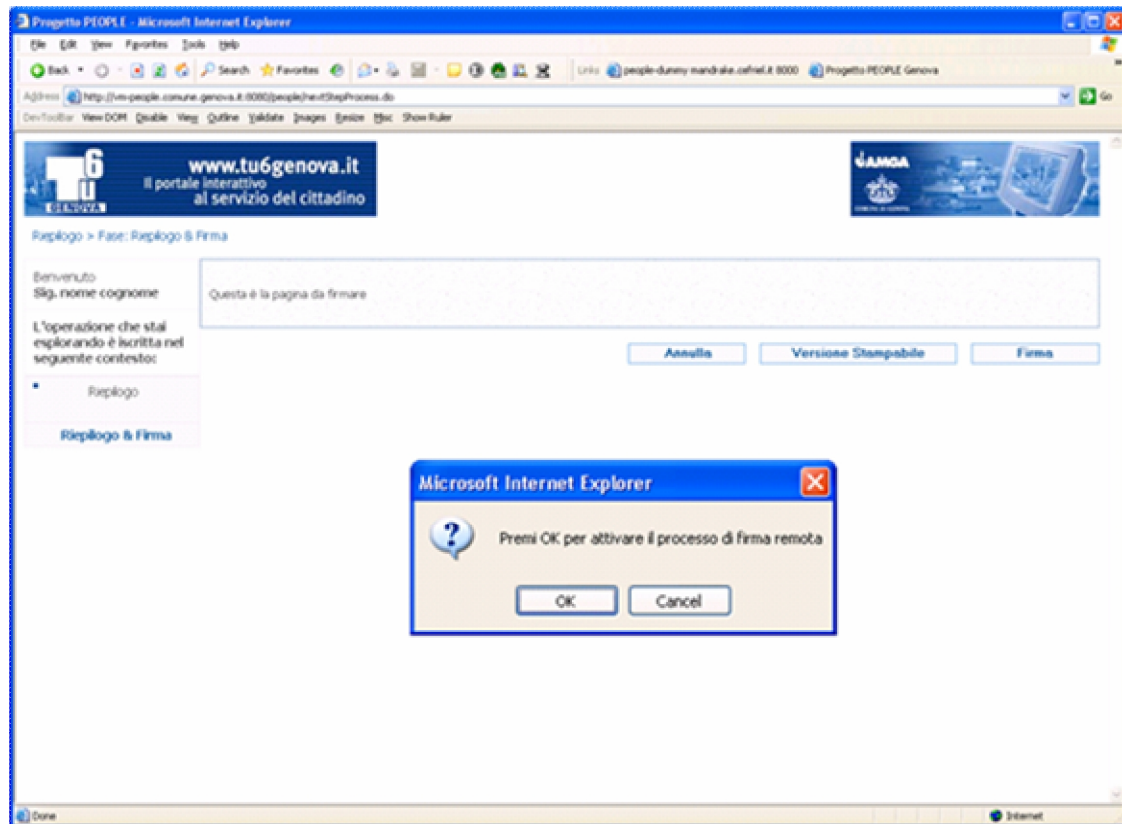


Per la firma su smartcard a questo punto basta selezionare il certificato corrispondente alla smartcard inserita nel lettore.

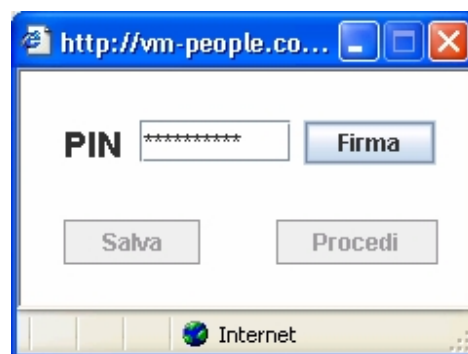
Nel caso si desideri invece utilizzare il servizio di firma remota erogato dalla CA-People del comune, quando questa finestra di dialogo viene visualizzata occorre premere 'Cancel' (o 'Annulla' se il sistema operativo è in versione italiana). Il risultato è la visualizzazione di un messaggio che indica il non corretto completamento dell'operazione di firma su smartcard:



Cliccando su 'OK' verrà visualizzata una seconda finestra di dialogo con la quale si può attivare il processo di Firma remota utilizzando il pulsante 'OK':

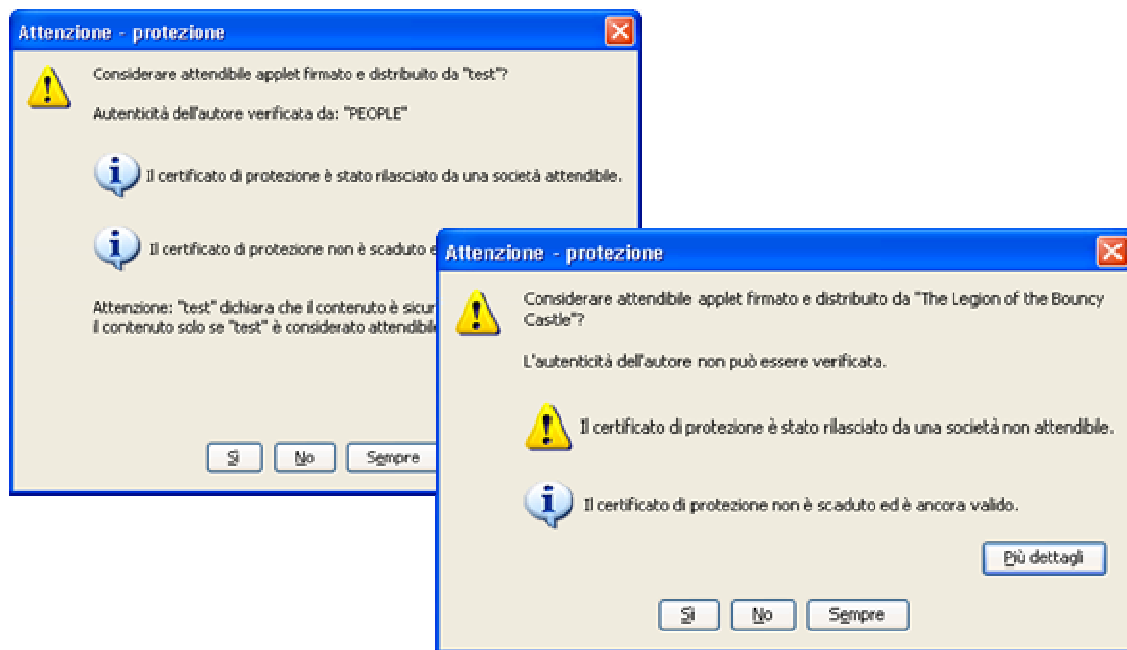


Premendo 'OK' il browser visualizzerà una finestra di dialogo secondaria per l'inserimento del PIN People che verrà utilizzato per validare la richiesta di firma remota:



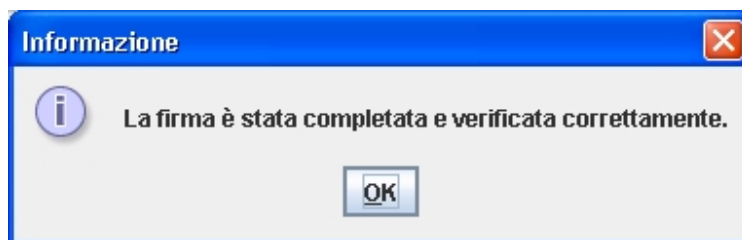
Nella finestra di dialogo è in esecuzione un'applet Java responsabile dell'interazione con il web service di firma remota messo a disposizione dalla CA-People di registrazione dell'utente. L'Applet trasmette in modo sicuro e cifrato il documento da firmare al web service di firma remota e ottiene come risultato dell'interazione il documento firmato digitalmente in formato .p7m.

Si noti che in fase di caricamento dell'applet di firma remota e delle relative librerie di supporto potranno essere visualizzati uno o più avvisi di protezione simili a quelli mostrati nella figura seguente:

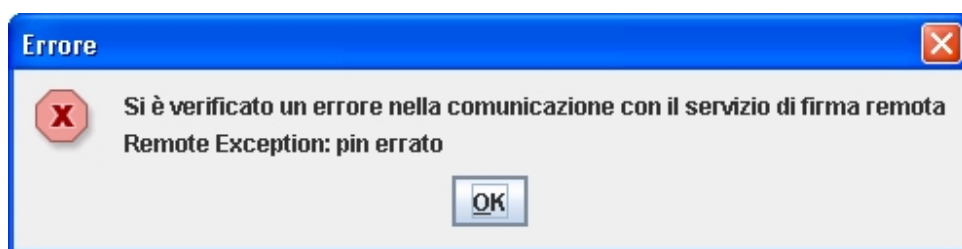


Se si è ragionevolmente sicuri dell'attendibilità dei certificati di protezione presentati si può premere 'Sì' o 'Sempre'. In questo modo sarà possibile eseguire le operazioni di firma remota (nel caso in cui si preme 'Sempre' l'avviso di protezione non verrà presentato in corrispondenza degli utilizzi successivi del componente di firma remota). Se non si è sicuri dell'attendibilità e/o si preme 'No' in corrispondenza anche di uno solo degli avvisi di protezione si fa presente che non sarà possibile utilizzare con successo le funzionalità di firma remota.

Alla prima esecuzione, analogamente a quanto accade per il componente di firma digitale su smartcard, se non è installata sul PC dell'utente la versione corretta della Java Virtual Machine all'interno della quale viene eseguita l'Applet Java, l'utente viene indirizzato automaticamente sul sito SUN per provvedere al download e installazione della Java Virtual Machine e successivamente procedere con l'operazione di firma remota. Il completamento positivo dell'operazione di firma remota così come gli eventuali errori verranno segnalati mediante la visualizzazione di opportune finestre di dialogo. La figura seguente mostra il messaggio visualizzato in caso di completamento con successo dell'operazione di firma remota:



Nel caso di errata immissione del PIN verrà invece visualizzato il seguente messaggio:



In caso di completamento positivo dell'operazione di firma, nella finestra utilizzata per l'immissione del PIN saranno utilizzabili due pulsanti, come mostrato nella figura seguente:



Il pulsante 'Salva' consente di salvare sul disco locale il documento firmato digitalmente, mentre il pulsante procedi consente di inviare il documento firmato digitalmente al portale del Comune erogatore del servizio e di completare il procedimento amministrativo:

