

Download ed Installazione del Software di Firma Digitale

1. Download del Software

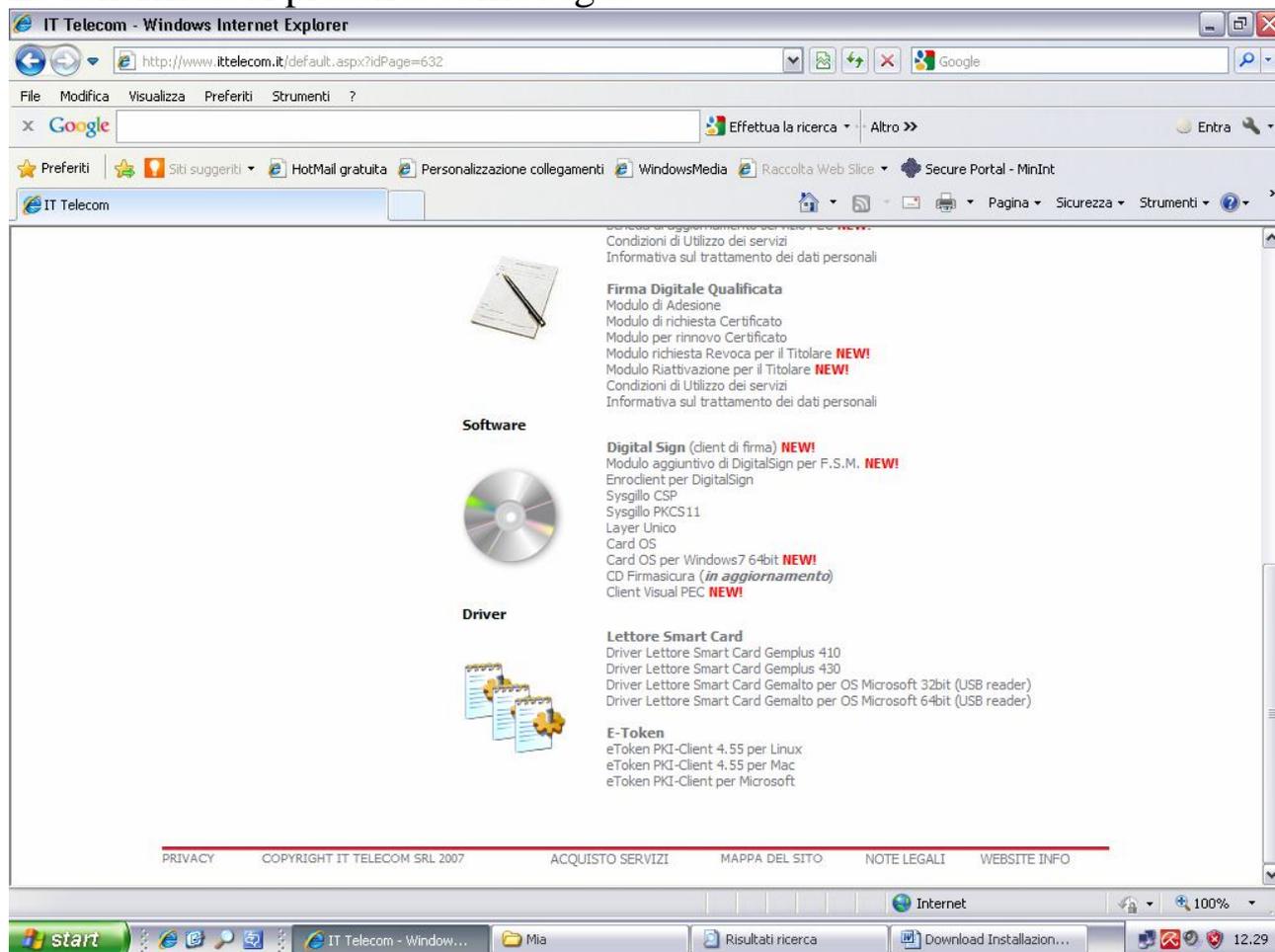
Il software necessario è disponibile sul sito
<http://www.ittelecom.it/default.aspx?idPage=632>

Le componenti da installare sono **3** :

- 1. driver del lettore di Smart Card GEMALTO*
- 2. driver della Smart Card*
- 3. programma di firma digitale*

1) Installazione del lettore di Smart Card GempcTwin

La schermata si presenta come segue



Scorrendo la pagina verso il basso, nella sezione “**Driver**” installare il driver per il lettore di Smart Card fornito, *previa verifica del Sistema Operativo della postazione di lavoro.*

I driver per gli **OS a 32 bit** sono disponibili facendo click su “**driver lettore Smart Card Gemalto per OS Microsoft 32 bit (USB reader)**”

I driver per gli **OS a 64 bit** sono disponibili facendo click su “**driver lettore Smart Card Gemalto per OS Microsoft 64 bit (USB reader)**”



IT Telecom S.r.l.

Se si effettua la selezione per i Sistemi Operativi a 32 bit si presenta la finestra che segue



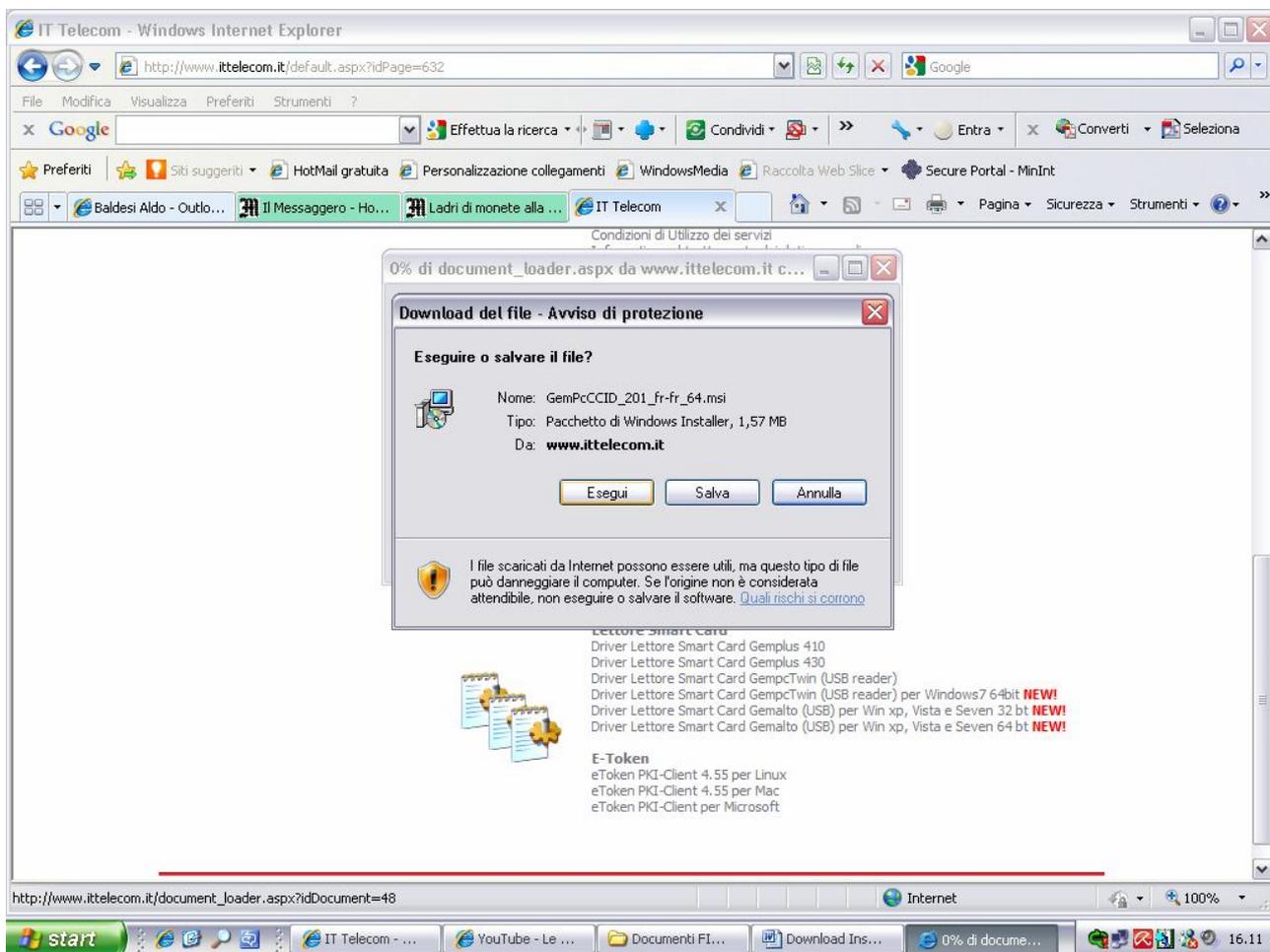
Salvare localmente il file compresso “**gempctwin.zip**” che, una volta estratto, creerà automaticamente la cartella “**gempctwin**”.

Aprire la cartella ed eseguire il file, “**GemPCTwin PC_SC Installer.exe**”.

Non è necessario, durante la procedura di installazione, cambiare nessuno dei parametri proposti, a meno di esigenze particolari dell'utente.

Alla fine dell'installazione sarà possibile inserire il lettore in una qualsiasi presa USB e la periferica deve essere correttamente riconosciuta dal sistema operativo

Se si effettua la selezione per i Sistemi Operativi a 64 bit occorre eseguire l'installazione che viene proposta come da immagine seguente



Seguire la procedura di setup sino alla fine, accettando le condizioni di uso e tutte le impostazioni proposte di default.

2) Installazione del driver della Smart Card

Importante : la seguente sezione è valida sia per postazioni di lavoro con Sistemi Operativi a 32bit che a 64bit

Nella sezione “**Software**”, fare click su “**CardOS**”

Si presenta la finestra che segue



Fare click su “**Salva**” e scegliere il percorso locale del file da scaricare.

Il risultato sarà il download del file compresso “**SETUP_CA_SMOC.....**”

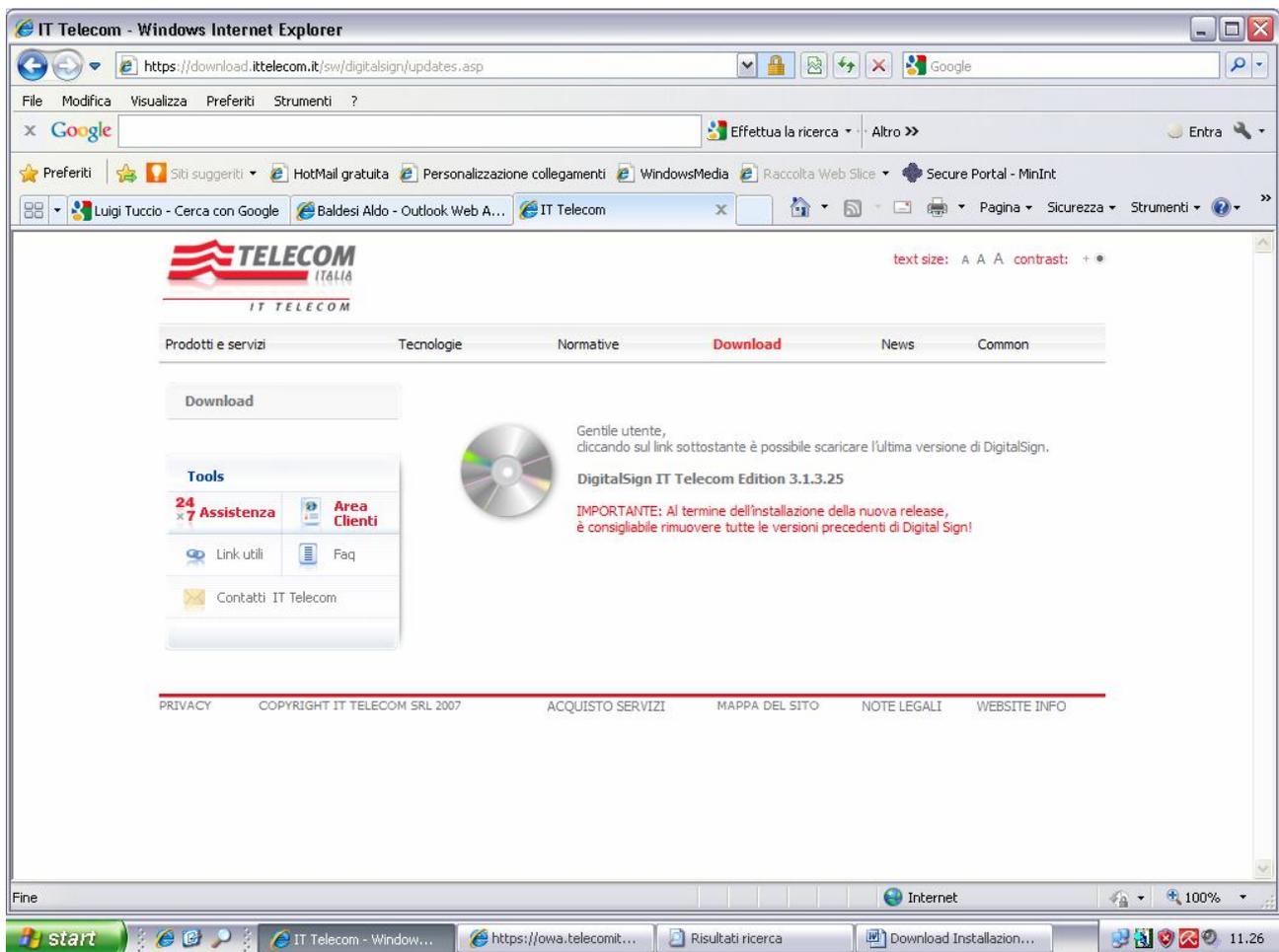
Effettuare la decompressione del file, ottenendo la cartella “**SETUP_CA_SMOC.....**”,

Una volta aperta, fare doppio click sul file “**Setup**”, che avvierà la procedura di installazione.

Anche qui, a meno di particolari esigenze dell'utente, non occorre cambiare le impostazioni proposte dalla procedura automatizzata.

3) Installazione del programma di Firma Digitale, DigitalSign IT Telecom Edition

Il programma è disponibile all'indirizzo <https://download.ittelecom.it/sw/digitalsign/updates.asp>, che si presenta come segue



Facendo click sul collegamento **“DigitalSign IT Telecom Edition....”** si scarica il file di Setup.

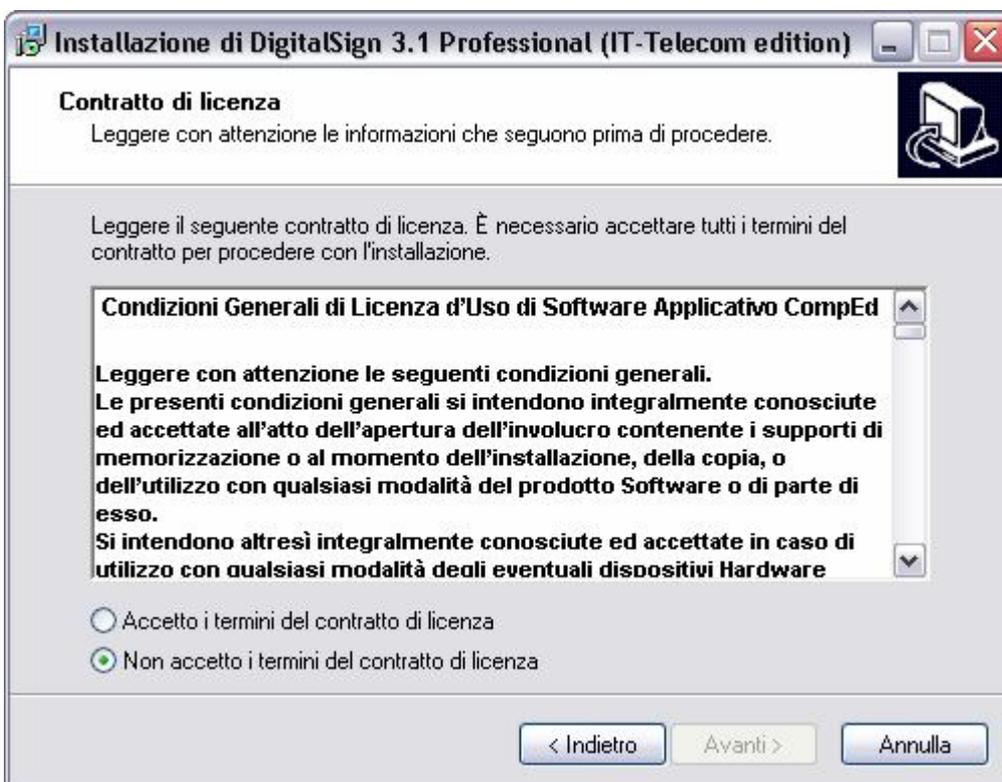
Al termine del download viene proposta la seguente finestra Nella quale selezionare il pulsante **“Esegui”**



A questo punto viene avviato lo wizard di installazione con la seguente schermata



Fare Click su **“Avanti”**

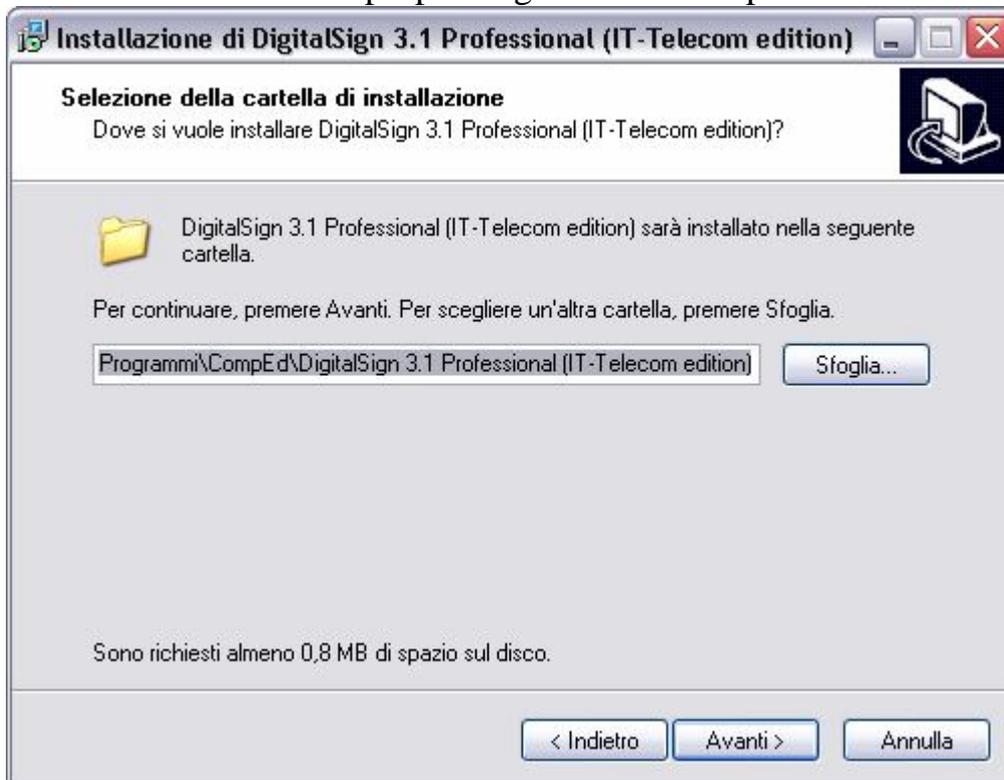


Selezionando **“Accetto i termini del contratto di licenza”**, viene abilitato il tasto **“Avanti”**.

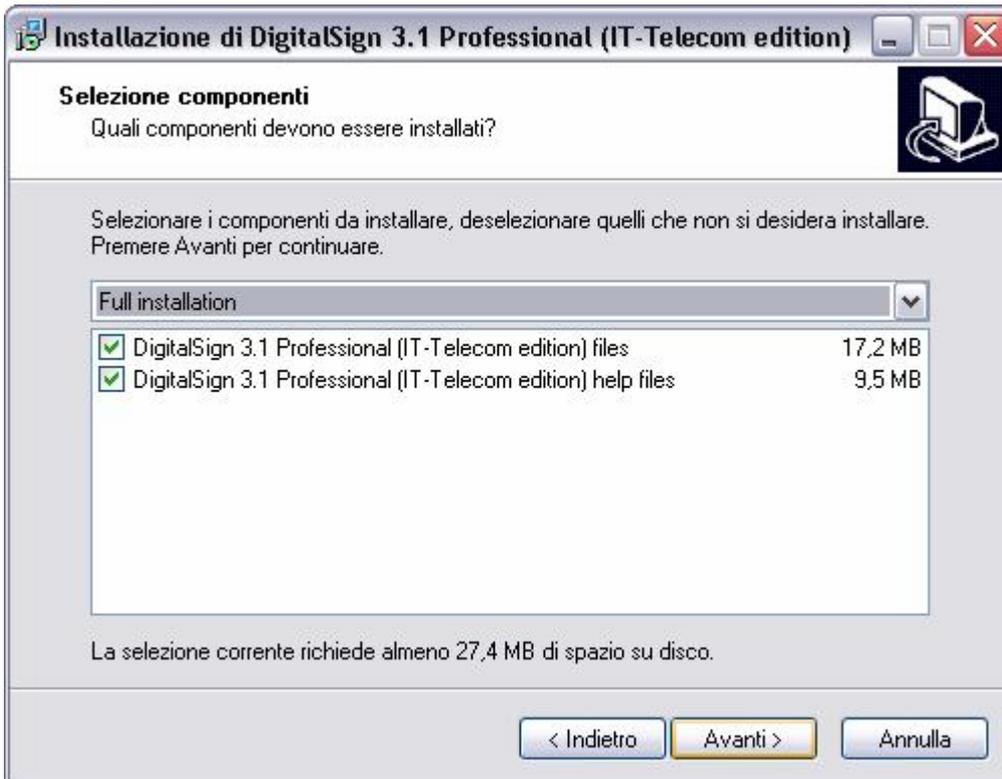
Fare Click su **“Avanti”**



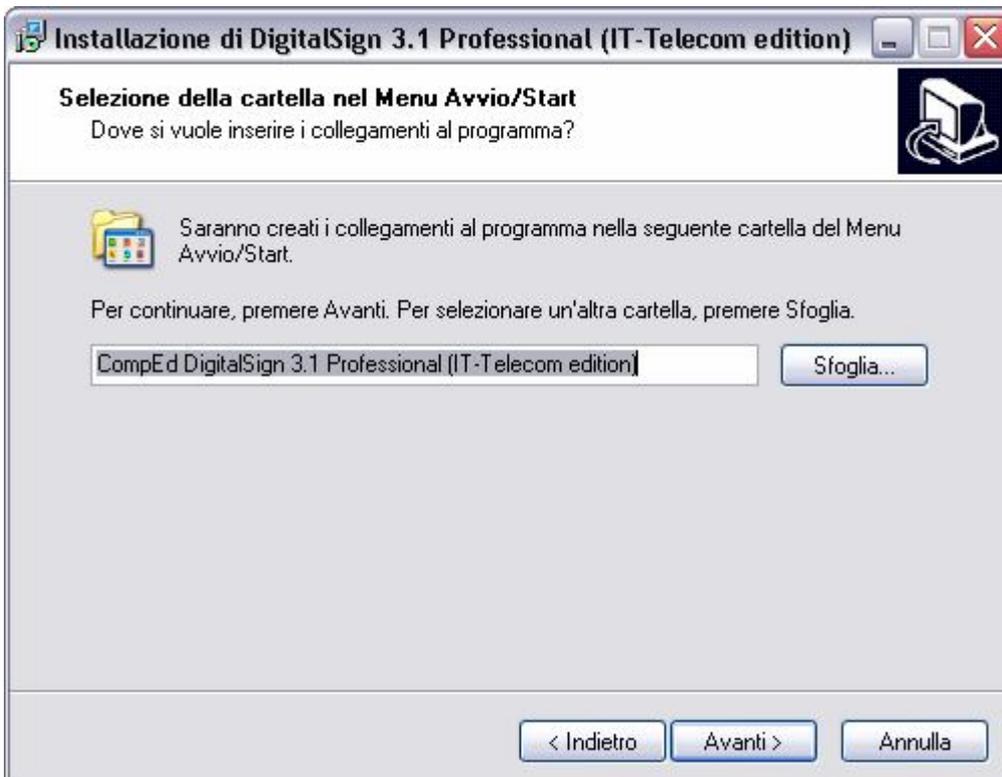
Nel campo **“Nome”** si può immettere il proprio nome mentre nel campo **“Società”** immettere la propria organizzazione e premere **“Avanti”**



Fare Click su **“Avanti”**



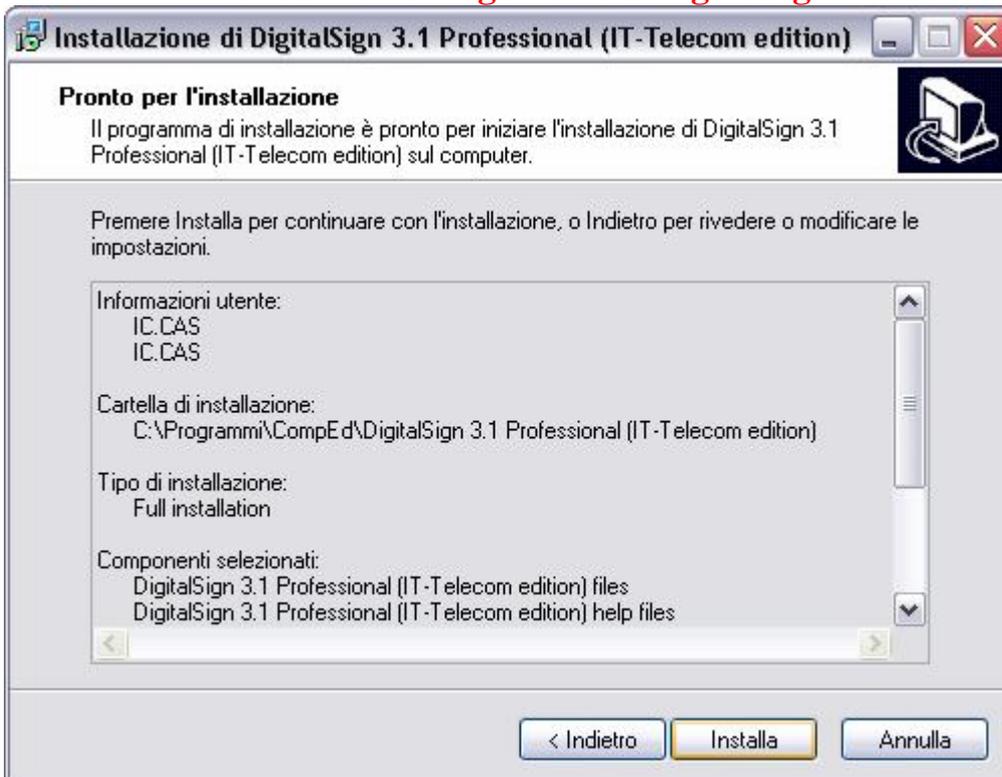
Fare Click su **“Avanti”**



Fare Click su **“Avanti”**



Fare Click su **“Creare un collegamento a DigitalSign”**



Fare Click su **“Installa”**



Fare Click su **“Fine”**

DigitalSign[®] IT Telecom Edition

Configurazione Post Installazione

Le personalizzazioni da effettuare rispetto ai default dell'installazione di DigitalSign sono, brevemente, le seguenti :

- 1. Impostazione Connessione Internet**
- 2. Verifica CRL (Certificate Revocation List)**
- 3. Verifica CA (Certification Authorities) accreditate / attendibili**
- 4. Configurazione Marcatura Temporale**
- 5. Rimozione della Precedente versione di DigitalSign**

1) Impostazione Connessione Internet

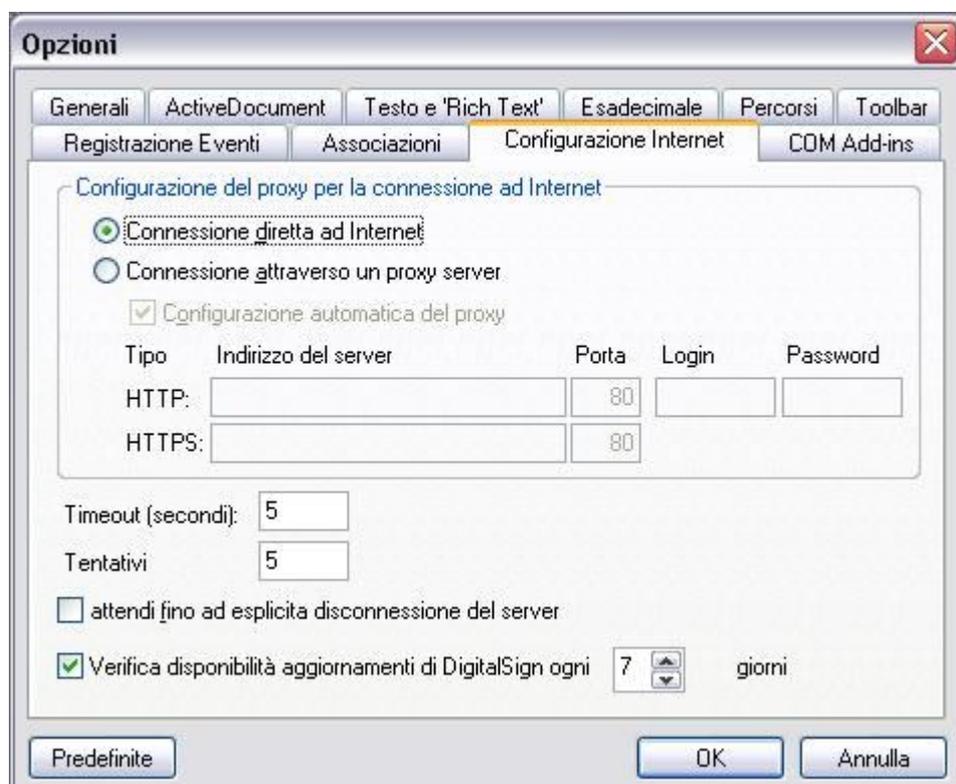
La connessione Internet è indispensabile a DigitalSign per effettuare dei controlli, non previsti di default, che per maggior sicurezza dell'utente riteniamo utile attivare.

Questa è la finestra che con i parametri di configurazione della Connessione Internet.

Fare **“Click”**

Strumenti => Opzioni

Selezionare il Tab **“Configurazione Internet”**



Fare **“Click”** sulla selezione **“Connessione attraverso un Proxy Server”**

Fare **“Click”** su **“OK”**

Una volta fatto lo switch della modalità di connessione, il programma necessita dell'indirizzo del proxy di accesso ad Internet e delle eventuali credenziali (user e password).

DigitalSign le può ottenere automaticamente, dalle impostazioni di Internet Explorer o di un eventuale altro browser predefinito.

In alternativa si possono impostare manualmente, digitandole nei campi HTTP, Porta, Login e Password.

2) Verifica CRL (Certificate Revocation List)

Il programma può attivare, rispetto alle impostazioni di default, il controllo sullo stato di validità dei certificati di firma, ovvero che i certificati di Firma non siano stati revocati o sospesi.

Per farlo deve consultare delle liste, le CRL, pubblicate su Internet dalle Certification Authorities.

Per l'impostazione fare **“Click”** su **Strumenti => Opzioni di Security**

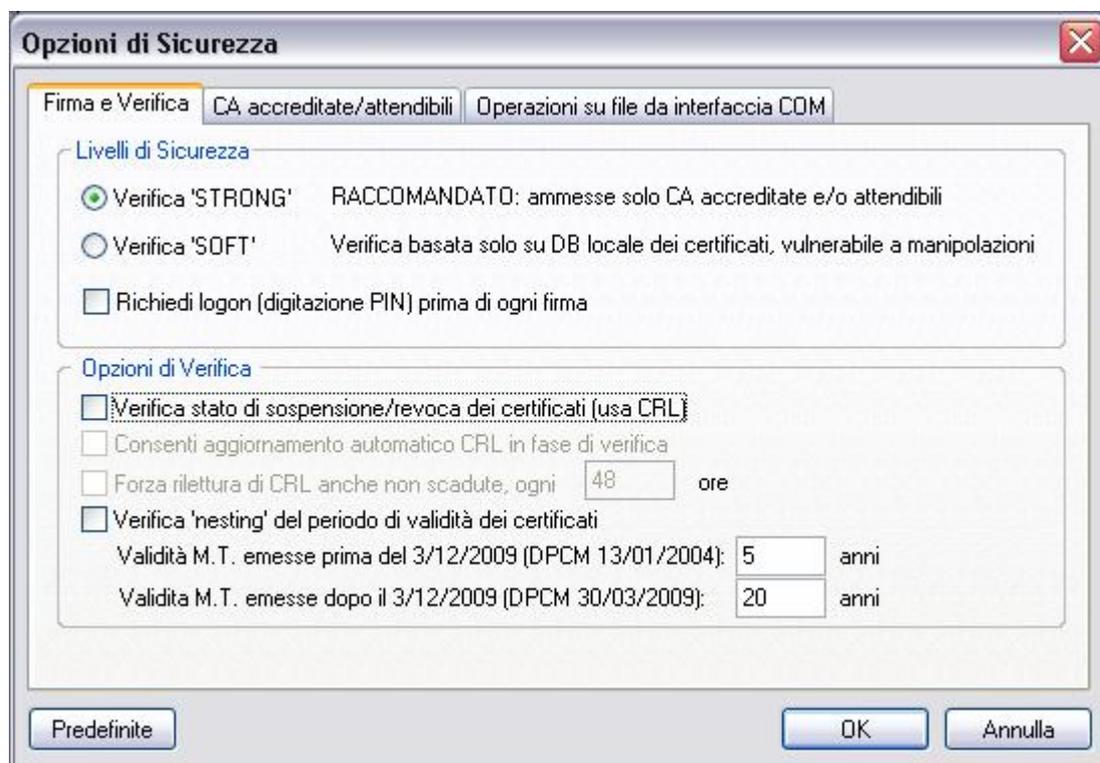
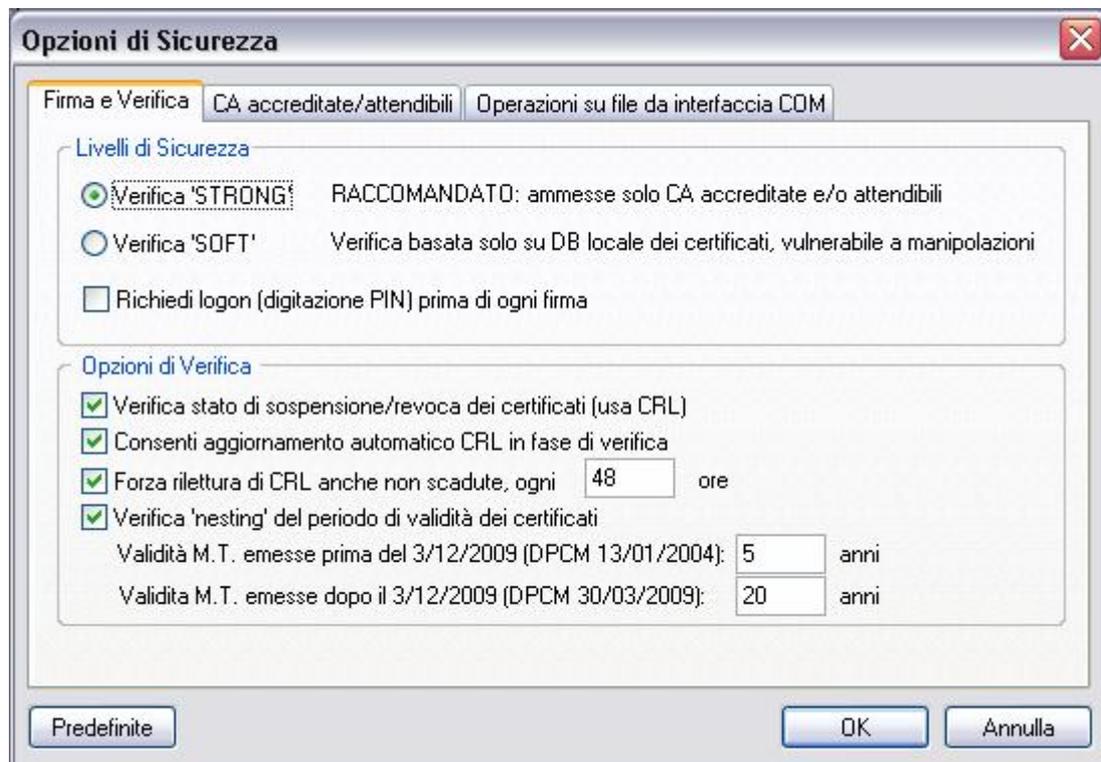


Fig. 8

Nel riquadro **“Opzioni di Verifica”**, selezionare, ***partendo dalla prima***, le 4 checkbox, sotto la dicitura **“Opzioni di Verifica”**.

Questo è il risultato dell' operazione

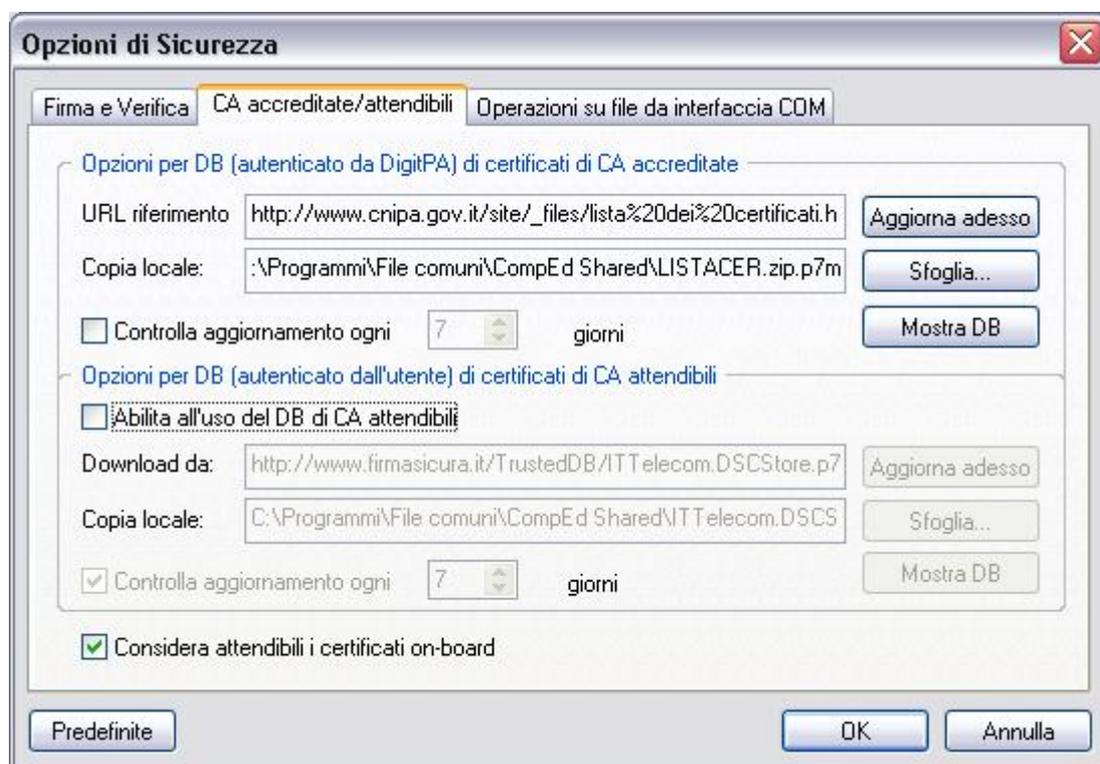


3) Verifica CA (Certification Authorities) accreditate / attendibili

Per maggior sicurezza è possibile attivare un ulteriore controllo sui certificati di Firma Digitale attivando la verifica dell'accREDITamento del Certificatore (Ente che emette il Certificato di Firma Digitale) presso il CNIPA, Centro Nazionale Informatico per la Pubblica Amministrazione.

E' possibile gestire un'ulteriore lista di Certificatori, non accreditati presso il CNIPA, ma ritenuti comunque attendibili da IT Telecom.

Per configurare queste opzioni fare **“Click”** su **Strumenti => Opzioni di Security**
Selezionare il Tab “CA accreditate / attendibili”.



Attivare la checkbox **“Controlla aggiornamenti ogni giorni “.**

Il valore di default, 7 giorni, per l'intervallo di aggiornamento, si può lasciare invariato.

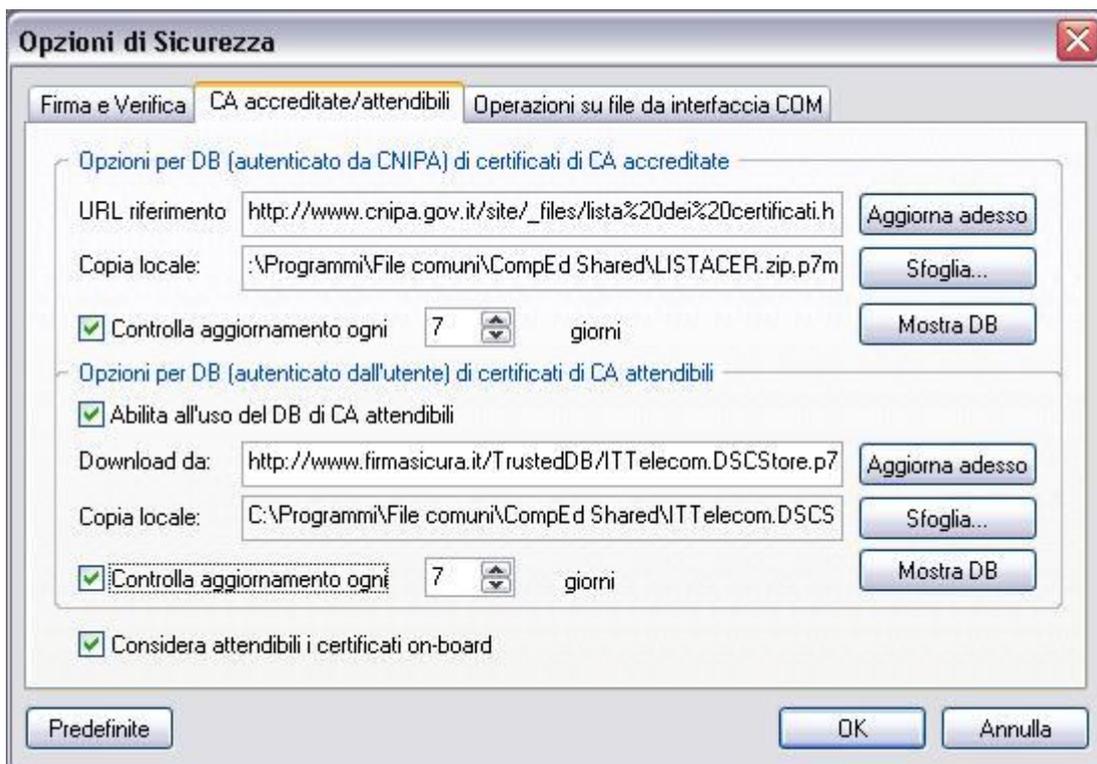
Attivare la checkbox **“Abilita all'uso del DB di CA attendibili“.**

A questo punto viene resa disponibile una seconda checkbox

“Controlla aggiornamenti ogni giorni “, occorre abilitare anche questa

Il valore di default, 7 giorni, per l'intervallo di aggiornamento, si può lasciare invariato.

Questo il risultato dell'operazione.



4) Configurazione del servizio di Marca Temporale

IMPORTANTE:

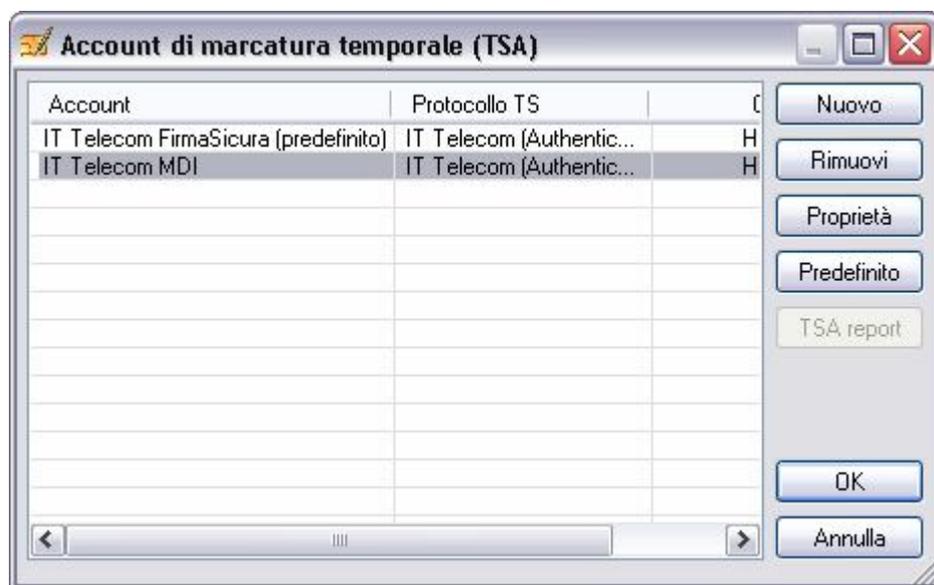
questa sezione è per i soli clienti che hanno acquistato il servizio di Marcatura Temporale. Da non considerarsi per gli altri utenti.

Aprire un documento da marcare temporalmente
Selezionare, dal menù “Documento”, la voce “Marca Temporale”

Apparirà la seguente finestra



Fare Click su **“Configurazione”**



Fare Click sull’account **“IT Telecom MDI”** e successivamente sul pulsante **“Rimuovi”**

A questo punto fare Click sul pulsante **“Proprietà”**



Inserire nel campo **“Nome Logon”** il proprio Codice Utente, presente nella busta oscurata che contiene il PIN della Firma Digitale.

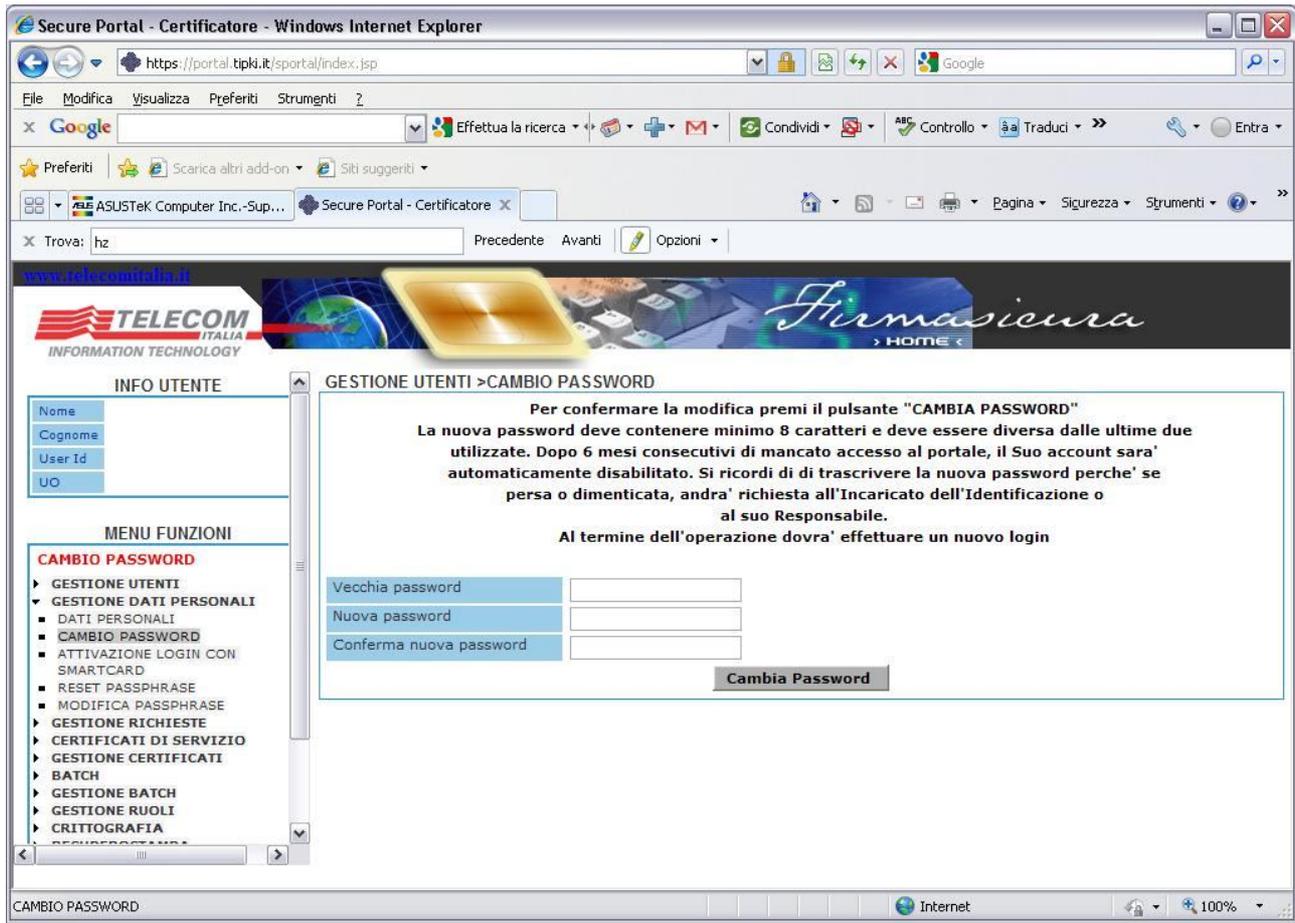
Collegarsi al sito

<https://portal.tipki.it/accessportal/control/InitService?reame=Certificatore&authMode=LightLogin>

Immettere nel campo **“Codice Utente”** il valore del campo **“Utente”** della busta oscurata che contiene il PIN della Smart Card

Immettere nel campo **“Password”** il valore del campo **“Password”** della busta oscurata che contiene il PIN della Smart Card

Fare click su **“Entra”**



Immettere di nuovo nel campo **“Vecchia Password”** la password presente nella busta oscurata.

Nel campo **“Nuova Password”** immettere una propria password tenendo conto delle informazioni evidenziate nella schermata.

Nel campo **“Conferma Nuova Password”** immettere di nuovo la password appena creata.

A questo punto inserire la password creata nella schermata precedente di DigitalSign, che per comodità riportiamo qui sotto.



A questo punto fare click su **“OK”**, di nuovo click su **“OK”** e selezionare **“Applica Timestamp”**

L’operazione fatta finora è da eseguirsi solo una volta, nella fase di configurazione del servizio.

Le volte successive sarà sufficiente fare click sul menù “Documento”, selezionare “Marca Temporale”, quindi “Applica Timestamp”.

5) Rimozione della precedente versione di DigitalSign

Accedere al Pannello di Controllo del Sistema Operativo ed accedere alla sezione di gestione Applicazioni/Programmi.

Nella finestra che si aprirà, simile a quella qui di seguito, verificare l'eventuale presenza di più versioni di DigitalSign.

Se si verifica questa condizione fare “Click” sulla versione più datata, *riconoscibile da un codice di versione numericamente inferiore* e di seguito sul pulsante **“Rimuovi”**

