

# SUAPPiemonte

## Prerequisiti tecnici e modalità di configurazione della postazione di lavoro

### STATO DELLE VARIAZIONI

Versione	Paragrafo o Pagina	Descrizione della variazione
V01	Tutto il documento	Versione iniziale del documento
V02	§ 2.2	Aggiunta Nota 2 in relazione ai certificati di autenticazione rilasciati da Postecom
	§ 4	Redazione intero paragrafo sui software aggiuntivi
V03	§ 2	Aggiunta della possibilità di accesso a SUAPPiemonte con username/password e PIN (o CIP)
	§ 2.1	Aggiunta delle modalità di impostazione dell'opzione "Chrome PDF Viewer" nel browser Chrome.
	§ 2.2	Adeguamento della prima parte del paragrafo a seguito dell'aggiunta dell'accesso a SUAPPiemonte con username/password e PIN (o CIP) è stato modificato
	§ 2.3	Introduzione del nuovo paragrafo "Accesso tramite username / password e PIN (o CIP)"
V04	§ 2.1	Aggiunta la compatibilità di SUAPPiemonte con il sistema Operativo Macintosh (Mac OS X)

## Sommario

1	Premessa.....	3
2	Prerequisiti per l'utilizzo del sistema SUAPPiemonte .....	3
2.1	Browser e sistemi operativi .....	4
2.2	Certificato di autenticazione e di firma digitale .....	8
2.2.1	Kit di firma digitale.....	10
2.3	Accesso tramite username / password e PIN (o CIP).....	15
3	Istruzioni utili unicamente ai funzionari della Pubblica Amministrazione (Comuni, ASL, Province, etc.) .....	16
3.1	Certificato di autenticazione personale rilasciato da CSI-Piemonte .....	16
3.1.1	Mozilla Firefox .....	16
3.1.2	Internet Explorer .....	18
3.1.3	Google Chrome .....	18
4	Software aggiuntivi .....	20
4.1	Software per la trasformazione dei documenti nel formato PDF/A.....	20
4.2	Software per lettura documenti firmati digitalmente .....	20

## 1 Premessa

**SUAPPiemonte** consente la gestione interamente telematica della domanda, nel rispetto dei requisiti del DPR 160/2010, dalla presentazione della pratica a carico del richiedente alla gestione della stessa a carico dell'ufficio SUAP e degli Enti terzi coinvolti nell'istruttoria.

E' frutto dell'adattamento di una soluzione applicativa esistente, denominata SPORVIC2, selezionata all'interno del catalogo DigitPA sulle soluzioni messe a riuso e sviluppata in origine per il Distretto del Cuoio della Regione Toscana, con capofila il Comune di Castelfranco di Sotto.

Sono stati realizzati gli interventi di base necessari a rendere fruibile il software all'arete dei SUAP Piemontesi. Sono in corso altri interventi di implementazione/miglioramento delle funzionalità presenti.

E' a disposizione di tutti i SUAP Piemontesi ed è integrato con la **Base Dati della Conoscenza Regionale**, sviluppata da Regione Piemonte, realizzata al fine di:

- uniformare e rendere trasparenti le informazioni ed i procedimenti concernenti l'insediamento e l'esercizio di attività produttive;
- mettere a disposizione delle imprese e dei SUAP, in relazione ai singoli procedimenti, l'indicazione della normativa applicabile, degli adempimenti procedurali, della modulistica, nonché dei relativi allegati, da utilizzare uniformemente nel territorio regionale.

Viene dato così pieno adempimento al mandato di semplificazione, standardizzazione e uniformazione dei processi della PA, definendo prassi unificate di interazione dei SUAP nei confronti degli Enti Terzi e viceversa.

Nel seguito si riportano i prerequisiti necessari per l'utilizzo del sistema **SUAPPiemonte**. Questi derivano dalle scelte effettuate originariamente nella realizzazione di SPORVIC2 presa a riuso, ed in particolare quella di non imporre all'utente l'acquisto di alcun software sottoposto a licenza, richiedendo soltanto di disporre sulla propria postazione di lavoro di software ausiliari Open Source, gratuitamente scaricabili da Internet (ad eccezione del kit di autenticazione e firma digitale richiesto dalla normativa vigente).

Progressivamente, Regione Piemonte potrà effettuare degli interventi atti a garantire il funzionamento del sistema anche con altri sistemi software proprietari.

## 2 Prerequisiti per l'utilizzo del sistema SUAPPiemonte

La postazione di lavoro di tutti gli utenti deve possedere:

- Uno tra i seguenti web browser:
  - Mozilla Firefox 9.0 e successivi (<http://www.mozilla.org/it/firefox/new/>) (**consigliato**)
  - Internet Explorer 9.0 (la versione 8 non funziona per incompatibilità)
  - Chrome 15.0 e successive (<https://www.google.com/chrome>)
- **Certificato di autenticazione digitale personale**, installato sulla Chiavetta USB<sup>1</sup> o sulla smart card<sup>2</sup>, o in alternativa **username, password e PIN (o CIP)** ottenuti mediante la regi-

<sup>1</sup> Occorre che siano installati correttamente funzionanti sulla postazione di lavoro dell'utente driver della CNS forniti

strazione dell'utente su Torinofacile (<http://www.torinofacile.it/registrazione/>) oppure su Sistemapiemonte (<http://www.sistemapiemonte.it/registrazione/index.shtml>)

- Certificato di firma digitale;
- Open Office 3.3 e successivi (<http://it.openoffice.org/>) o in alternativa Libre Office (<http://www.libreoffice.org/>)
- Adobe Reader versione più recente disponibile (<http://www.adobe.com/it/>).

Tutti questi moduli sono gratuiti, scaricabili da Internet o forniti con il kit di firma digitale, fatta eccezione per **username, password e PIN (o CIP)** che gli utenti ottengono a seguito della registrazione utente.

## 2.1 Browser e sistemi operativi

I browser sui quali sono stati effettuati sufficienti test sono quelli maggiormente diffusi e disponibili gratuitamente sulla rete Internet: Mozilla Firefox e Google Chrome.

### browser supportati:

- Internet Explorer 9 (sufficientemente garantito da test interni su sistema Windows XP SP3 e Windows Vista)
- Chrome 15.0 e successive (<https://www.google.com/chrome>)
- Mozilla Firefox 7.0 e successivi (<http://www.mozilla.org/it/firefox/new/>)
- Firefox Portable - in caso non siate amministratori della macchina si potrebbe scaricare una versione portable del browser - ([http://portableapps.com/apps/internet/firefox\\_portable](http://portableapps.com/apps/internet/firefox_portable))

### browser non supportati:

- Internet Explore 8: è stato provato, sono state trovate incompatibilità con il software quindi è consigliato non utilizzare questa versione.

### I sistemi operativi sui quali sono stati effettuati sufficienti test sono:

Windows 2000

Windows 7

Windows XP

Windows Vista

Macintosh (Mac OS X)

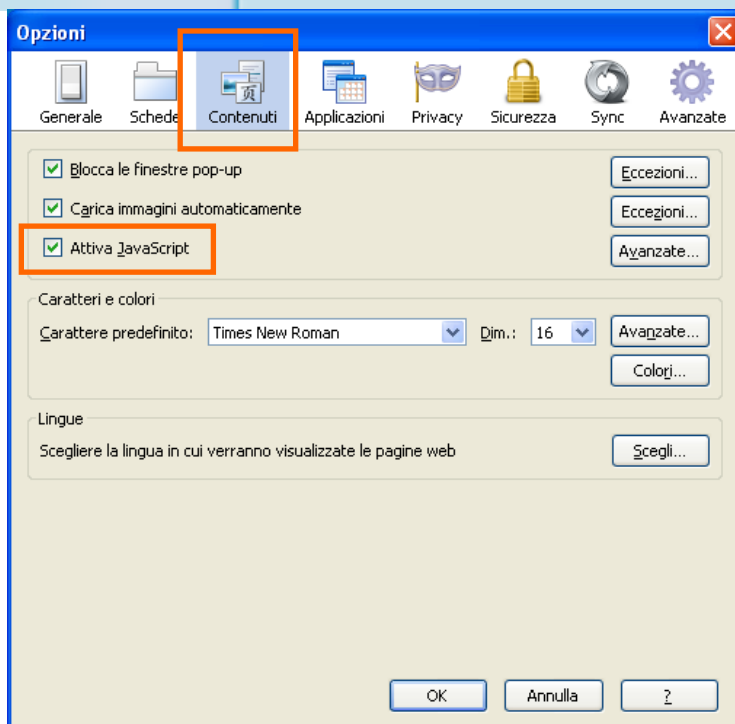
**IMPORTANTE:** su ogni browser utilizzato verificare che siano **attivati i Java Script**. Il possibile malfunzionamento dei Menù a tendina e dei pulsanti della componente applicativa web, può dipendere dall'attivazione o meno dei Java Script.

Per attivare i Java Script su **FireFox** da **Strumenti => Opzioni => Contenuti**.

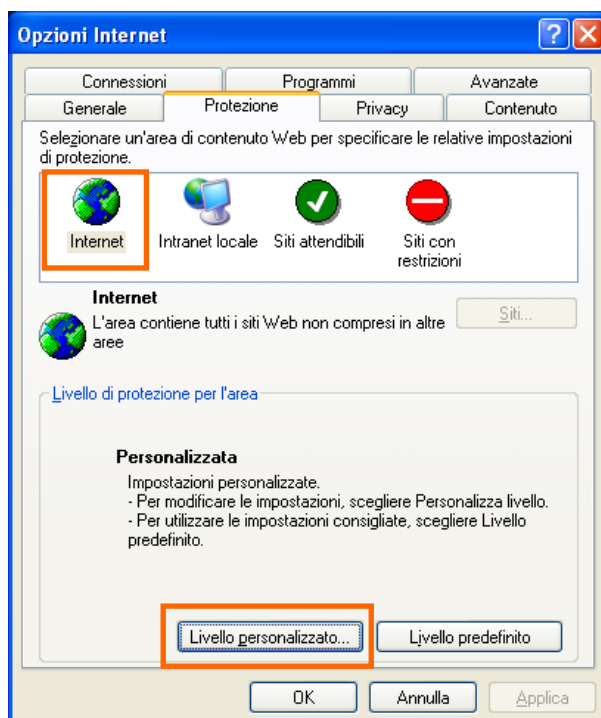
---

insieme alla Chiavetta USB da parte dell'Ente Certificatore.

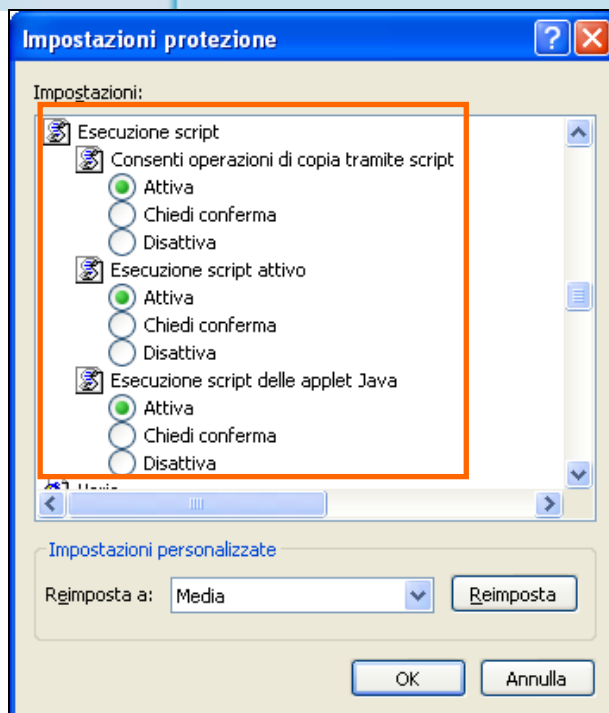
<sup>2</sup> Occorre che il lettore di Smart card sia correttamente installato e funzionante sulla postazione dell'utente, con anche i driver della CNS forniti insieme alla carta da parte dell'Ente Certificatore



Per attivare i Java Script su **Explorer** da **Strumenti** => **Opzioni Internet** => **Protezione** selezionare **Internet** e premere il pulsante **Livello personalizzato**



Nella finestra delle **Impostazioni di protezione**, circa a metà dell'elenco, attivare **tutte** le esecuzioni script proposte.



Quindi confermare e chiudere con **OK** tutte le finestre aperte.

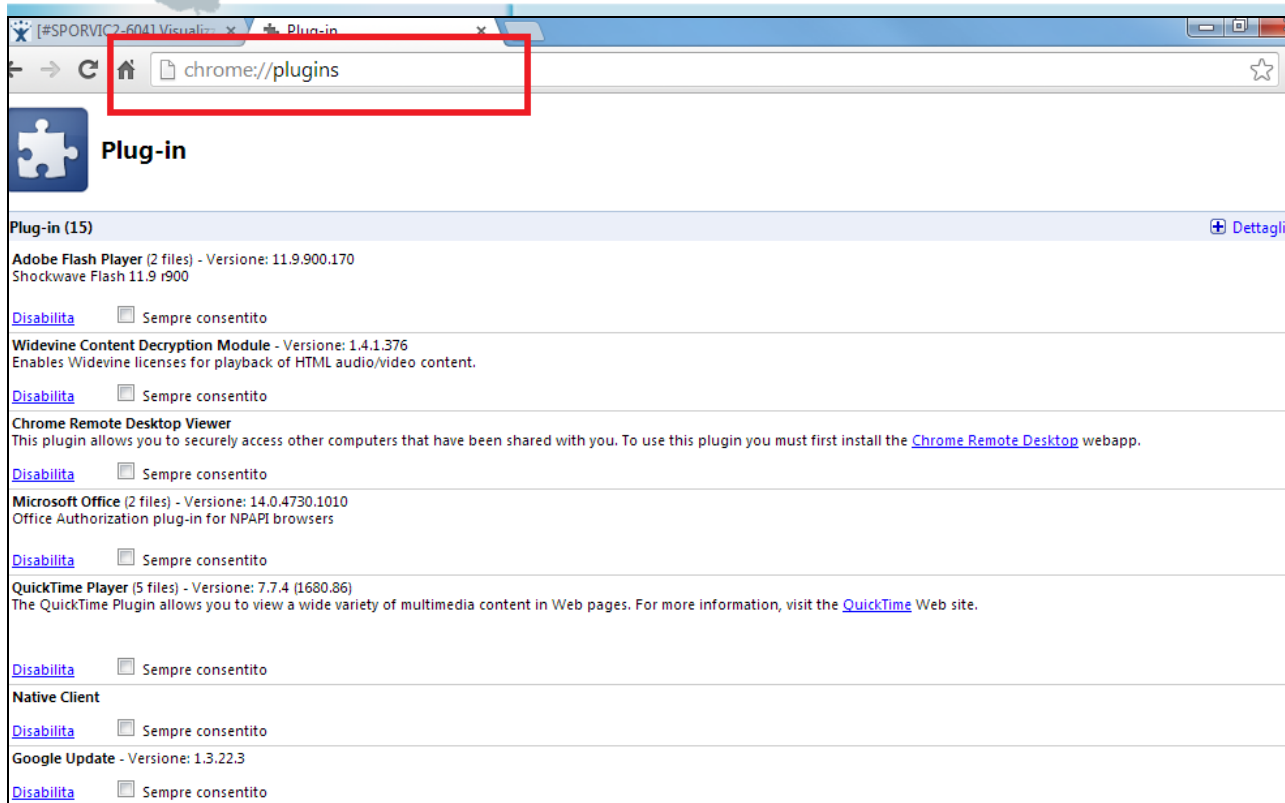
Per attivare i Java Script su **Chrome** da **Strumenti => Opzioni => Roba da smanettoni => Impostazioni contenuti dentro privacy**.



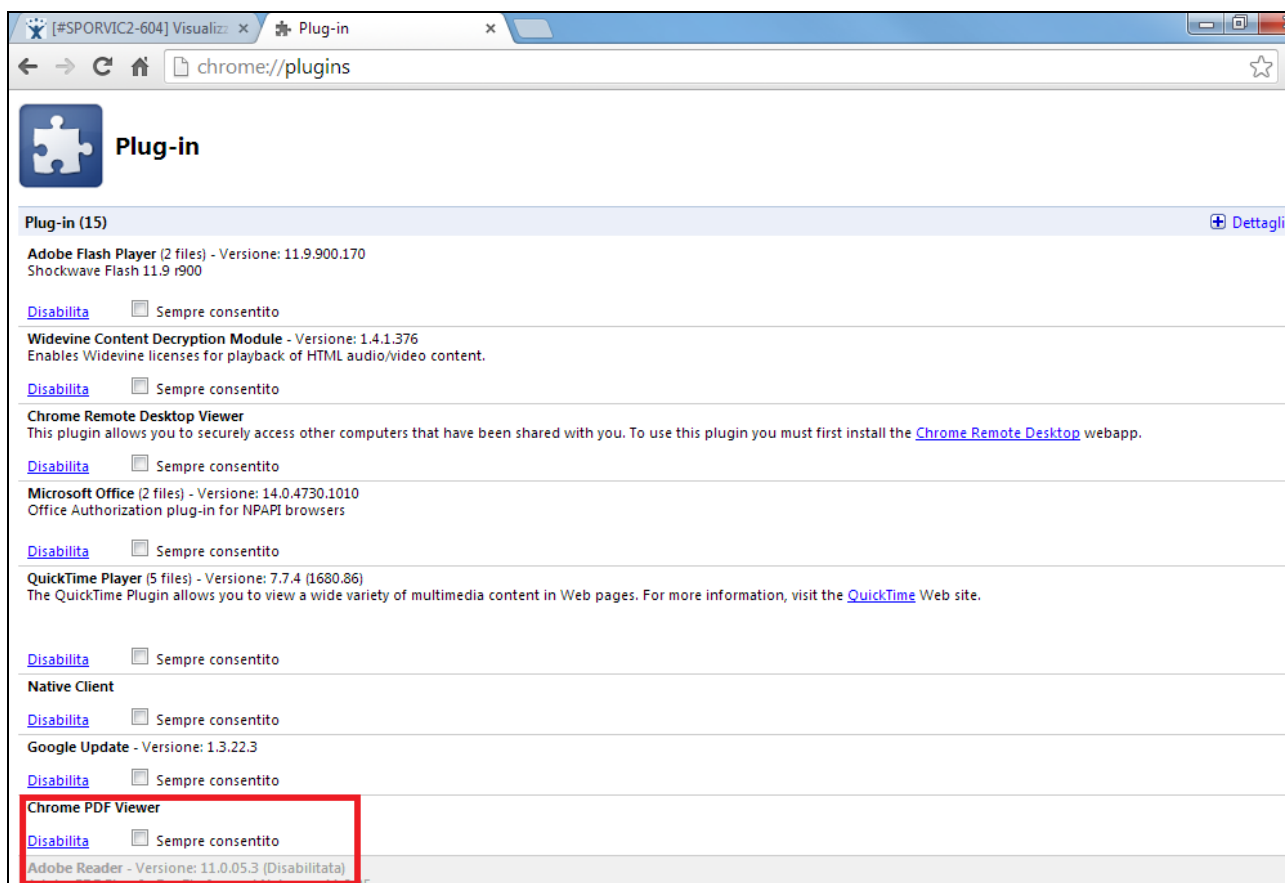
Dentro **Impostazione contenuti** si trova la sezione dei Javascript per poterli abilitare.

Su **Chrome** è necessario anche verificare che sia disabilitata l'impostazione dell'opzione del **Chrome PDF Viewer**. Seguire i seguenti istruzioni per verificare ed eventualmente disabilitare questo parametro.

- Aprire una sessione di Chrome
- Nello spazio dove si scrive l'indirizzo digitare <chrome://plugins/> e poi Invio (cfr immagine seguente)



- Cercare nell'elenco la voce e “**Chrome PDF Viewer**” e cliccare su “**Disabilita**” (cfr immagine seguente)



La voce “**Chrome PDF Viewer**” deve essere impostata come nella figura seguente.



## 2.2 Certificato di autenticazione e di firma digitale

L'accesso a questo servizio può avvenire mediante il certificato di autenticazione digitale, solitamente disponibile nel kit di firma digitale (smart card o Chiavetta USB), obbligatorio per presentare una istanza al SUAP, in quanto tutti i documenti devono essere firmati digitalmente.

Il certificato di autenticazione serve per il riconoscimento della persona che accede al sistema (autenticazione dell'utente), mentre il certificato di firma serve per la firma digitale dei documenti associati alla domanda/SCIA (dal punto di vista legale equivale alla firma autografa).

Sul mercato sono disponibili supporti differenti contenenti il certificato di autenticazione e quello di firma digitale: la **Smart Card** e la **Chiavetta USB**<sup>3</sup>.

Sul sito DigitPA ([http://www.digitpa.gov.it/certificatori\\_firma\\_digitale](http://www.digitpa.gov.it/certificatori_firma_digitale)) è disponibile l'elenco degli Enti certificatori accreditati a livello nazionale, che rilasciano certificati di autenticazione e di firma digitale compatibili con SUAPPi Piemonte.

Ogni Ente Certificatore è libero di realizzare software, dispositivi e manualistica secondo le proprie esigenze. Pertanto per qualsiasi problema di configurazione della postazione e di utilizzo del kit di firma si deve fare riferimento alla manualistica o direttamente all'Ente Certificatore che ha rilasciato il dispositivo.

Il sistema SUAPPi Piemonte accetta come certificato di autenticazione i certificati della Carta Nazionale dei Servizi (CNS).

Il sistema **non** è stato testato con i certificati rilasciati da tutti gli Enti Certificatori.

Si ricorda che i kit di firma digitale dovrebbero contenere al loro interno due certificati:

- certificato di autenticazione necessario per essere riconosciuti dal sistema;
- certificato di firma per firmare digitalmente i documenti

Pertanto a chi rilascia il kit di firma si **deve** richiedere sia il certificato di firma sia quello di autenticazione in formato CNS.

<sup>3</sup> Ad esempio la chiavetta USB fornita da InfoCert prende il nome di Business Key



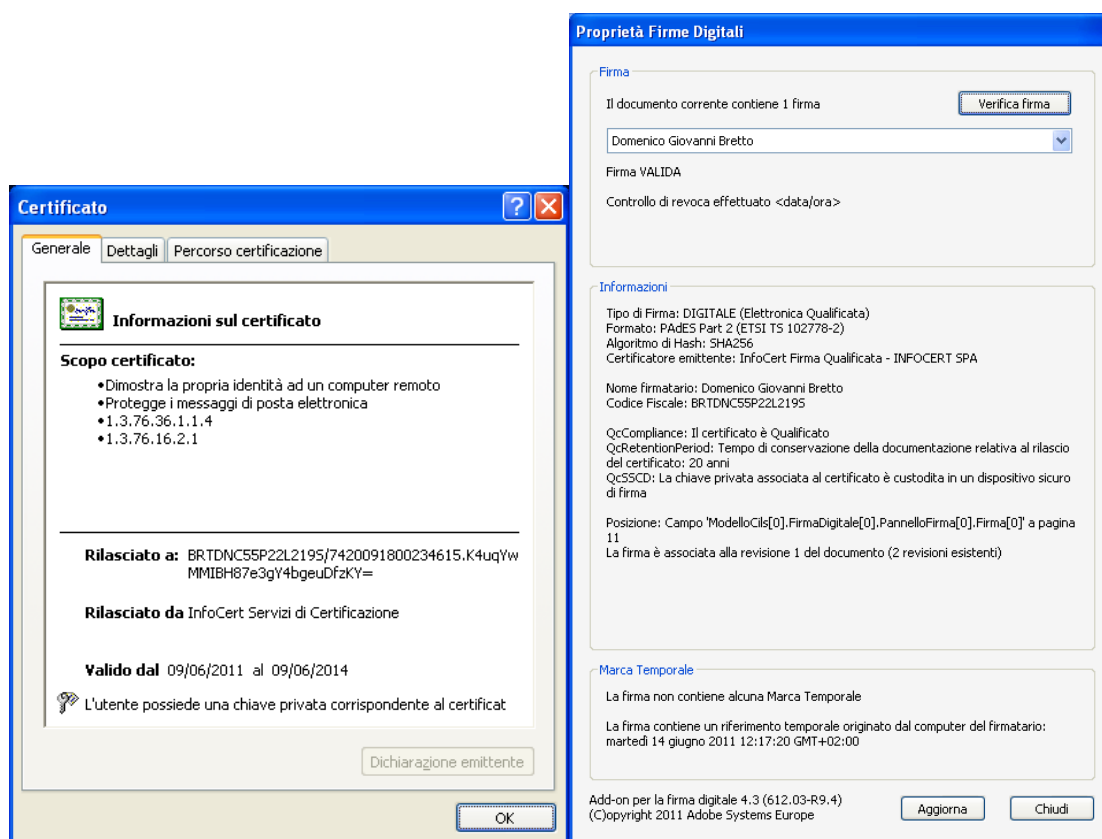
Generalmente la chiavetta USB dispone anche del browser Firefox Portable con al suo interno il certificato già installato, è necessario pertanto utilizzare il predetto browser Portable.

Nel caso in cui si sia in possesso di Smart Card o della chiavetta USB senza browser Firefox Portable installato, è necessario fare riferimento alle istruzioni previste dal certificatore<sup>4 5</sup> per installare il certificato di autenticazione all'interno del browser utilizzato.

**ATTENZIONE:** è importante firmare i moduli PDF/A del SUAPPiEmonte usando il certificato specifico per la firma e non quello usato per l'accesso al sistema !

Nel manuale dell'Ente certificatore sono riportate le spiegazioni su quale sia la differenza e come riuscire a distinguere le tipologie di certificato in funzione dell'operazione che si deve compiere.

Nel seguito si riporta un esempio di certificato di autenticazione e certificato di firma rilasciato da InfoCert.



Esempio di Menù per la verifica del certificato di autenticazione e firma rilasciato da Aruba.

<sup>4</sup> Ad esempio per le smart card di Postecert le istruzioni sono disponibili all'indirizzo <http://www.postecert.it/faq/servizi.shtml>

<sup>5</sup> Ad esempio per le smart card di InfoCert le istruzioni sono disponibili all'indirizzo <https://www.firma.infocert.it/installazione/>



## 2.2.1 Kit di firma digitale

### 2.2.1.1 Smart card

Nel caso si utilizzi una Smart Card il certificato di autenticazione deve essere importato sul browser che si intende utilizzare:

- **Firefox:** => Menù **Strumenti** => **Opzioni** => **Avanzate** => **Cifratura** => **Mostra certificati** => **Certificati Personali** => **Importa**
- **Explorer:** Menu **Strumenti** => **Opzioni** => **Contenuto** => **Certificati** => **Personale** => **Importa certificato**.
- **Chrome:** => **Personalizza Chrome** => **Opzioni** => **Roba da smanettoni** => **Gestisci certificati** => **Personali** => **Importa**.

Questa operazione deve essere effettuata ogni volta che si utilizza una diversa postazione di lavoro. Il certificato così installato sarà riconosciuto automaticamente ad ogni accesso al sistema SUAPiemente. Se sul browser persistono più certificati, il browser presenta una finestra di dialogo per la scelta del certificato opportuno.

Successivamente sarà richiesto il PIN e si accede al sistema.

### 2.2.1.2 Business Key o Chiavetta USB

La chiavetta inserita nella porta USB del PC viene vista come una risorsa del computer.

**SEGNALAZIONE:** si suggerisce di utilizzare **sempre** la stessa porta USB per l'utilizzo della

chiavetta.

Al momento dell'inserimento dovrebbe partire automaticamente ("Autorun") la visualizzazione dei Menù operativi.

"Autorun" di Business Key di Aruba



"Autorun" di Business Key di InfoCert



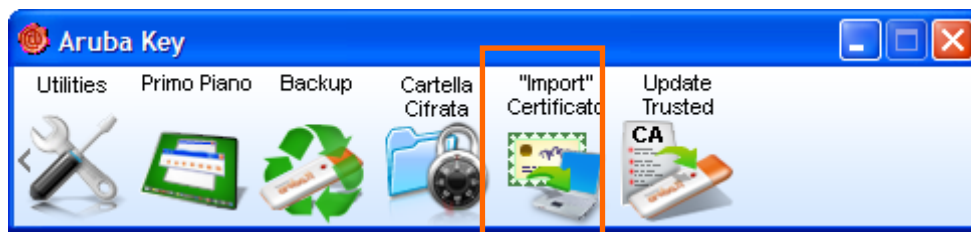
Nel caso in cui il Menù operativo non si attivi automaticamente, utilizzare le risorse del computer per visualizzare il contenuto della chiavetta ed eseguire manualmente il file con il nome "Autorun.exe" che si trova nella radice principale della chiavetta.

**IMPORTANTE:** ogni volta che eseguite l'"Autorun" il dispositivo verifica gli eventuali aggiornamenti software da apportare al dispositivo stesso e chiede se procedere all'aggiornamento. Eseguire **sempre** gli aggiornamenti richiesti.

L'utilizzo della Business Key richiede alcuni passaggi **obbligatori** di configurazione. Queste configurazioni sono necessarie per operare al meglio utilizzando il browser installati sul computer (**scelta consigliata**). Tali operazioni vanno eseguite su ogni postazione di lavoro che si intende utilizzare. Le operazioni di seguito descritte sono maggiormente dettagliate nei manuali d'uso della chiavetta.

Configurazione per **Aruba**: selezionare **Utilities**, quindi **Import Certificato**



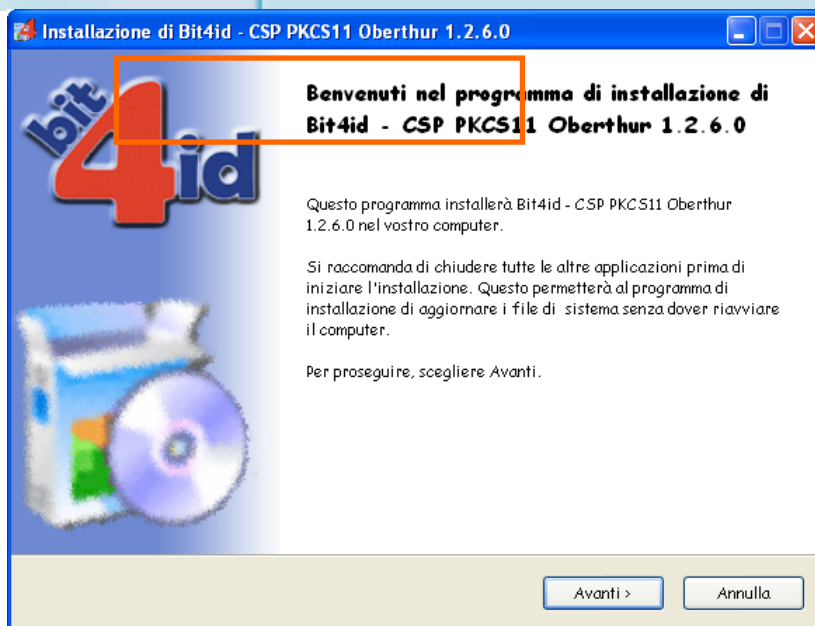


Configurazione per **InfoCert**: selezionare **Impostazioni**, quindi **Utilizza la business key con le applicazioni del tuo PC**.



In entrambi i casi viene eseguito l'applicativo **bit4id.exe**; completare l'installazione seguendo i passi richiesti dall'applicativo.

Questo prodotto installa nella cartella della postazione di lavoro **\\windows\system32** un file che, a seconda del tipo di certificato utilizzato, può chiamarsi "**bit4ipki.dll**" oppure "**bit4opki.dll**".



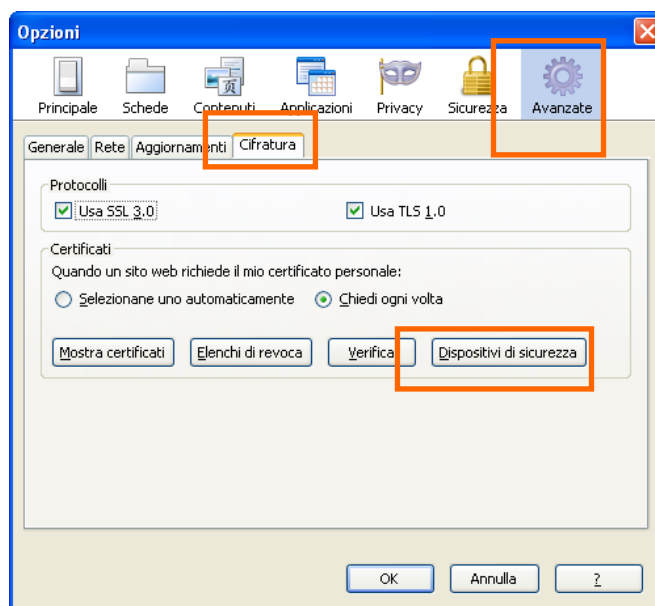
Il file installato permette ai browser presenti sul computer di individuare i certificati digitali presenti nella chiavetta.

Tuttavia esistono comportamenti diversi a seconda del browser:

- Explorer e Google Chrome identificano automaticamente il file installato e quindi il posizionamento dei certificati sulla chiavetta;
- per Mozilla FireFox è necessario procedere con l'installazione manuale del file.

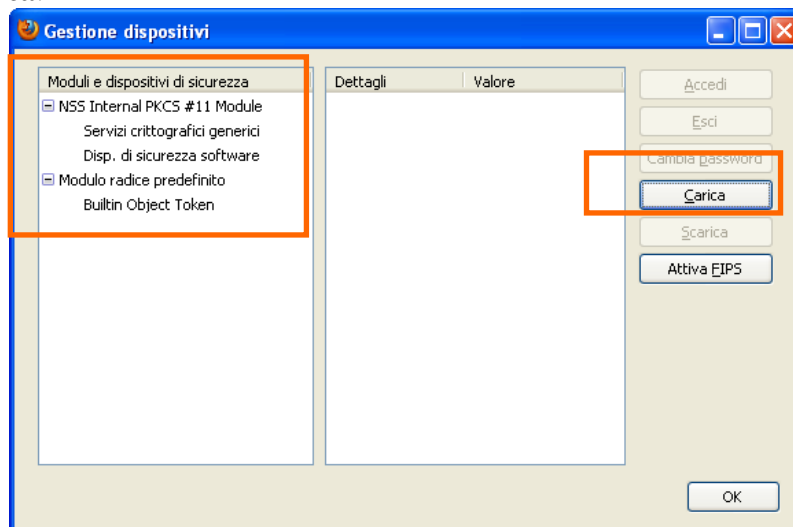
### Configurazione di FireFox residente sul proprio computer.

Eseguire **FireFox**, quindi dal Menù **Strumenti** selezionare **Opzioni** => **Avanzate** => **Cifratura**  
E selezionare il pulsante **Dispositivi di sicurezza**

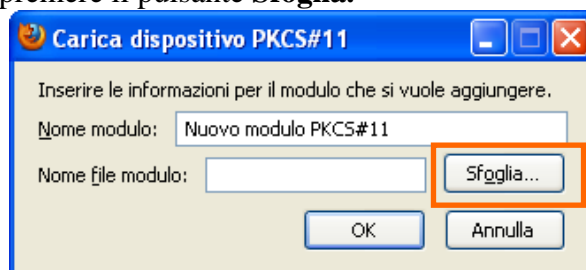


Tipicamente vengono visualizzati solo due dispositivi, per aggiungere quello di interesse cliccare

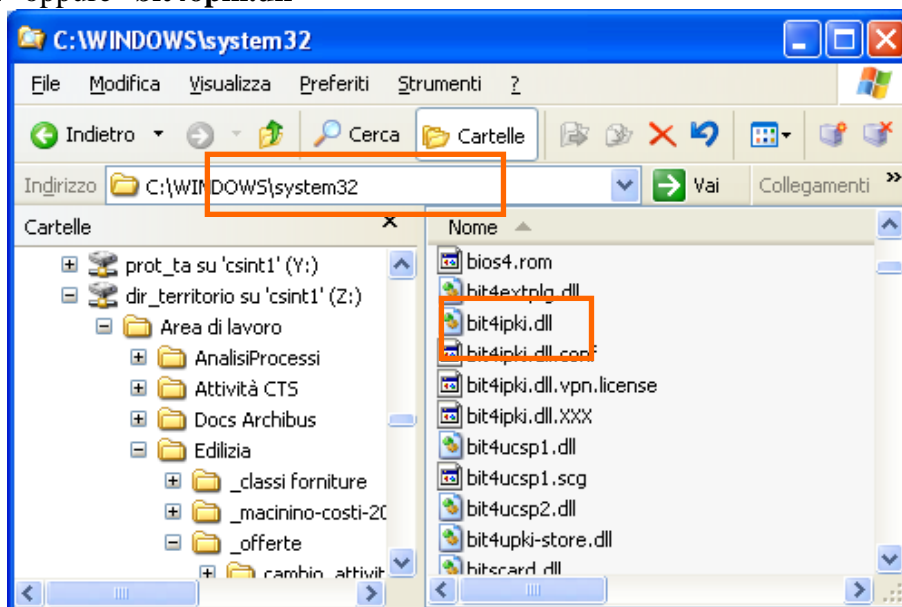
sul pulsante **Carica**.



Nella finestra **Carica dispositivo PKCS#11** inserire un **Nome modulo** a piacere identificativo del proprio dispositivo e premere il pulsante **Sfoglia**.



Quindi posizionarsi sulla cartella **\\windows\system32** e selezionare, secondo i casi, il file **"bit4ipki.dll"** oppure **"bit4opki.dll"**



**IMPORTANTE:** selezionare **esclusivamente** il file con estensione **.DLL**

Il file acquisito viene riportato nel **Nome file modulo**, quindi premere **Ok** per confermare e



chiudere e così per tutte le finestre di **FireFox** finora aperte.

### 2.2.1.3 Firma digitale

Si considera in questo caso la firma digitale da apporre in locale ai file (PDF/A) che saranno allegati alle Domande/SCIA e che generano l'estensione "p7m".

Nel caso si disponga del kit fornito da **ArubaKey**, il modulo per la firma digitale è disponibile nella barra degli strumenti.



Nel caso si disponga del kit fornito da **InfoCert**, il modulo per la firma digitale, denominato **Dike**, è disponibile alla voce di Menù **Firma Digitale**.



## 2.3 Accesso tramite username / password e PIN (o CIP)

Con il rilascio della versione di inizio febbraio 2014, è stata introdotta la possibilità per l'utente privato di accedere a SUAPiemente mediante username/password e PIN (o CIP).

Per ottenere le credenziali di accesso occorre che l'utente sia registrato o al sito di Torinofacile (<http://www.torinofacile.it/registrazione/>) oppure al sito di Sistemapiemonte (<http://www.sistemapiemonte.it/registrazione/index.shtml>).

Qualora l'utente disponesse già di credenziali complete (username/password e PIN (o CIP)) può accedere immediatamente a SUAPiemente con questa modalità.

Qualora l'utente disponesse soltanto di Username e Password rilasciate da uno dei due portali, occorre richiedere anche il PIN (o CIP) prima di essere in grado di utilizzare questa modalità.

### 3 Istruzioni utili unicamente ai funzionari della Pubblica Amministrazione (Comuni, ASL, Province, etc.)

Gli utenti della Pubblica Amministrazione che necessitano di utilizzare il servizio SUAPPiemonte e non devono firmare digitalmente i documenti, possono utilizzare il certificato di autenticazione digitale emesso da CSI Piemonte. La richiesta di emissione del certificato deve essere effettuata alla casella servizi.suap@csi.it.

Viceversa se l'utente necessita di firmare digitalmente i documenti, **deve** dotarsi di una CNS dotata sia di certificato di autenticazione sia di certificato di firma digitale personali.

#### 3.1 *Certificato di autenticazione personale rilasciato da CSI-Piemonte*

A seguito dell'emissione del certificato di autenticazione personale da parte del servizio di CSI-Piemonte, l'intestatario riceverà una mail alla propria casella di posta elettronica ed una lettera contenenti i codici per scaricare e installare il Certificato Digitale Personale nel browser (cfr istruzioni all'indirizzo <http://www.ruparpiemonte.it/portal/public/rupar/sicurezzaAutenticazione> )

#### IMPORTANTE:

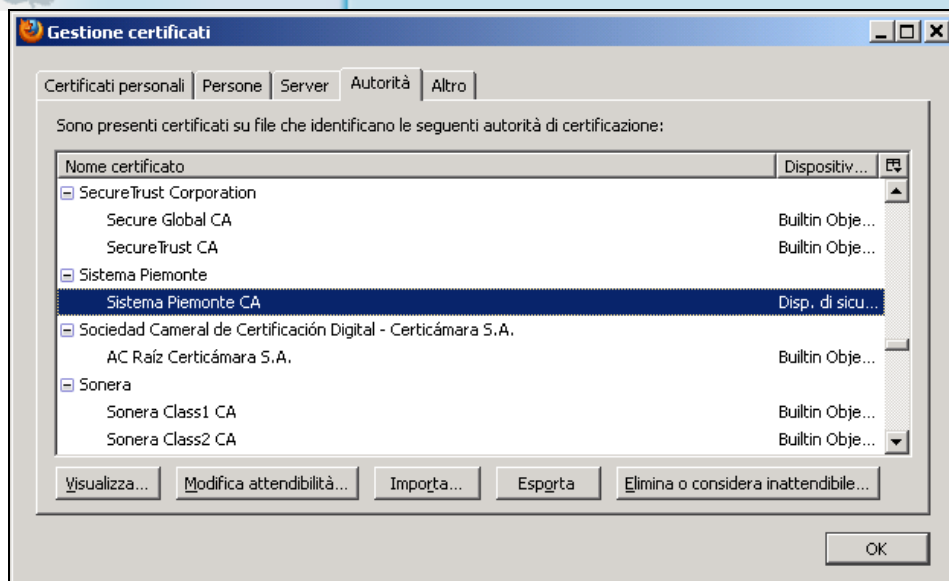
- per scaricare e installare il certificato è necessario inserire un codice. Questo codice si compone di due parti contenute in una mail e in una lettera che riceverete direttamente. Questa modalità è dettata dalle norme sulla sicurezza.
- è importante **conservare** la mail e la lettera contenente i due codici perchè in futuro potrebbe avere la necessità di reinstallare il certificato su un altro PC.
- è importante scaricare il certificato e **PRIMA** di installarlo è **NECESSARIO** salvarne una copia in una chiave **USB** se un domani ha la necessità di installarlo su un secondo PC

Successivamente all'installazione effettuare eseguire anche la seguente procedura.

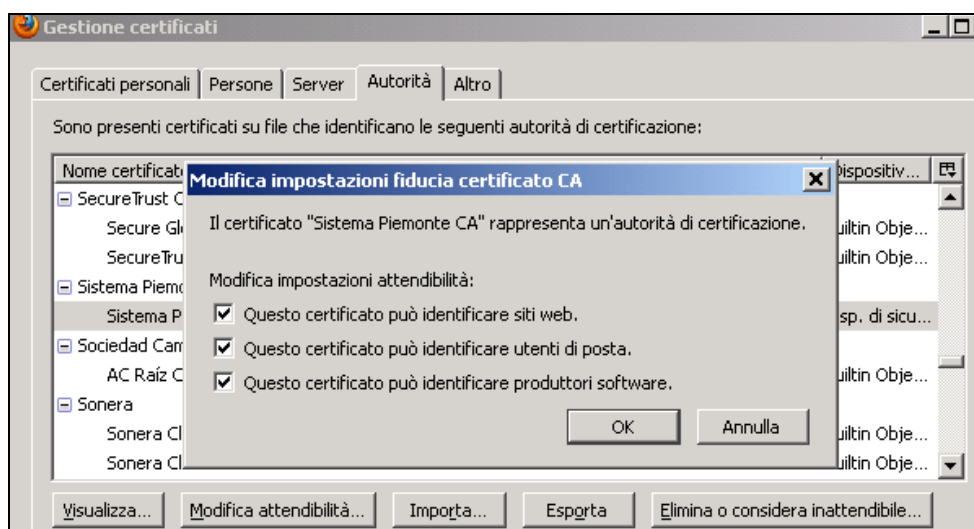
##### 3.1.1 Mozilla Firefox

Selezionare Menu - **Strumenti** – **Opzioni** – **Avanzate** – **Cifratura** - **Mostra Certificati** – **Autorità**  
Selezionare la voce **Sistema Piemonte** – **Sistema Piemonte CA**





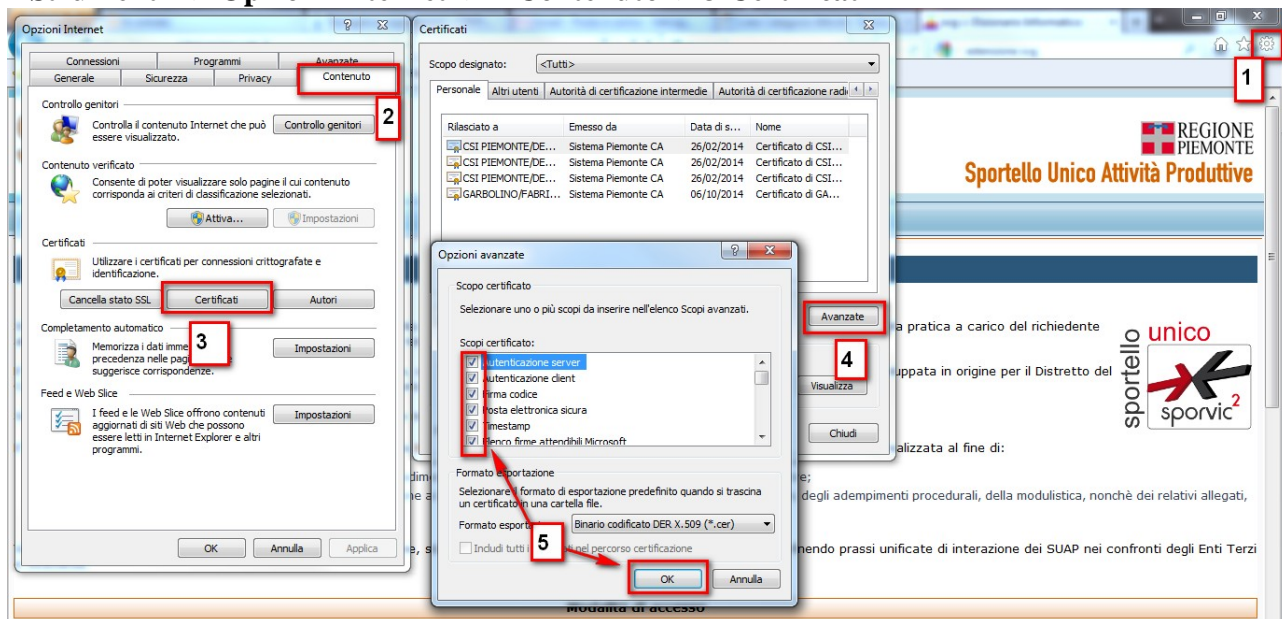
E selezionare tutti **Mostra Attendibilità** e tutti e tre i segni di spunta presenti e poi **OK**.



## 3.1.2 Internet Explorer

Selezionare:

**1 Strumenti => Opzioni Internet=> 2 Contenuto=> 3 Certificati**



Aperta la finestra dei certificati, si può importare il proprio certificato ricevuto dal CSI.

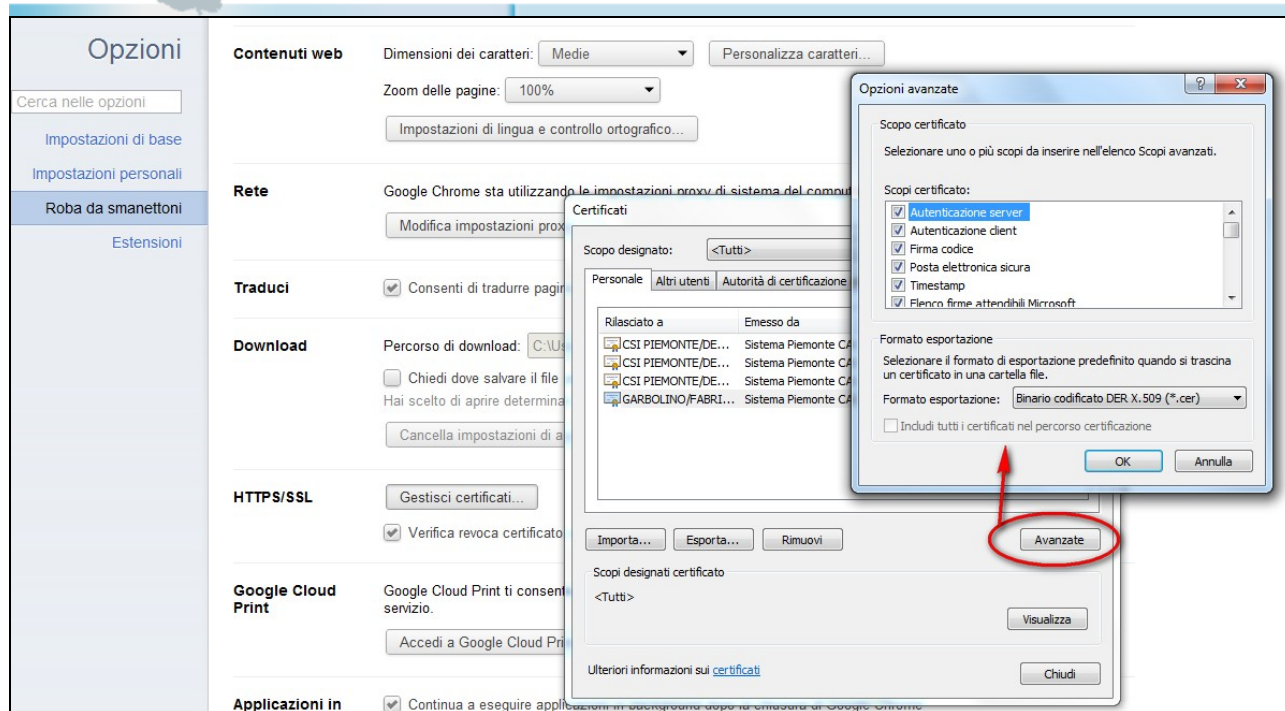
Successivamente, cliccando sul bottone **4 Avanzate**, spuntare tutte le voci all'interno e cliccare **5 OK**.

## 3.1.3 Google Chrome

Chrome abitualmente recupera tutti i dati dal sistema, quindi da quello che è stato installato su Internet Explorer.

Se non si è installato internet Explorer, allora andare nel menu

**Strumenti => Opzioni => Roba da smanettoni => Gestisci certificati**



Aperta la finestra dei certificati, si può importare il proprio certificato ricevuto dal CSI.  
Successivamente, cliccando sul bottone **Avanzate**, spuntare tutte le voci all'interno e cliccare **OK**.

## 4 Software aggiuntivi

### 4.1 Software per la trasformazione dei documenti nel formato PDF/A

La norma relativa al CAD (Codice dell'amministrazione digitale) prevede che i documenti soggetti a conservazione abbiano il formato **"PDF/A"** (Standard ISO 19005).

Di conseguenza, la postazione di lavoro richiede per tutte le tipologie di utenti un software in grado di trasformare i documenti nel formato PDF/A.

Con la suite gratuita "OpenOffice", l'utente può aprire il documento redatto con un altro word processor e con la funzione disponibile nel menù "File → *Esporta nel formato PDF*" trasforma il file con estensione PDF.

Si ricorda di utilizzare il formato **"PDF/A"** per l'esportazione di un file in formato PDF. Trasformato il file in formato PDF/A è possibile apporre la firma digitale.

Apposta la firma digitale, il file assumerà l'estensione **PDF.P7M**.

Nel caso in cui la postazione di lavoro dell'utente necessiti di uno strumento per la trasformazione dei documenti nel formato PDF/A, si consiglia di ricercare il testo seguente

**software gratuito per trasformazione documento in PDF/A**

con un qualsiasi motore di ricerca (ad esempio [www.google.it](http://www.google.it)).

La ricerca produrrà un elenco di siti internet da cui l'utente può scaricare liberamente il software ricercato.

### 4.2 Software per lettura documenti firmati digitalmente

Nel caso in cui l'utente non sia dotato di kit di firma digitale, deve disporre sulla postazione di lavoro di un software per la lettura dei documenti firmati digitalmente.

Si consiglia di ricercare il testo seguente

**software gratuito per apertura di documenti firmati digitalmente**

con un qualsiasi motore di ricerca (ad esempio [www.google.it](http://www.google.it)).

La ricerca produrrà un elenco di siti internet da cui l'utente può scaricare liberamente il software ricercato.