

**“InfoCert”  
Società per azioni**

**Prodotto INDI – Ente Certificatore InfoCert  
MI/RAO\_ICERT  
Manuale Installazione Workstation RAO –  
IR informatizzato**

Funzione emittente    Assistenza Clienti

Redatto da              G. Pinton

Verificato da

Approvato da

## Sommario

- 1. Introduzione al documento ..... 3**
- 2. Installazione workstation RAO per rilascio dispositivi di firma .....  
4**
- 3. Workstation IR informatizzato ..... 43**

## 1. Introduzione al documento

### 1.1 Novità introdotte rispetto alla precedente emissione

|                               |   |                                |            |
|-------------------------------|---|--------------------------------|------------|
| <b>Versione/Release n° :</b>  | 8                                       | <b>Data Versione/Release :</b> | 27/04/2016 |
| <b>Descrizione modifiche:</b> |   |                                |            |
| <b>Motivazioni :</b>          | Aggiornamento dei prerequisiti software |                                |            |

### 1.2 Scopo e campo di applicazione del documento

Il documento ha l'obiettivo di:

- guidare l'installazione dei prodotti software e dell'hardware utilizzati nella workstation RAO, per l'emissione dei certificati digitali forniti da InfoCert S.p.A.;
- guidare la configurazione della workstation per l'IR informatizzato.

### 1.3 Termini e definizioni

**ActiveX** (Dall'inglese *Active* e *eXtension*, Estensione Attiva) è il nome di una tecnologia sviluppata dalla Microsoft destinata agli sviluppatori e creata per poter estendere le potenzialità e le funzioni di una applicazione.

**Controlli ActiveX** I controlli ActiveX sono veri e propri file al cui interno sono raggruppati comandi e funzioni. Alcuni programmi, come Internet Explorer, possono importare questi controlli e quindi sfruttarne le potenzialità.

**Plugin** (o Plug-in) è un programma non autonomo che interagisce con un altro programma per aprirne le funzioni. La capacità di un software di supportare i plugin è un'ottima caratteristica che rende possibile l'ampliamento delle sue funzionalità in maniera semplice e veloce.

**RAO** Operatore dell'Ufficio di Registrazione: soggetto incaricato a verificare l'identità e, se applicabile, ogni specifico attributo di un Titolare, nonché ad attivare la procedura di certificazione per conto del Certificatore. (Dal Manuale Operativo dell'Ente Certificatore InfoCert).

**IR** Incaricato della Registrazione, soggetto facente capo ad un determinato Ufficio di Registrazione, che effettua la sola identificazione dell'Utente Titolare e ne annota i dati necessari (su apposito modulo cartaceo, o in alternativa in una maschera via internet).

## 2. Installazione workstation RAO per rilascio dispositivi di firma

Attraverso le istruzioni contenute nel presente manuale è possibile configurare un computer con l'hardware e il software necessari per il rilascio dei certificati digitali di InfoCert su dispositivi di firma, affinché possa operare come workstation ad uso dei RAO. Per le procedure dell'Ufficio di Registrazione si rimanda al Manuale Utente Ufficio di Registrazione disponibile al link “**Comunicazioni ai RAO**” presente nella home page.

Le URL di collegamento al sito dell'Ufficio di Registrazione sono le seguenti:

- accesso via **Internet**: <http://ncar.infocert.it> •

accesso via **Intranet** <http://ncar.infocert.it>

### 2.1 Prerequisiti

#### 2.1.1 Hardware

- Processore: Intel e compatibili e a 64 bit – 1 gigahertz (GHz)
- Memoria RAM: 1 GB (32 bit) o 2 GB (64 bit)
- Disco fisso: 16 GB (32 bit) o 20 GB (64 bit)
- 2 lettori di smart card PC/SC compatibili, come ad esempio: bit4id miniLector USB U38
- 2 porta USB 2.0 disponibili e accessibili anche con cavo di prolunga (per rilascio delle Business Key)
- Stampante collegata alla Work Station
- Stampante termo-grafica (per le CNS)

#### 2.1.2 Software

- Sistemi Operativi Windows Client attualmente supportati da Microsoft®
- Internet Explorer 8 SP1 e successivi
- Middleware CSP reperibile gratuitamente ai seguenti link:
  - [www.firma.infocert.it/software/bit4id\\_xpki\\_1.4-ccid.zip](http://www.firma.infocert.it/software/bit4id_xpki_1.4-ccid.zip) ○
  - [www.firma.infocert.it/software/SafeDive2\\_setup.zip](http://www.firma.infocert.it/software/SafeDive2_setup.zip)
- Ultima versione dei driver relativi ai lettori utilizzati (link reperibili gratuitamente sul sito [www.firma.infocert.it](http://www.firma.infocert.it))
- Microsoft SOAP Toolkit vers. 3.0 o superiore
- Aver effettuato preventivamente tutti gli aggiornamenti previsti da Microsoft attraverso il sito di Windows Update
- Token Eutron CryptoIdentity Card Reader/Writer (nel caso ci sia la necessità di emettere certificati in questo tipo di dispositivo – vedere “Nota Installazione Token Eutron” disponibile nella sezione “comunicazioni ai RAO” della procedura)

**Attenzione: si ricorda che tutte le installazioni SW devono essere effettuate come Utente “Amministratore” del Computer.**

Per la configurazione della stampante grafica per le CNS, presso gli Uffici competenti delle camere di Commercio, rivolgersi al Commerciale di riferimento.

### 2.1.3 Rete

Di seguito vengono riportati i parametri di rete per le postazioni dei RAO extra-camerali:

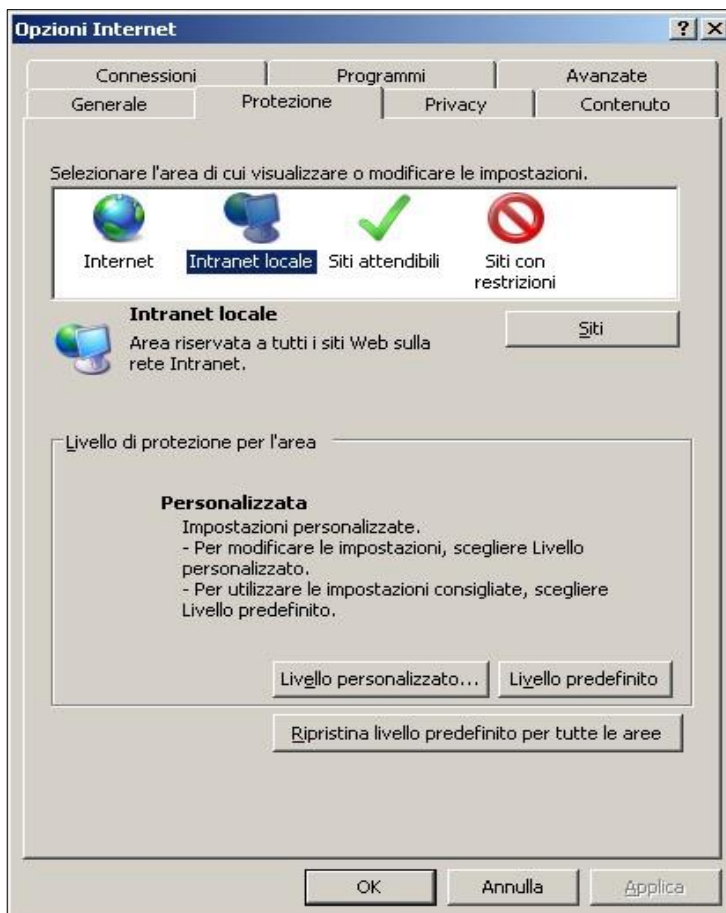
- Connessione HTTP su porta 80 e HTTPS su porta 443 agli URL:
  - ncar.infocert.it
  - wcar.infocert.it
- Connessione ldap porta 389 (standard LDAP) per lo scarico delle CRL:
  - [ldap.infocert.it](http://ldap.infocert.it)

### 2.1.4 Internet Explorer 8.0 e successivi

La procedura di registrazione e di emissione prevede l'utilizzo del browser Internet Explorer versione 8.0 o superiore, solitamente installato con il sistema operativo, aggiornato all'ultimo service pack disponibile. Eventualmente è possibile richiedere un aggiornamento delle versioni precedenti collegandosi sempre al sito **Windows Update**.

Per il corretto funzionamento della procedura di emissione è necessario verificare la corretta impostazioni della protezione del browser:

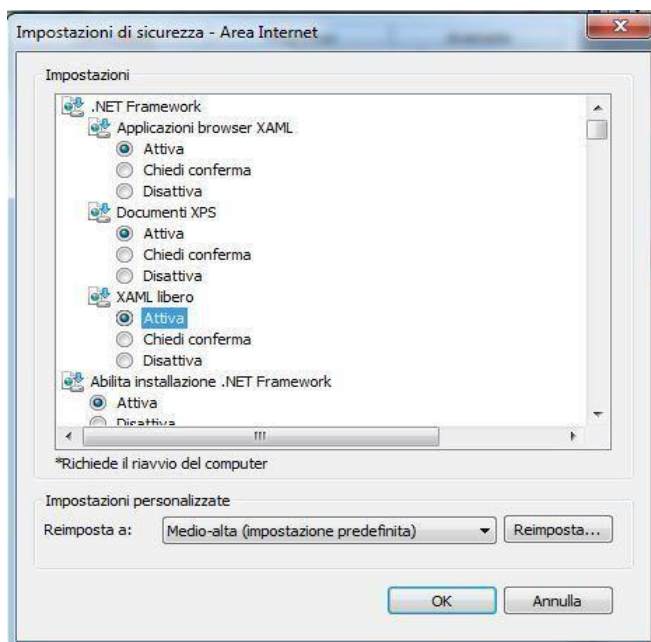
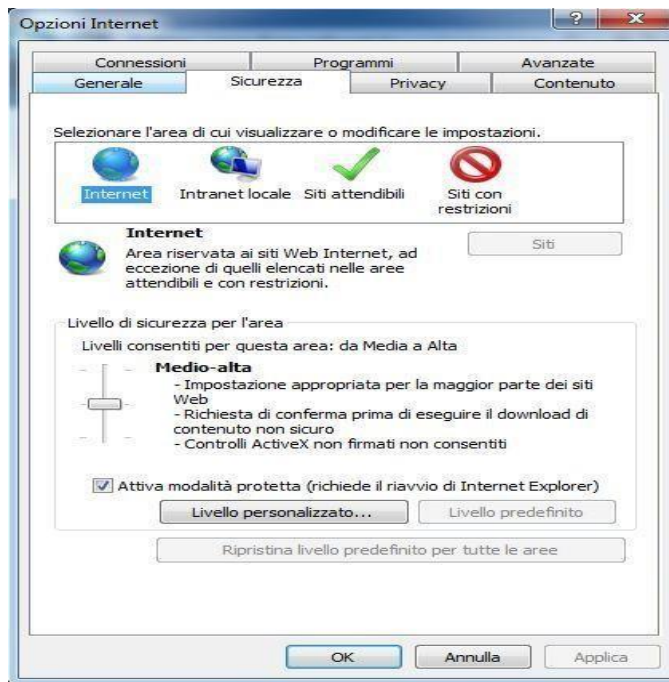
- aprire il browser e cliccare su “**Strumenti**”
- clic su “**Opzioni Internet**”
- clic su “**Protezione**”

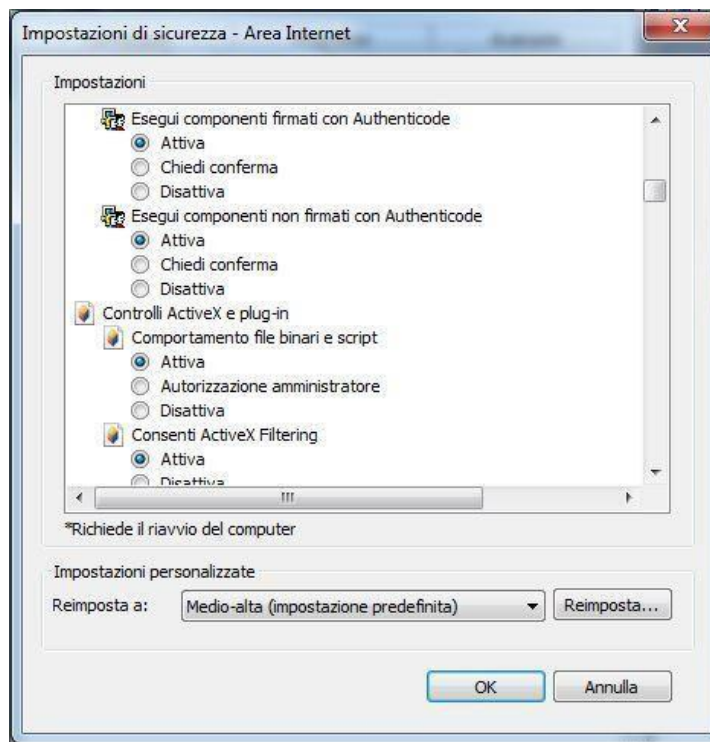
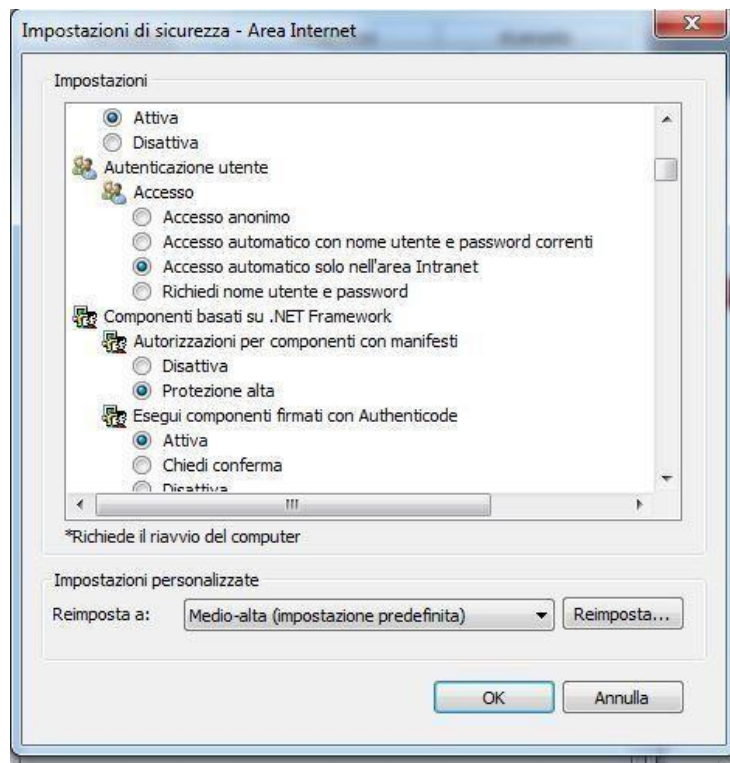


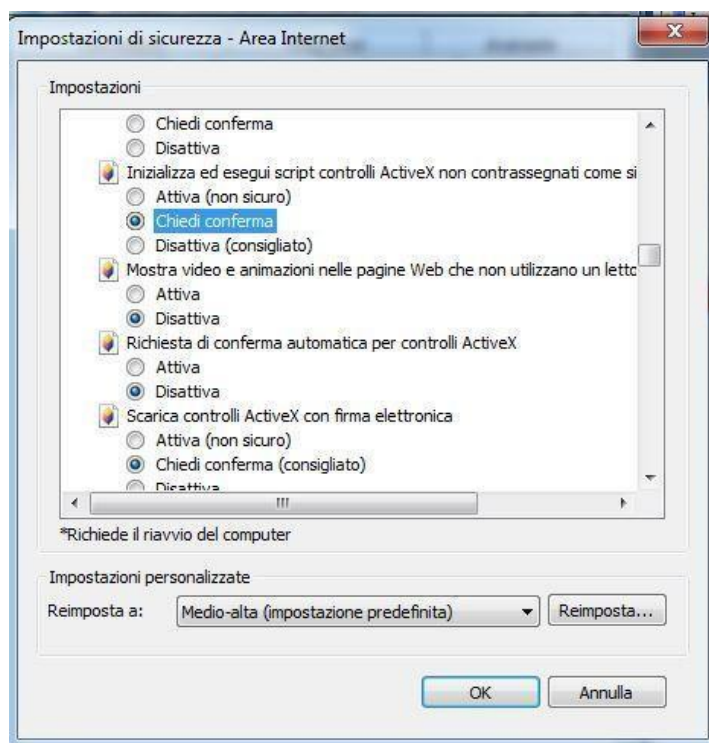
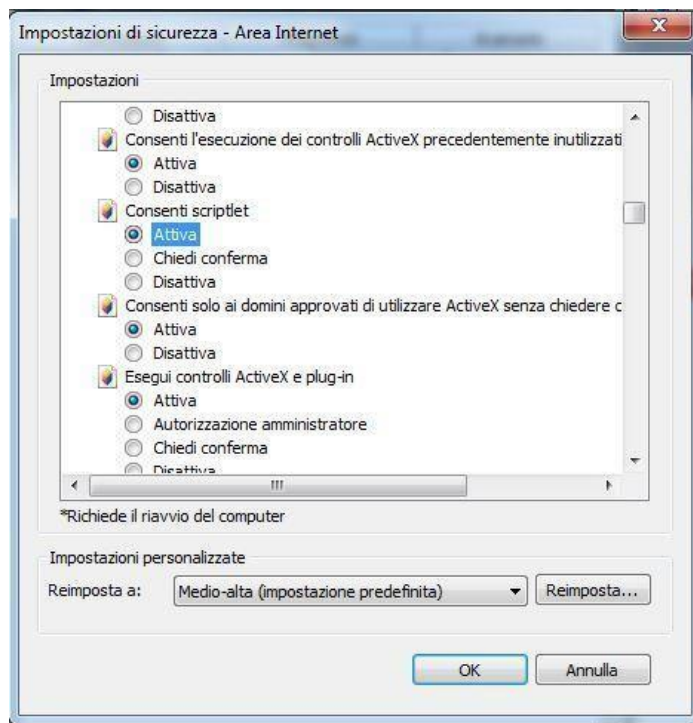
- selezionare “**Internet**” o “**Intranet**” (a seconda del sito dal quale si emetteranno le smart card) e quindi cliccare su “**Livello personalizzato**”:

- controllare le impostazioni di sicurezza, personalizzandole nel modo seguente:

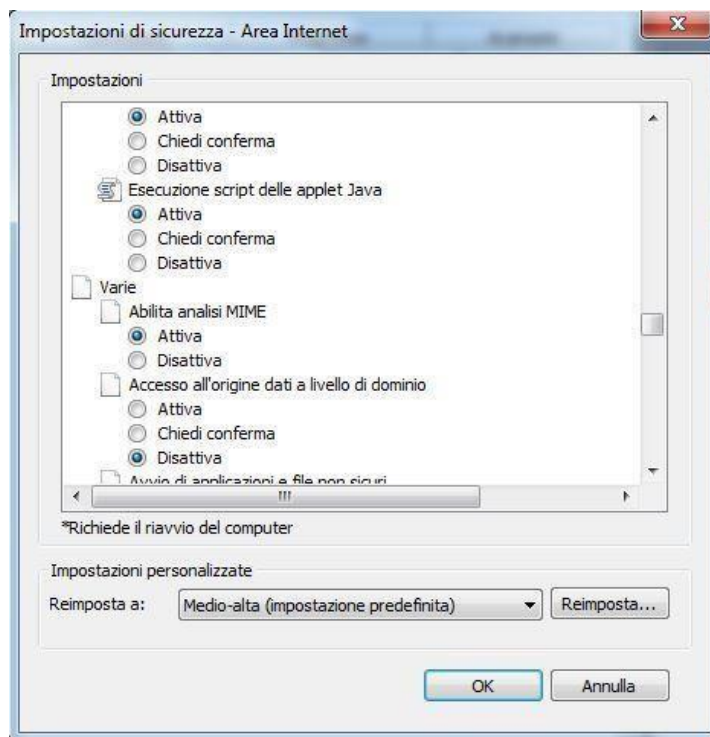
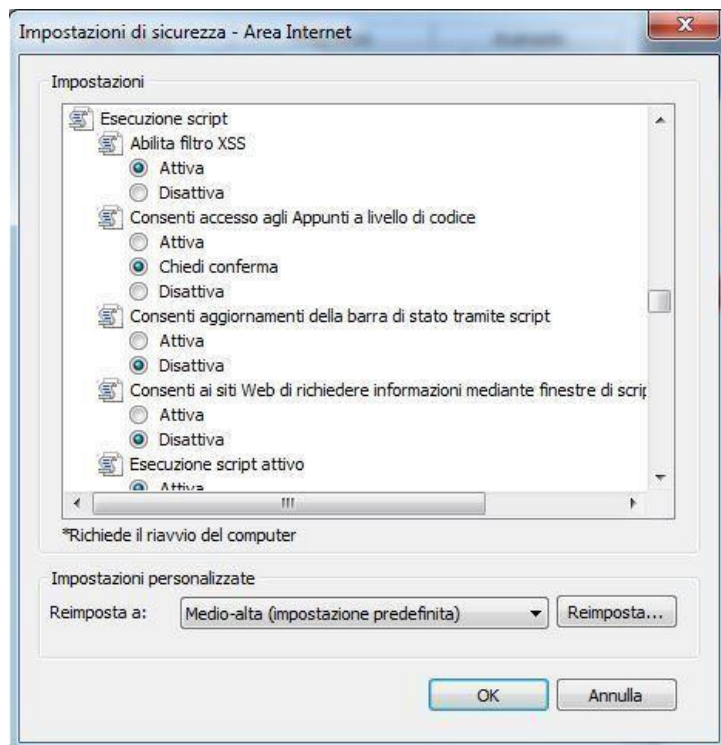
Esempio di configurazione per s.o. Windows 7 a 64 bit – Internet Explorer 10 a 64 bit

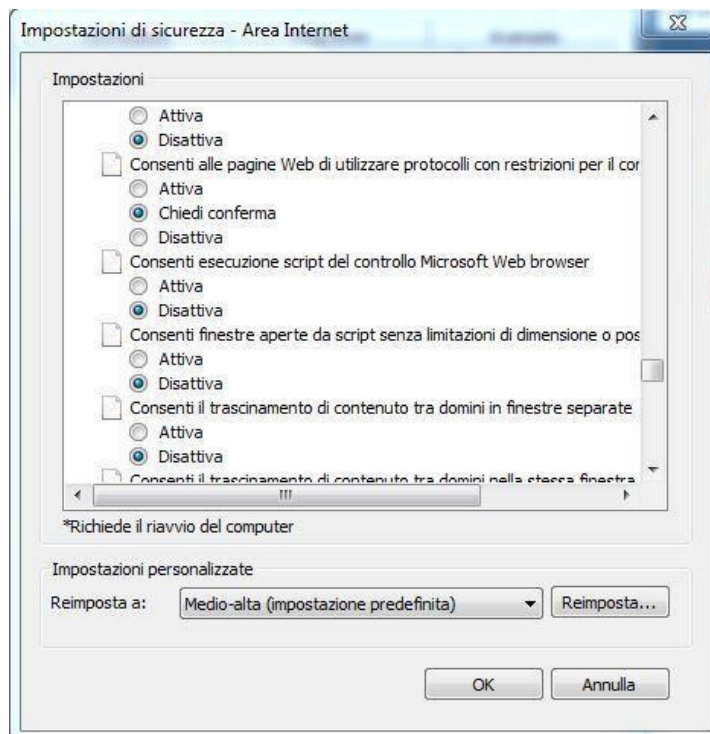
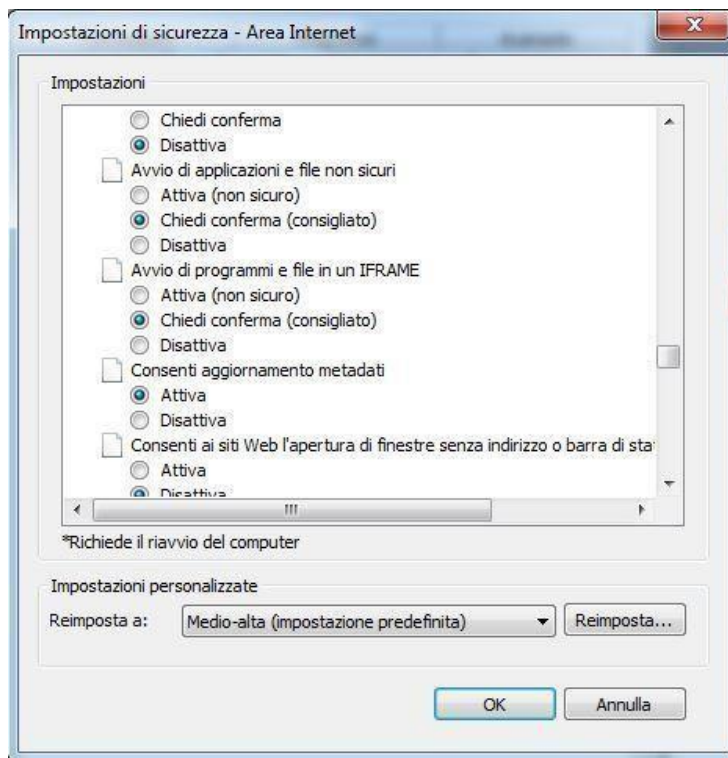


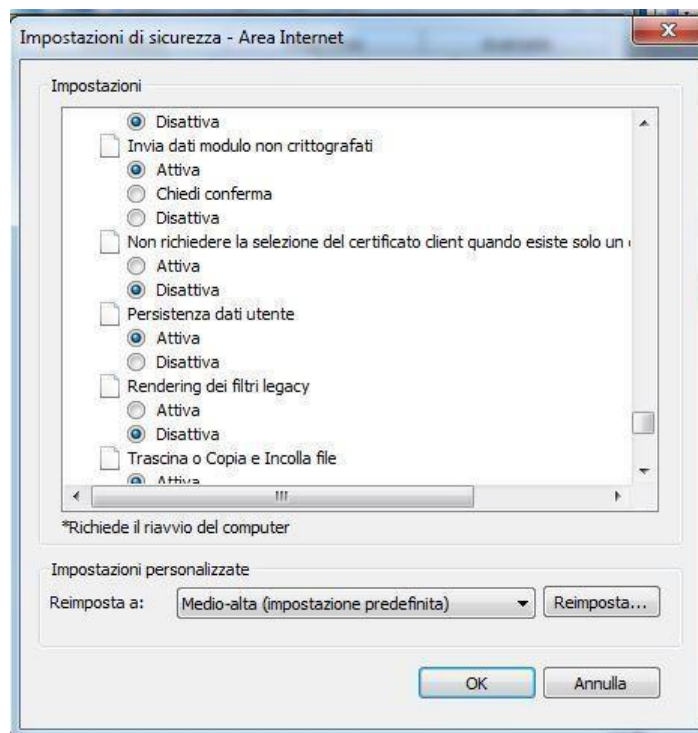
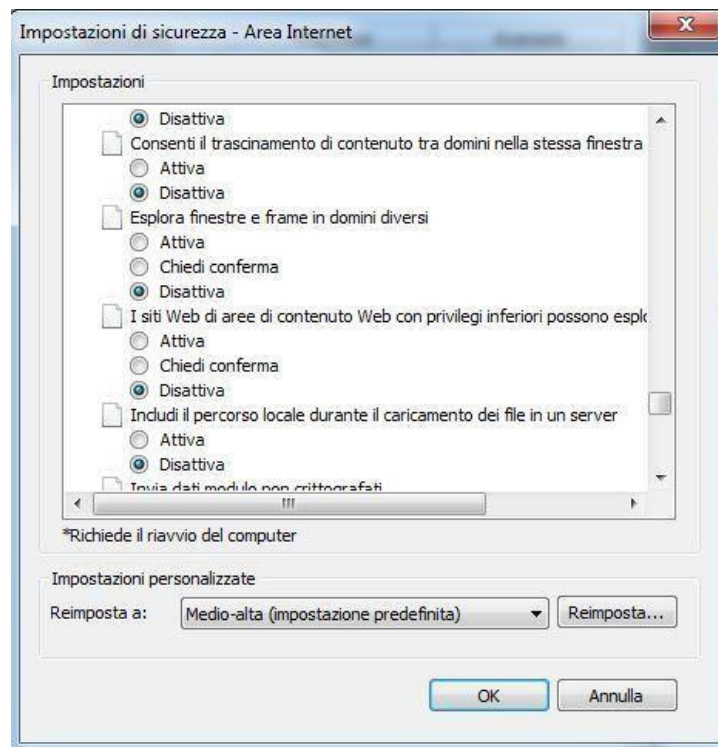


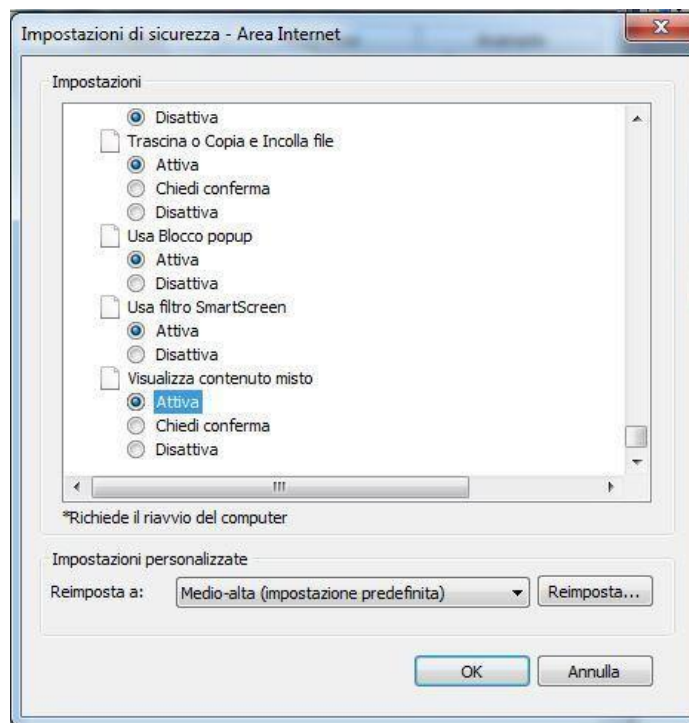






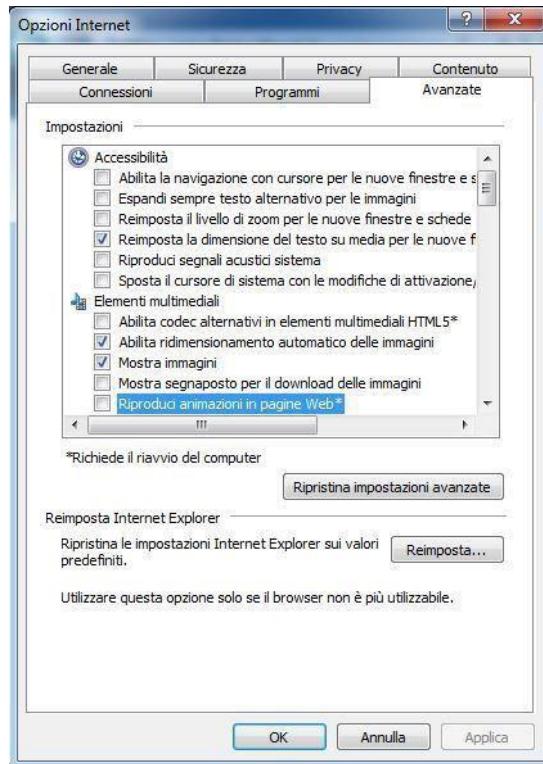


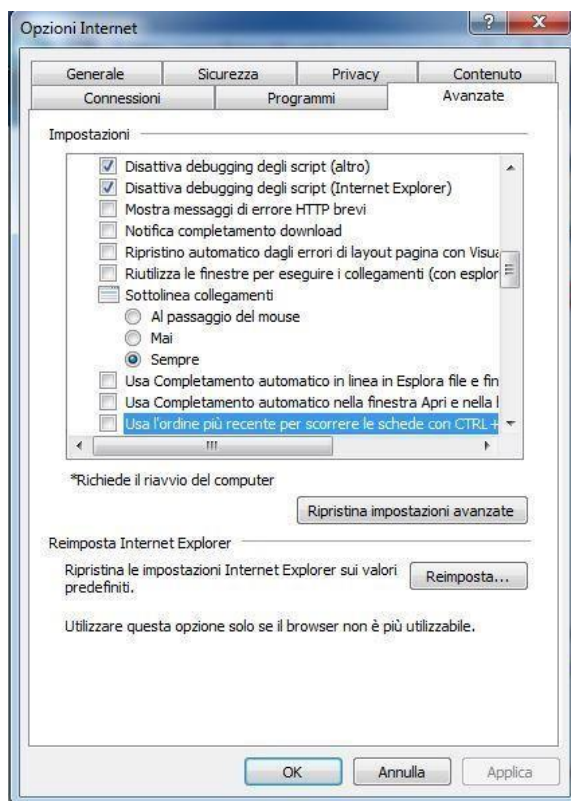
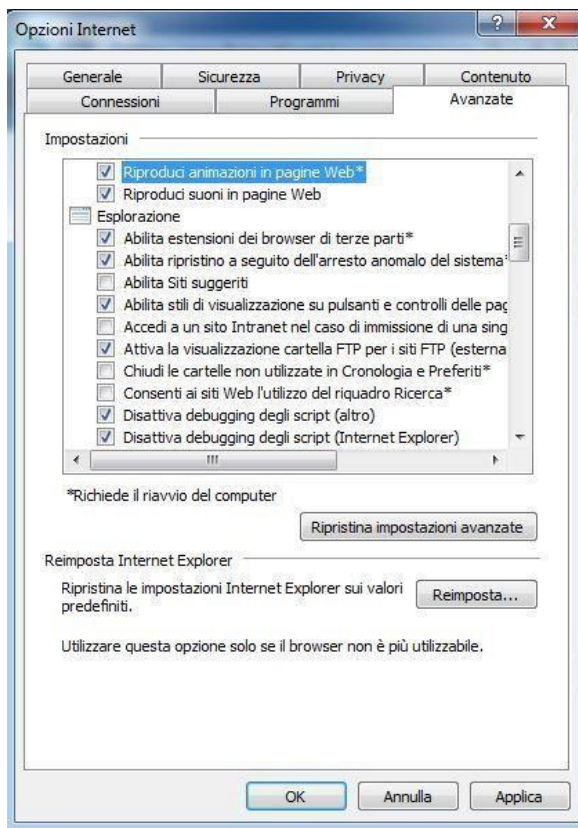




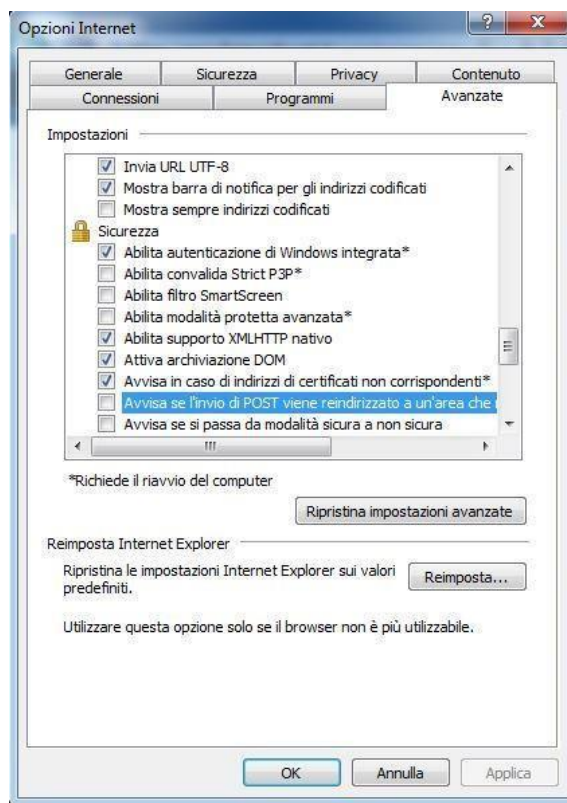
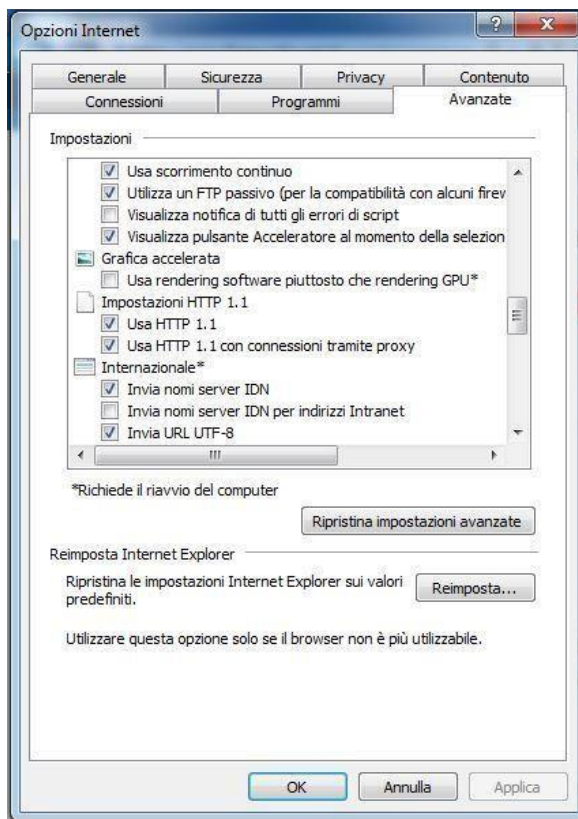
Sucessivamente , sempre da “**Strumenti**”

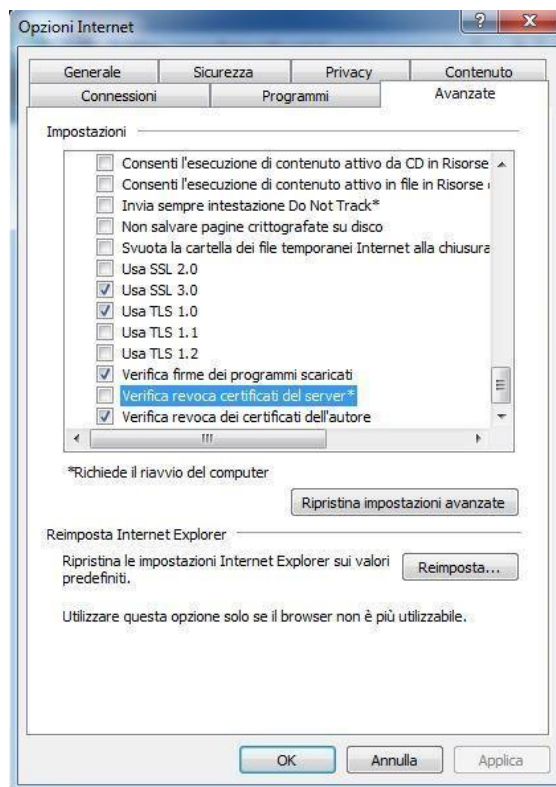
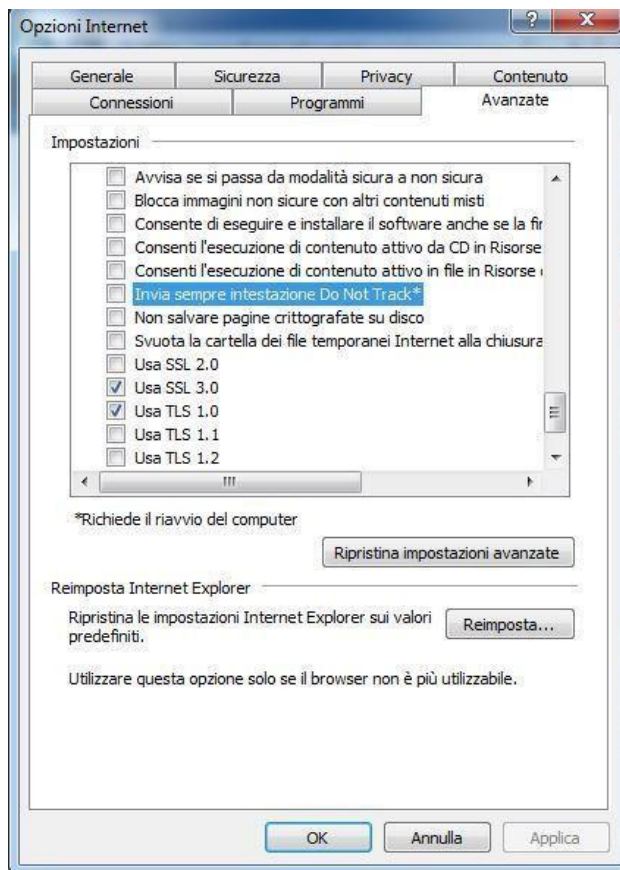
- clic su “**Opzioni Internet**” - clic su “**Avanzate**” , controllando le Impostazioni, personalizzandole nel seguente modo:



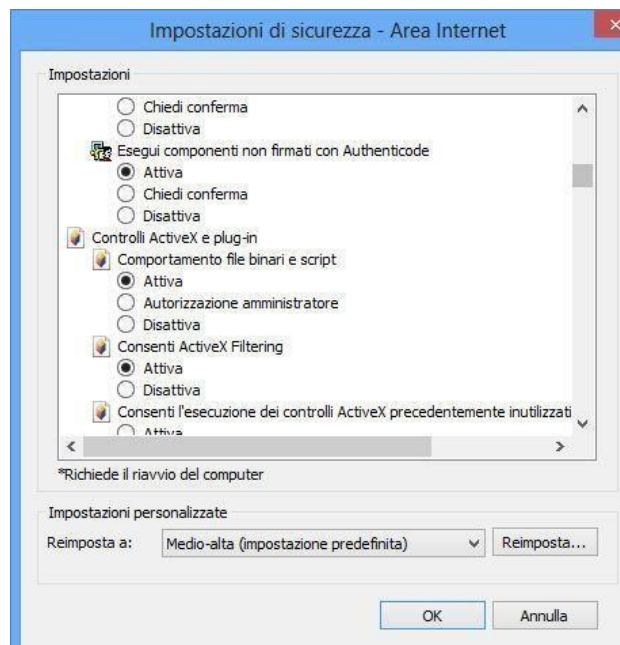
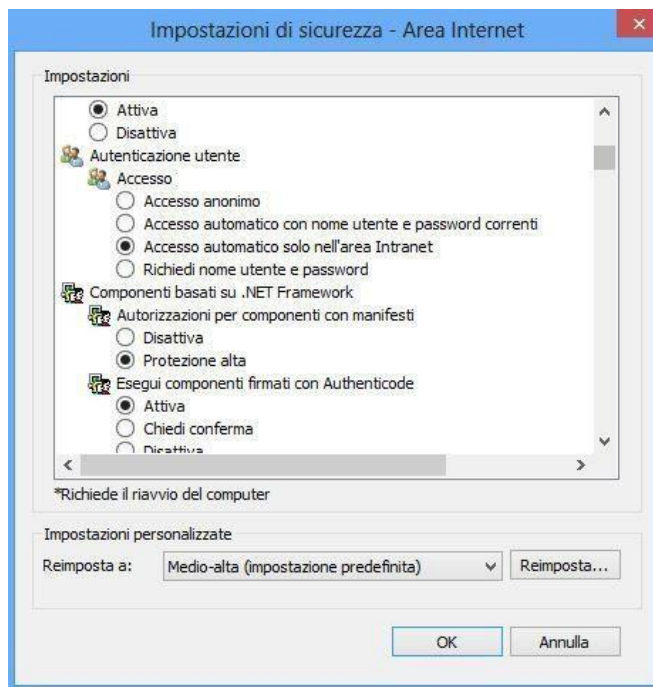




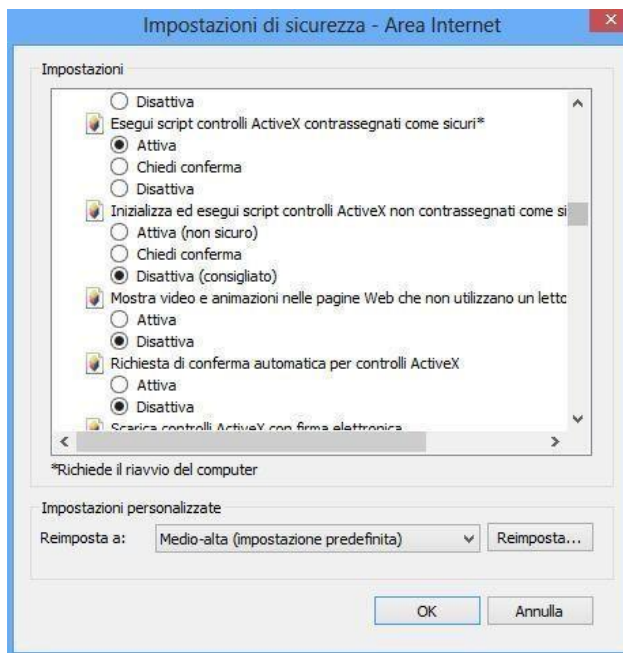
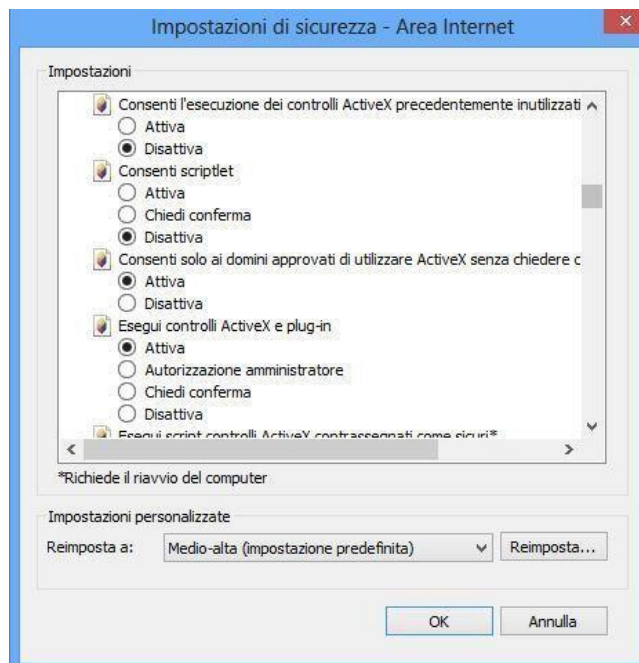


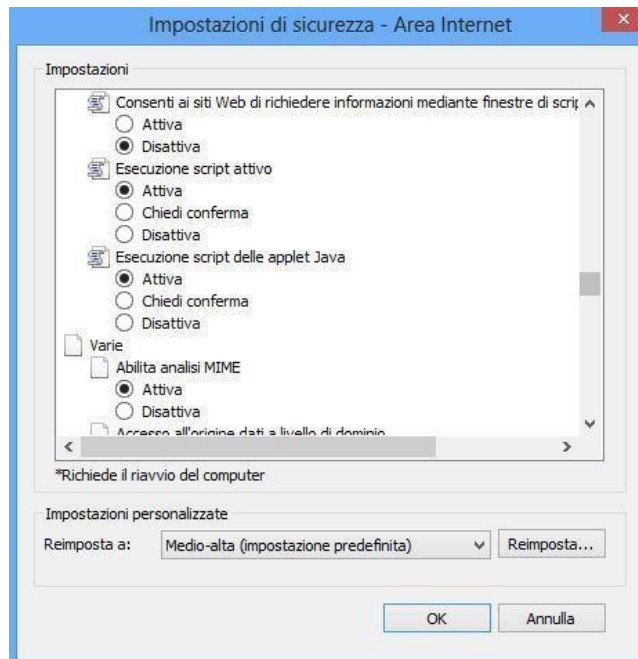
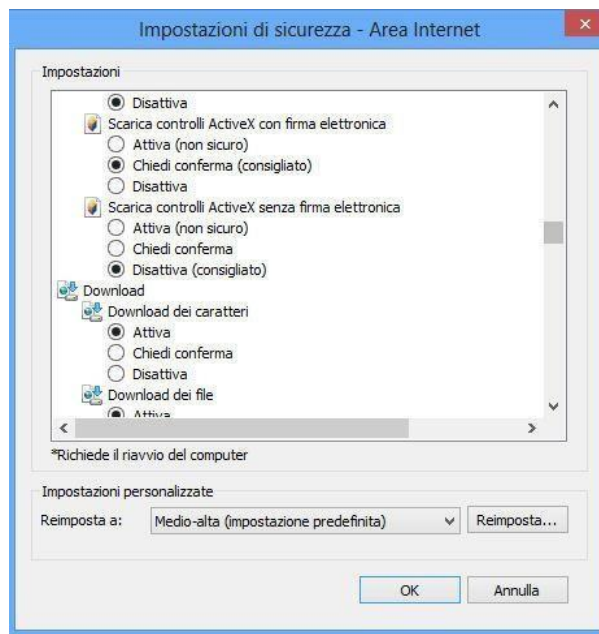


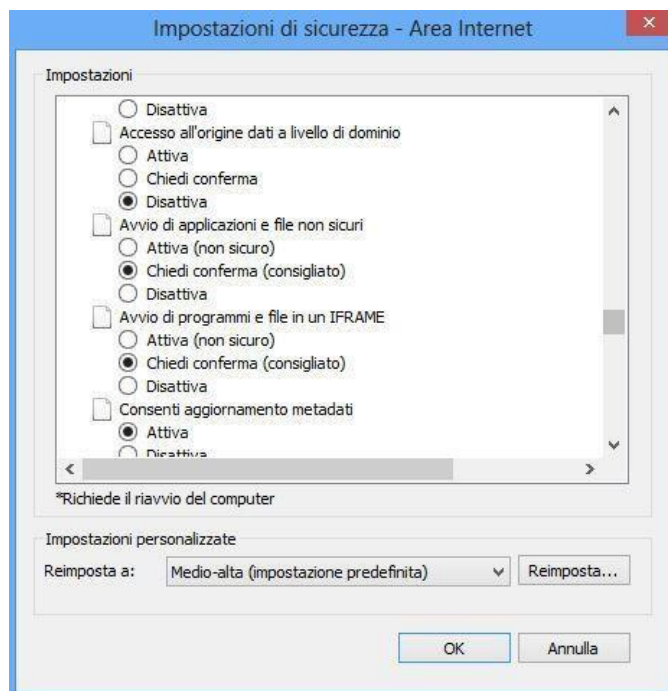
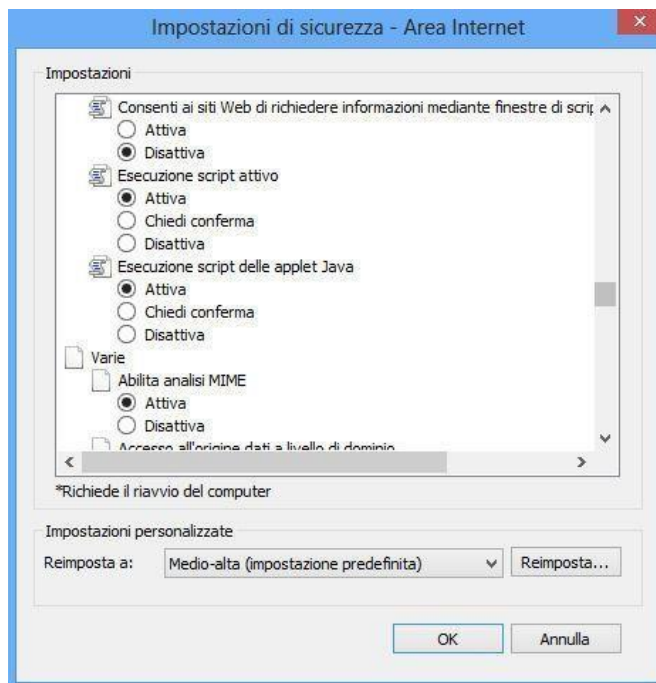
Esempio di configurazione per s.o. Windows 8/10 - 64 bit – Internet Explorer 10/11

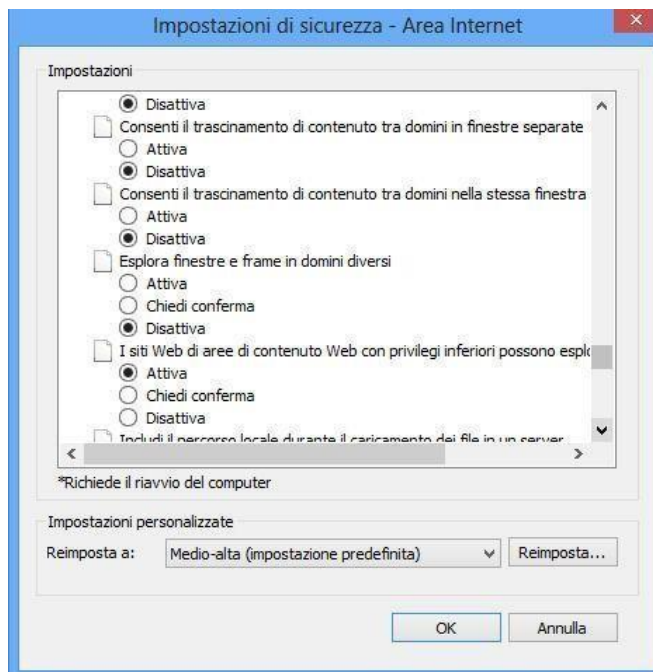
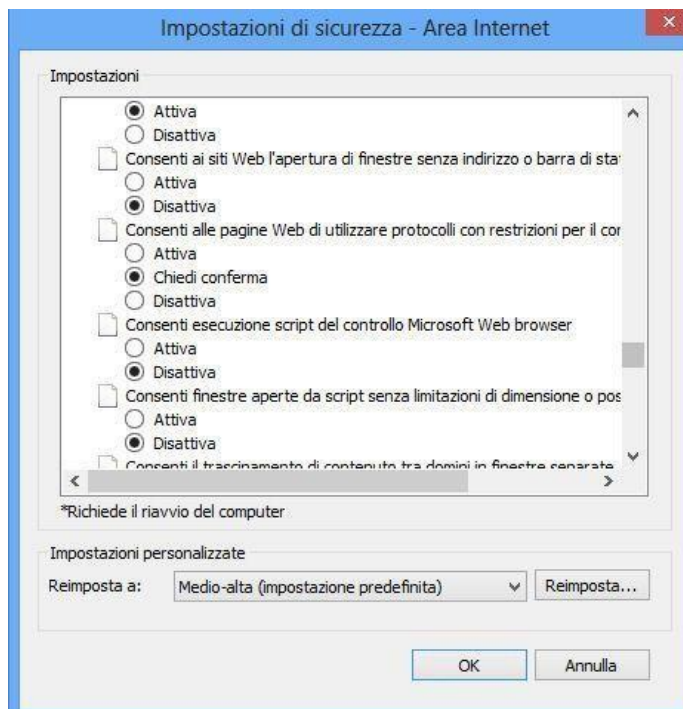


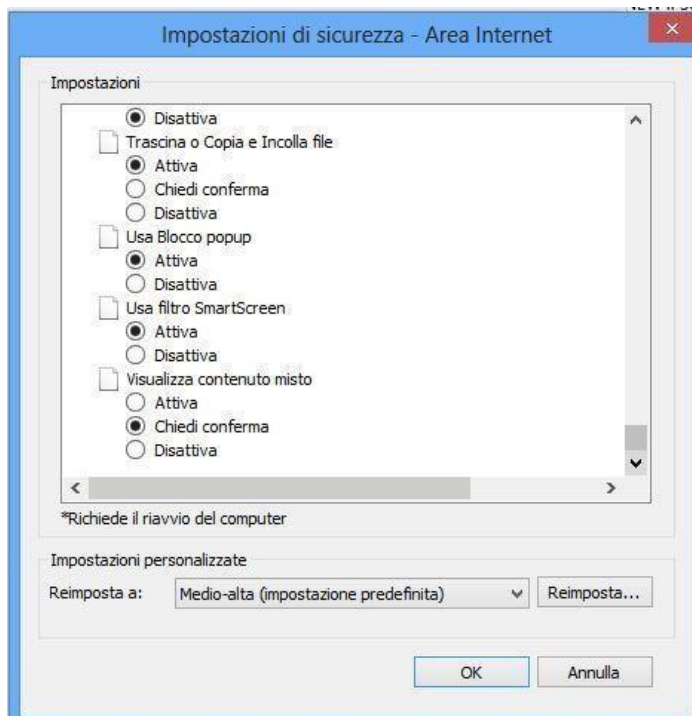
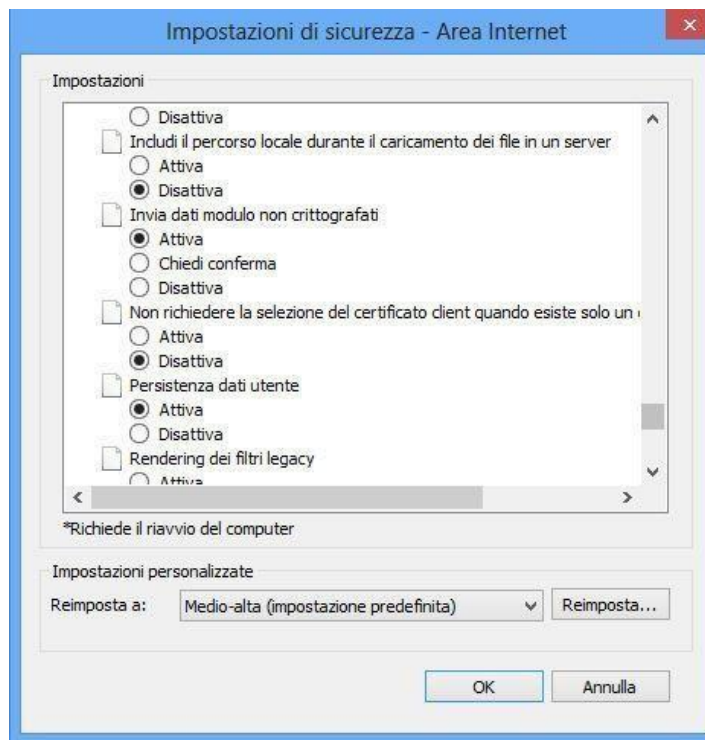


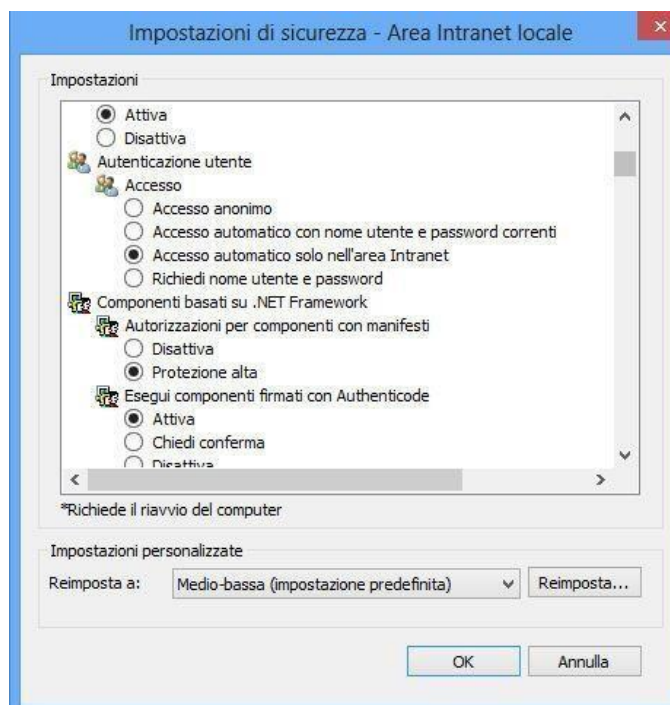
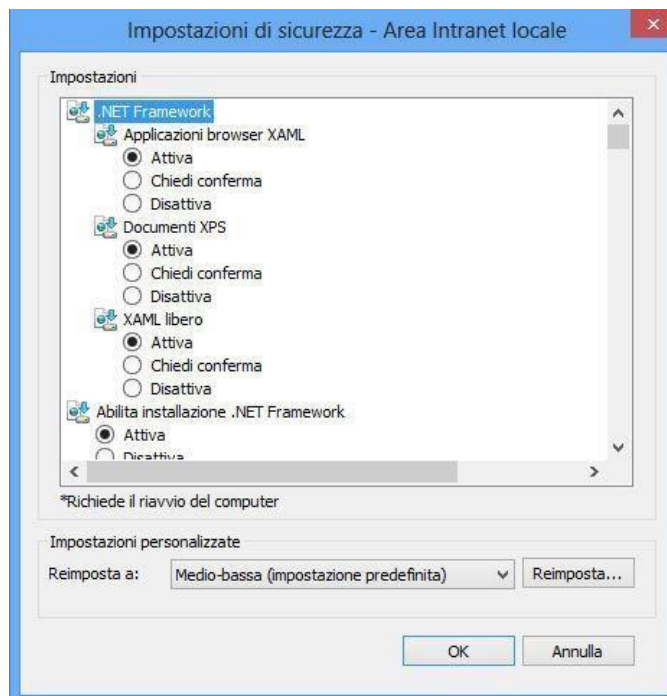


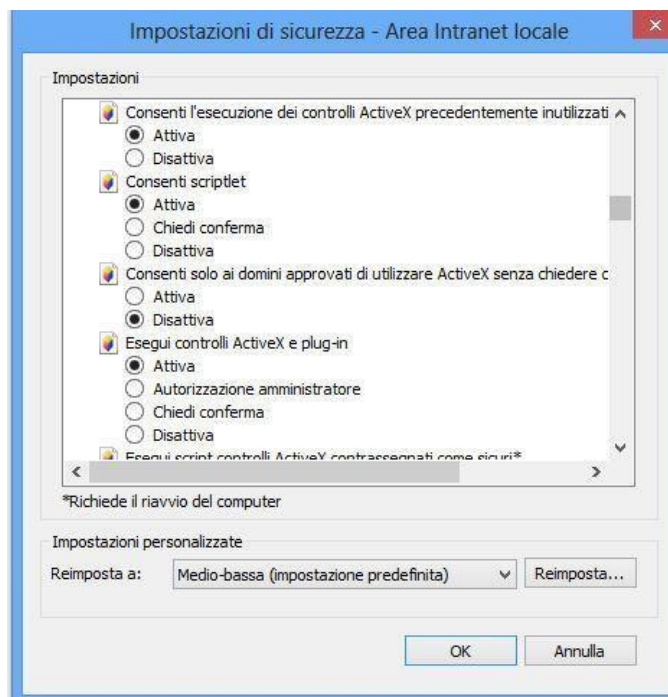
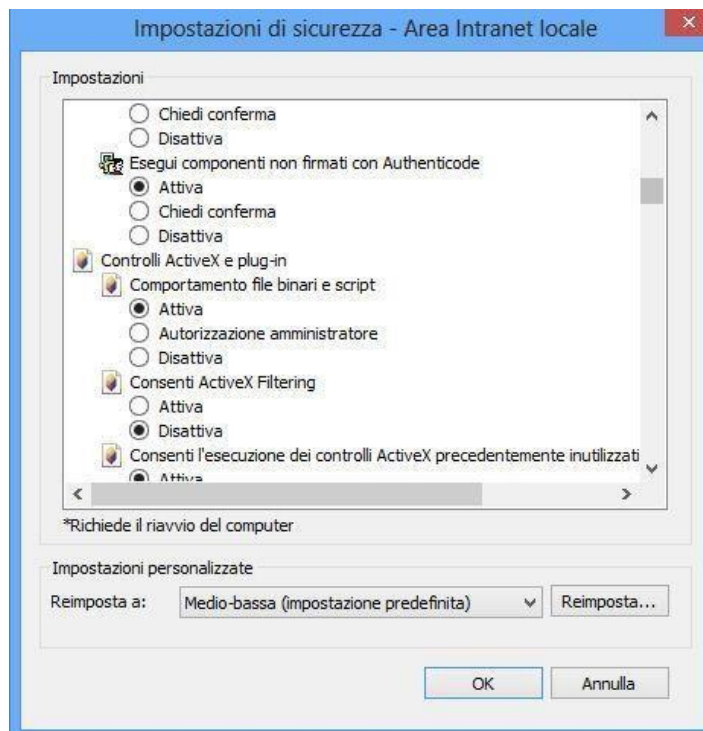




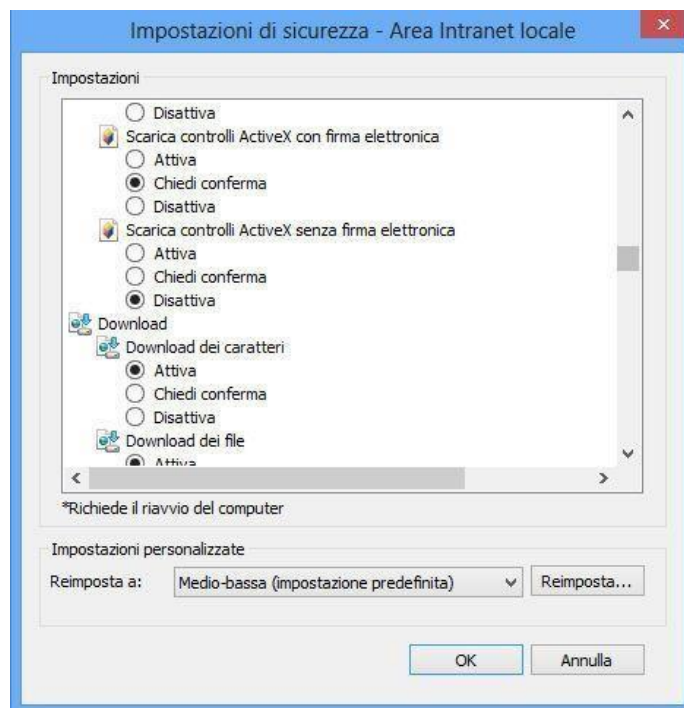
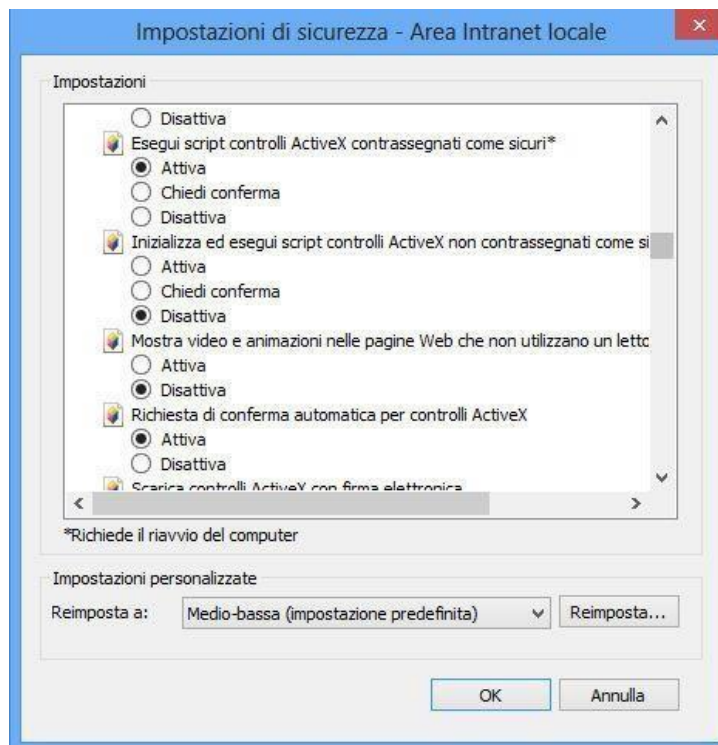




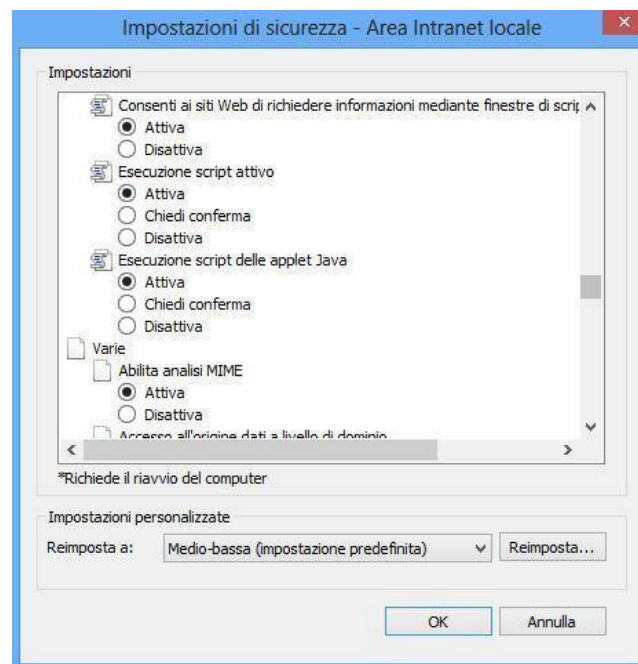
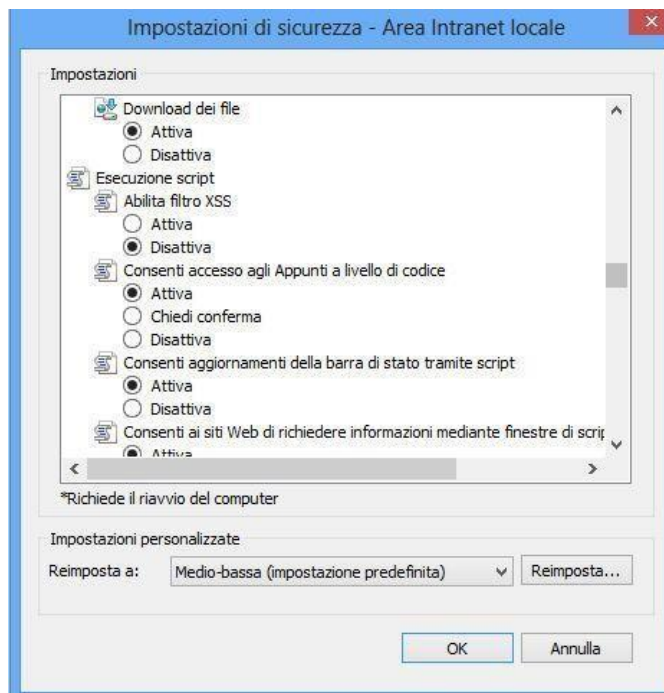


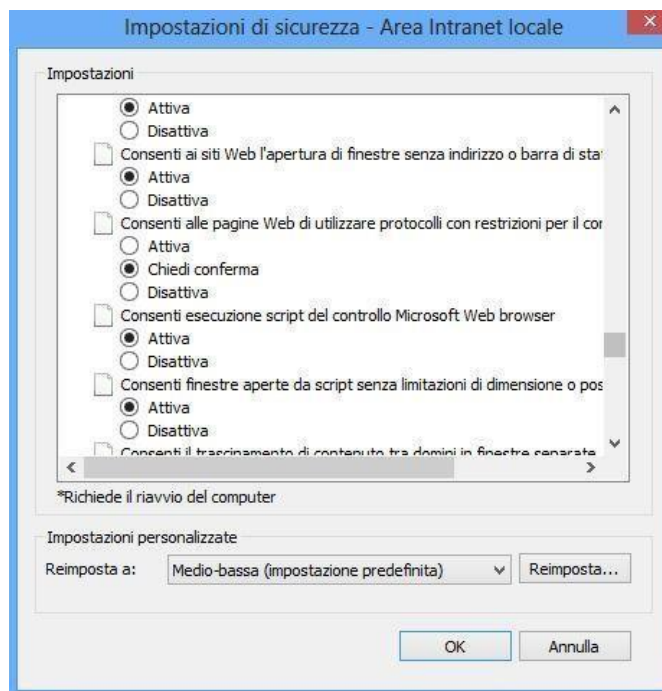
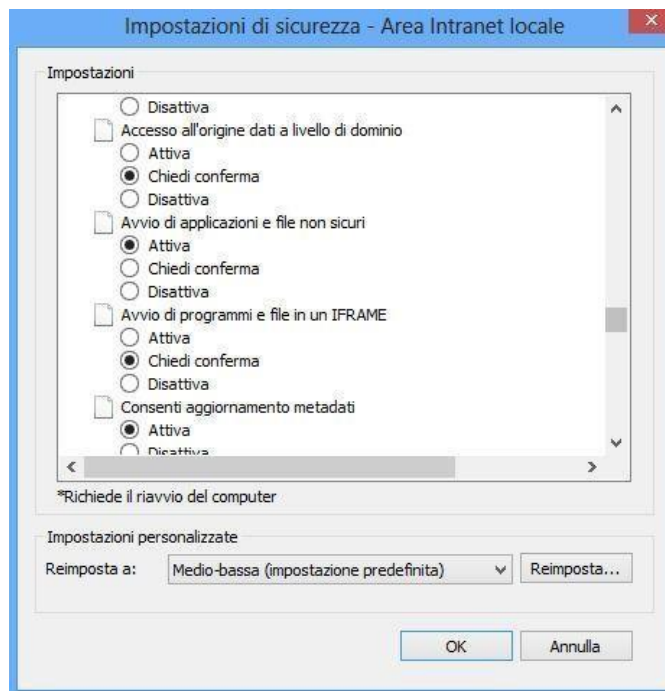


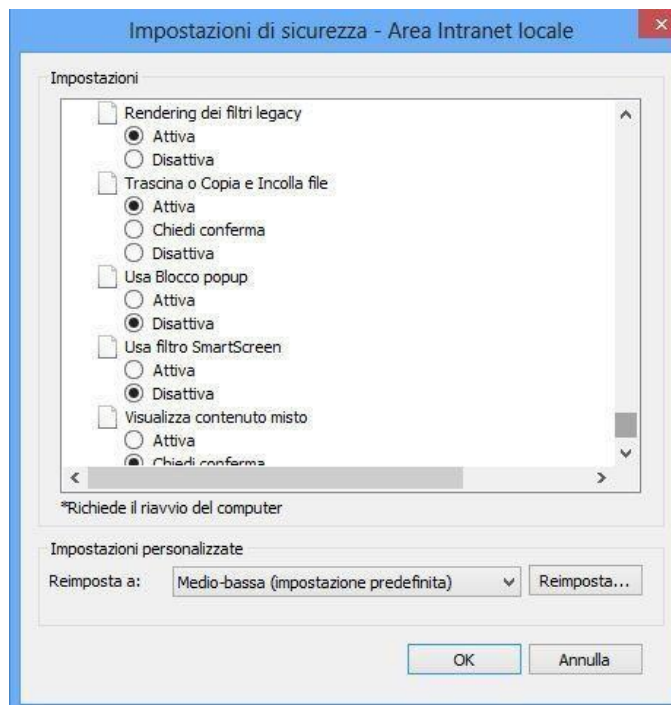
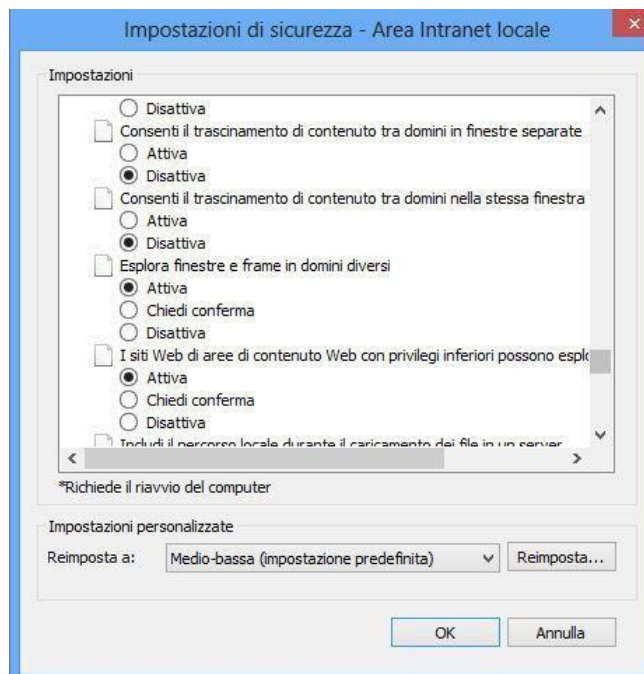


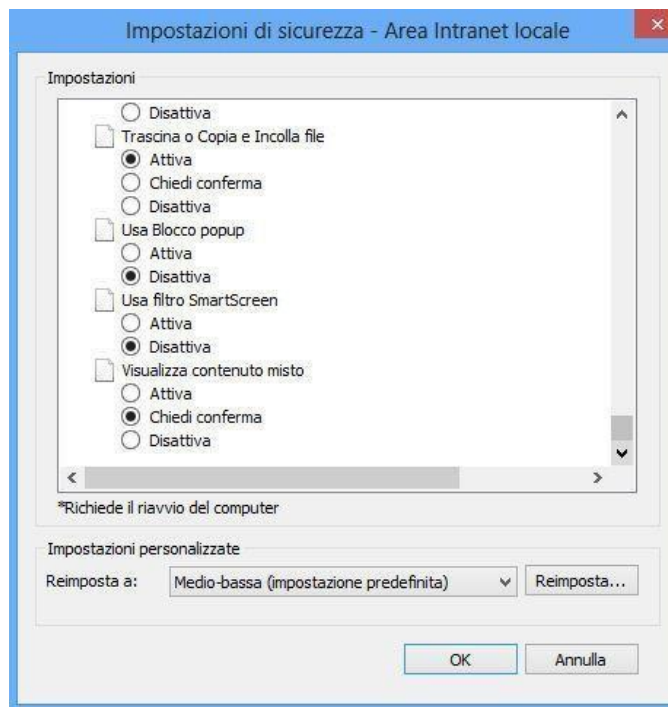






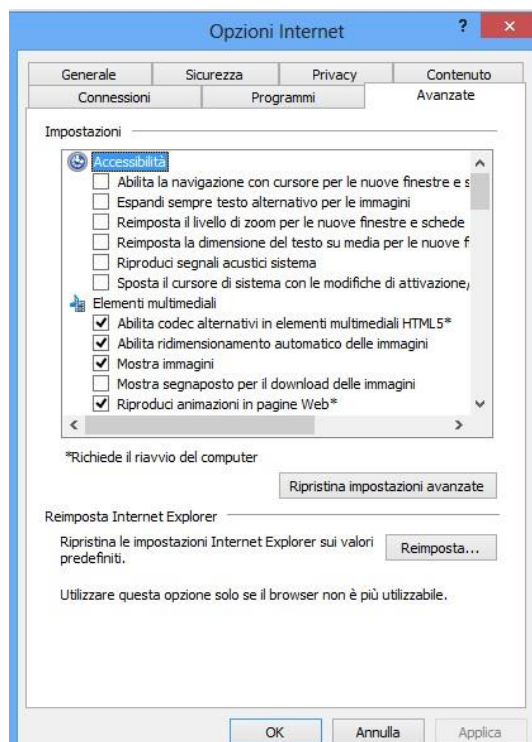


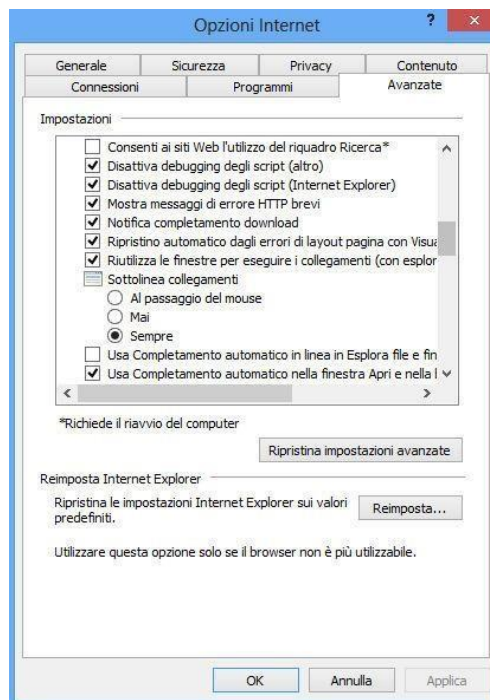
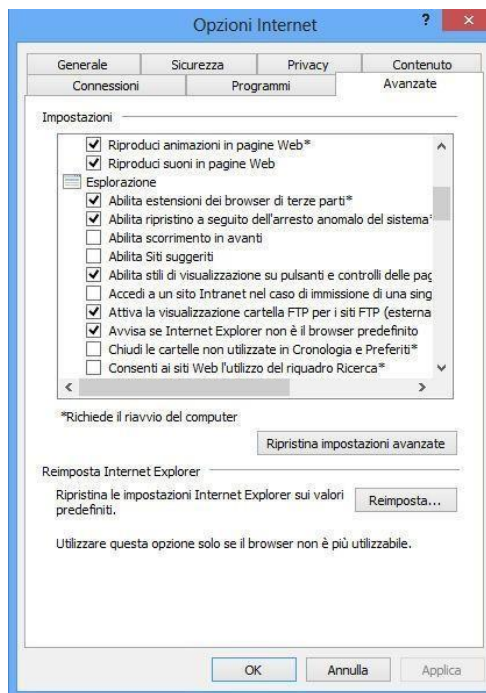


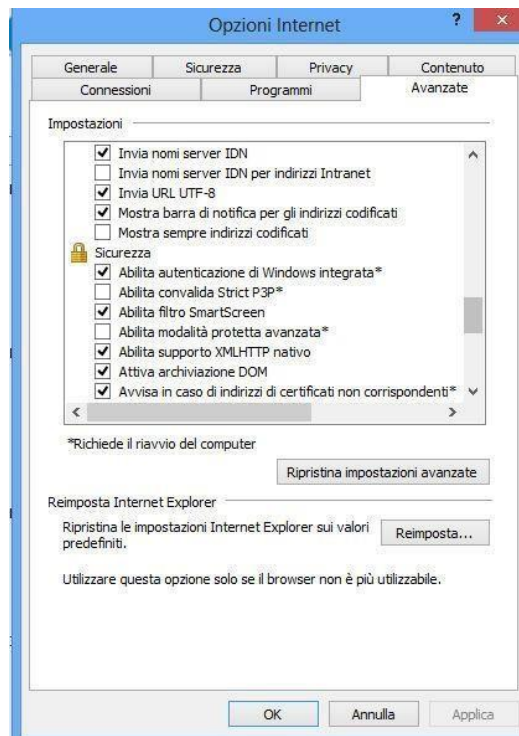
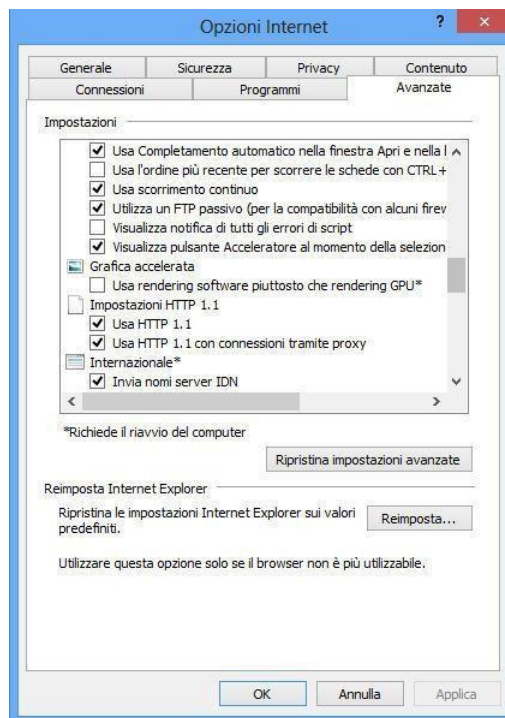


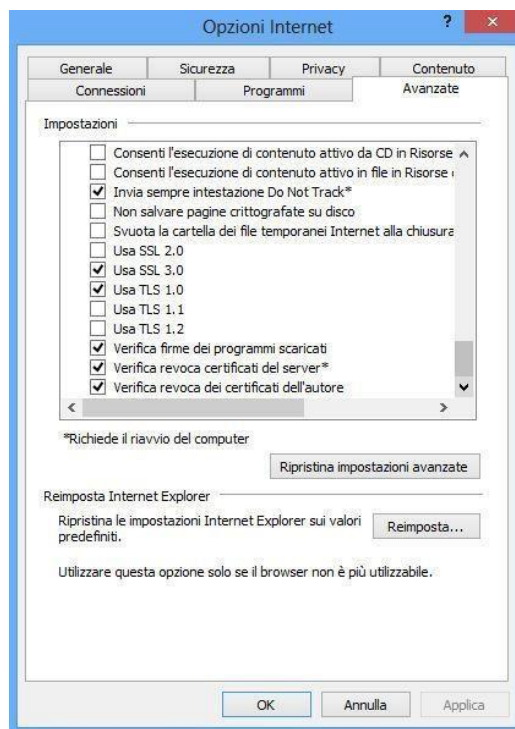
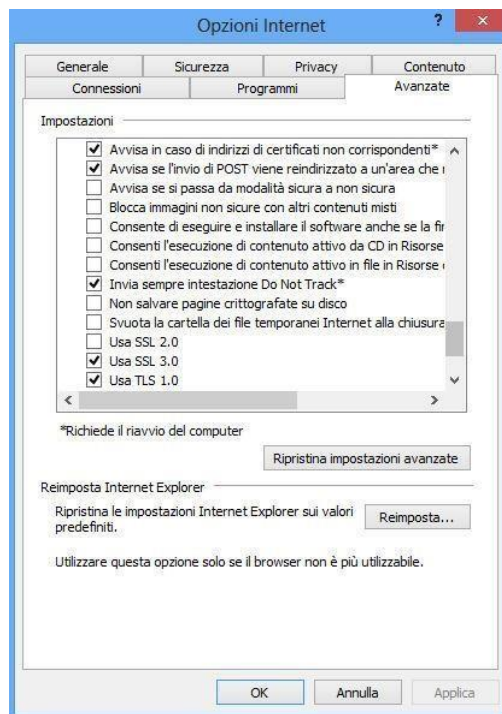
Sucessivamente , sempre da “**Strumenti**”

- clic su “**Opzioni Internet**”
- clic su “**Avanzate**” , controllando le Impostazioni, personalizzandole nel seguente modo:
- 









### 2.1.5 Lettori di smart card

Nella workstation RAO devono essere installati due lettori (Utente e RAO) e i middleware CSP seguenti:

- [www.firma.infocert.it/software/bit4id\\_xpki\\_1.4-ccid.zip](http://www.firma.infocert.it/software/bit4id_xpki_1.4-ccid.zip)
- [www.firma.infocert.it/software/SafeDive2\\_setup.zip](http://www.firma.infocert.it/software/SafeDive2_setup.zip)



E' possibile scaricare i driver dei lettori collegandosi ai link pubblicati nella pagina <http://www.firma.infocert.it/installazione/lettore.php>

### 2.1.6 Microsoft SOAP Toolkit 3.0

SOAP è un protocollo per lo scambio di informazioni in un ambiente distribuito e il Toolkit fornisce interfacce di alto e basso livello che permettono di realizzare Web Services e di invocarli.

Per installare Microsoft SOAP Toolkit 3.0 scaricare il file **soapsdk.exe** direttamente dal link:

<https://www.firma.infocert.it/software/soapsdk.zip>

Attivare soapsdk.exe e rispondere “**Si**” all’installazione del toolkit, cliccare su “**Next**”, “**Accept**” e alla fine “**Install**”.

Terminata l’installazione, aprire il “**Pannello di controllo**”, cliccare su “**Installazione applicazioni**” e verificare che sia presente anche la voce Microsoft SOAP toolkit 3.0 altrimenti eseguire nuovamente l’installazione.



## 2.1.7 Middleware CSP (Cryptografic Service Provider)

Per consentire il corretto utilizzo della postazione RAO è necessario i seguenti middleware CSP (Cryptografic Service Provider):

- [www.firma.infocert.it/software/bit4id\\_xpki\\_1.4-ccid.zip](http://www.firma.infocert.it/software/bit4id_xpki_1.4-ccid.zip)
- [www.firma.infocert.it/software/SafeDive2\\_setup.zip](http://www.firma.infocert.it/software/SafeDive2_setup.zip)

Salvare i file zip in locale ed eseguire doppio click sui file estratti.

## 2.1.8 Token Eutron

Per informazioni su questo tipo di dispositivo è possibile visualizzare il documento presente nella pagina delle “**comunicazioni ai RAO**”, disponibile nel sito dell'Ufficio di Registrazione.

Per l'installazione, si consiglia comunque di contattare l'Assistenza Monitor in quanto sono necessarie delle particolari modifiche nei Registri di Windows per stabilire l'esatto posizionamento del lettore Utente e del lettore RAO in fase di emissione.

## 2.1.9 Installazione Controllo Active X

I componenti ActiveX di emissione (**IcNewCertRA**) e lettura del seriale (**icscsnrX**) vengono installati automaticamente al primo rilascio effettuato da una nuova stazione RAO.

**La prima volta che si procede dunque ad una emissione è necessario innanzitutto essere collegati al computer come utente “Amministratore”; quindi procedere alla registrazione di una richiesta.**

Cliccando sulla funzione per l'emissione della smart card il sistema presenterà automaticamente le maschere per l'accettazione dell'installazione dei componenti ActiveX.

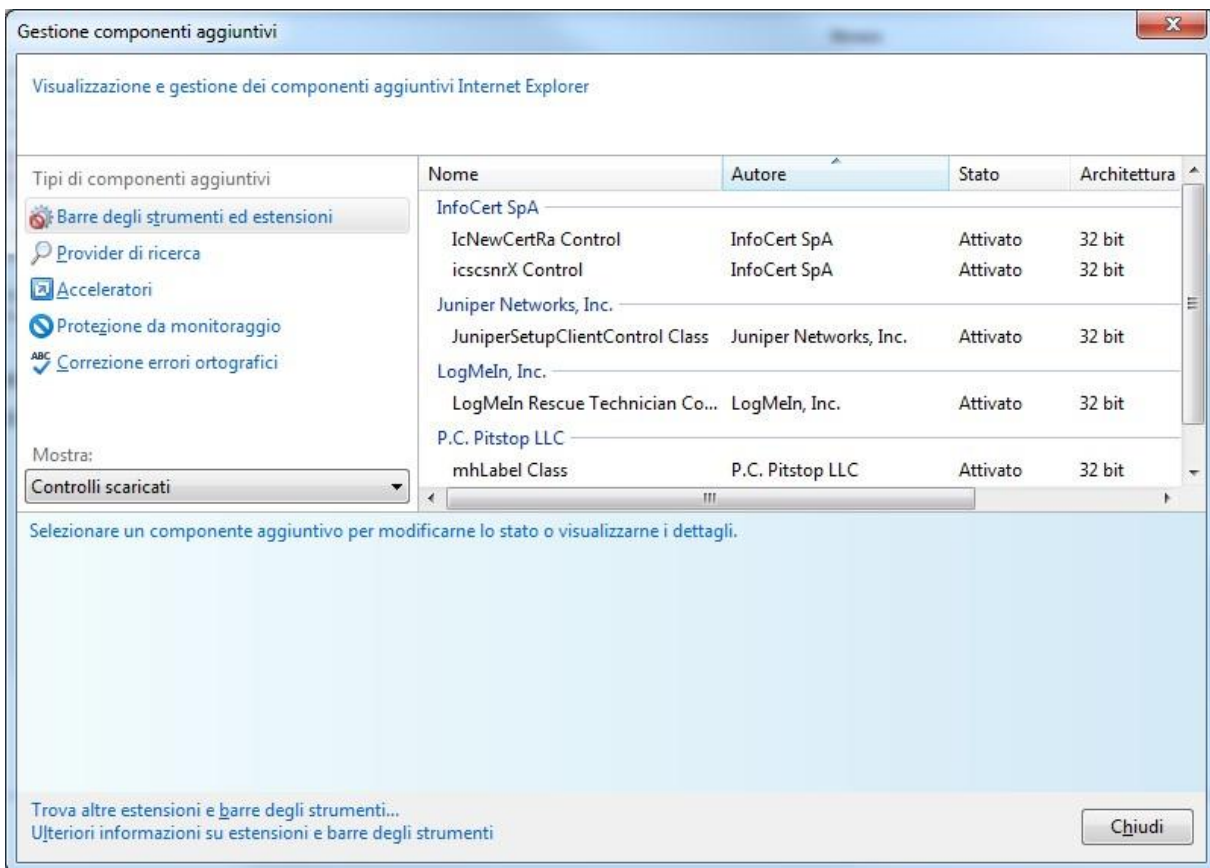
Per l'installazione del controllo **IcNewCertRa** si veda per esempio l'immagine seguente:



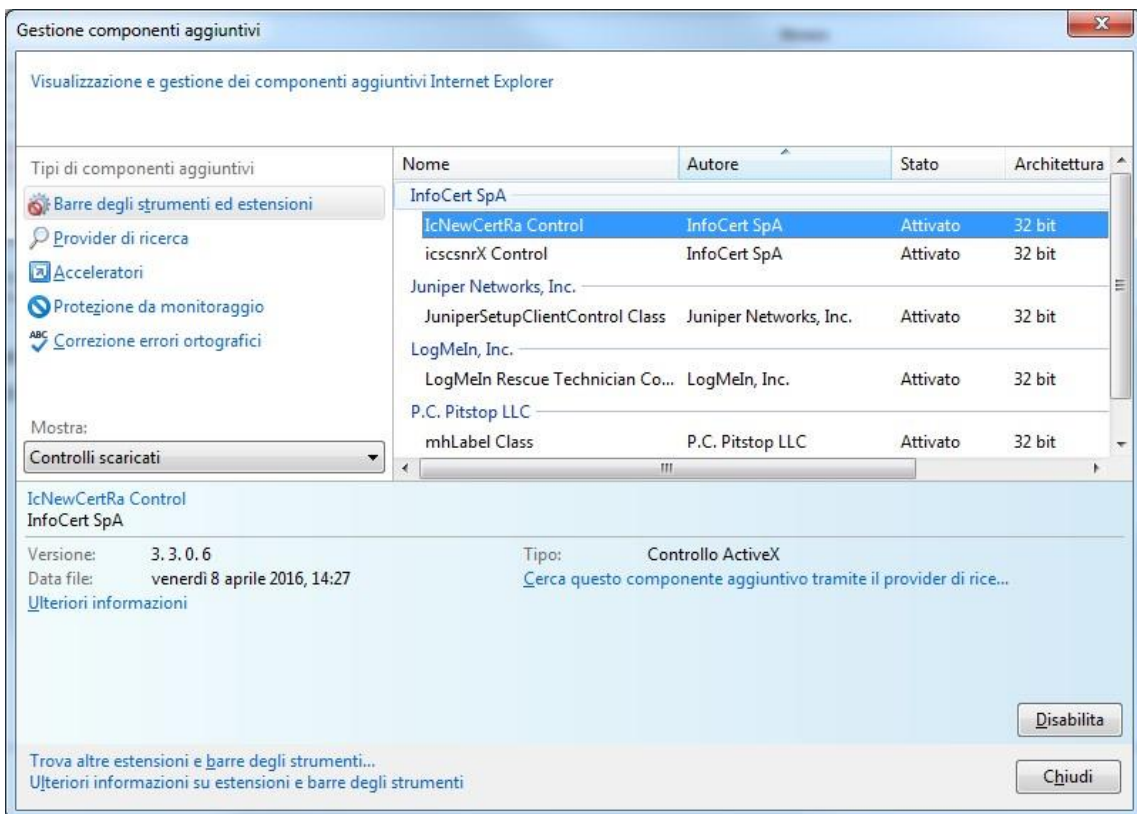
Cliccare su “Installa”.

Terminata l'installazione è possibile verificare che il componente IcNewCertRa sia stato installato correttamente:

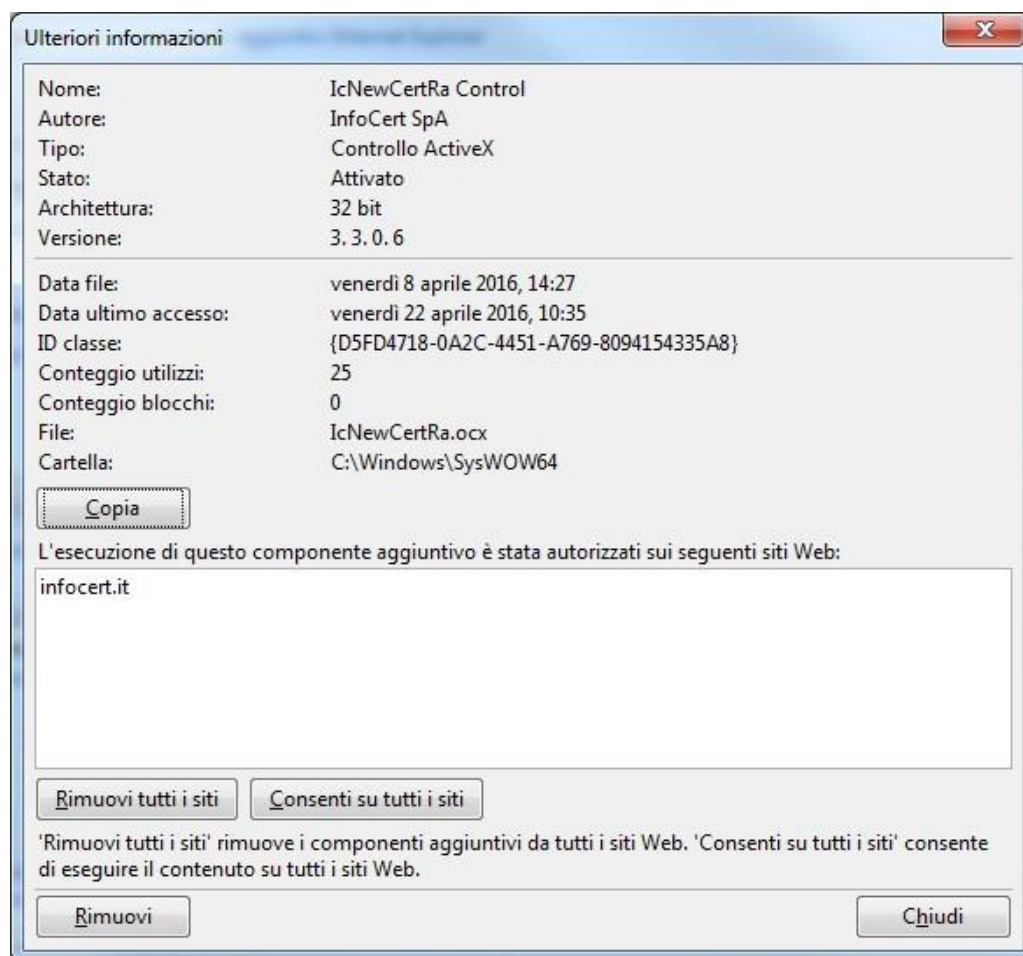
selezionare la voce “**Strumenti – Gestione Componenti aggiuntivi**” dal menù del browser Internet Explorer:



- clic su **“Mostra: Controlli scaricati”** e cliccare sul componente installato **“IcNewcertRa Control”**:



Per ulteriori dettagli andare col tasto destro del mouse e scegliere “**Ulteriori Informazioni**”



### **2.1.10 Installazione Driver per Business Key**

Alla prima emissione di BK, collegarsi alla WS come Utente Amministratore; inserire una BK in una porta USB ed eseguire il software cliccando su autorun.exe. Questa operazione, che può durare anche qualche minuto, installa automaticamente i driver della BK.

## **2.2 File utilizzati dalla procedura**

In caso di necessità o in seguito ad una specifica richiesta da parte dell'Assistenza/Monitor, potrebbe essere necessario procedere alla verifica del file di Log utilizzato dalla procedura: "IcNewcertRa.log".

Il file denominato "**IcNewCertRa.log**", si trova sempre nella directory Utente (tipicamente: <C:\Users\NomeUtente\AppData\Local\Temp>), contiene il log applicativo delle operazioni condotte dal client in fase di emissione, quali:

- dati ricevuti •
- operazioni effettuate
- eventuali errori

E' possibile quindi controllare visivamente quali siano le ultime operazioni compiute, oppure a richiesta, inviarlo al servizio di assistenza per un maggiore controllo sulla postazione utente.

## 2.3 Impostazione Parametri del Proxy

Nel caso in cui una Stazione Rao sia all'interno di una rete con un Proxy (cioè non abbia un accesso diretto verso Internet), E' necessario riportare nel registry di Windows le eventuali impostazioni dei parametri **proxy**, **proxyPort**, **proxyUser** e **proxyPassword**, prima di utilizzare la procedura di emissione.

Le entry da valorizzare nel registry sono le seguenti :

[**HKEY\_LOCAL\_MACHINE\SOFTWARE\InfoCamere\IcNewCertRa**]

"**ProxyServer**"="Nome.proxy:Porta" oppure <CURRENT\_USER> per autenticazione integrata

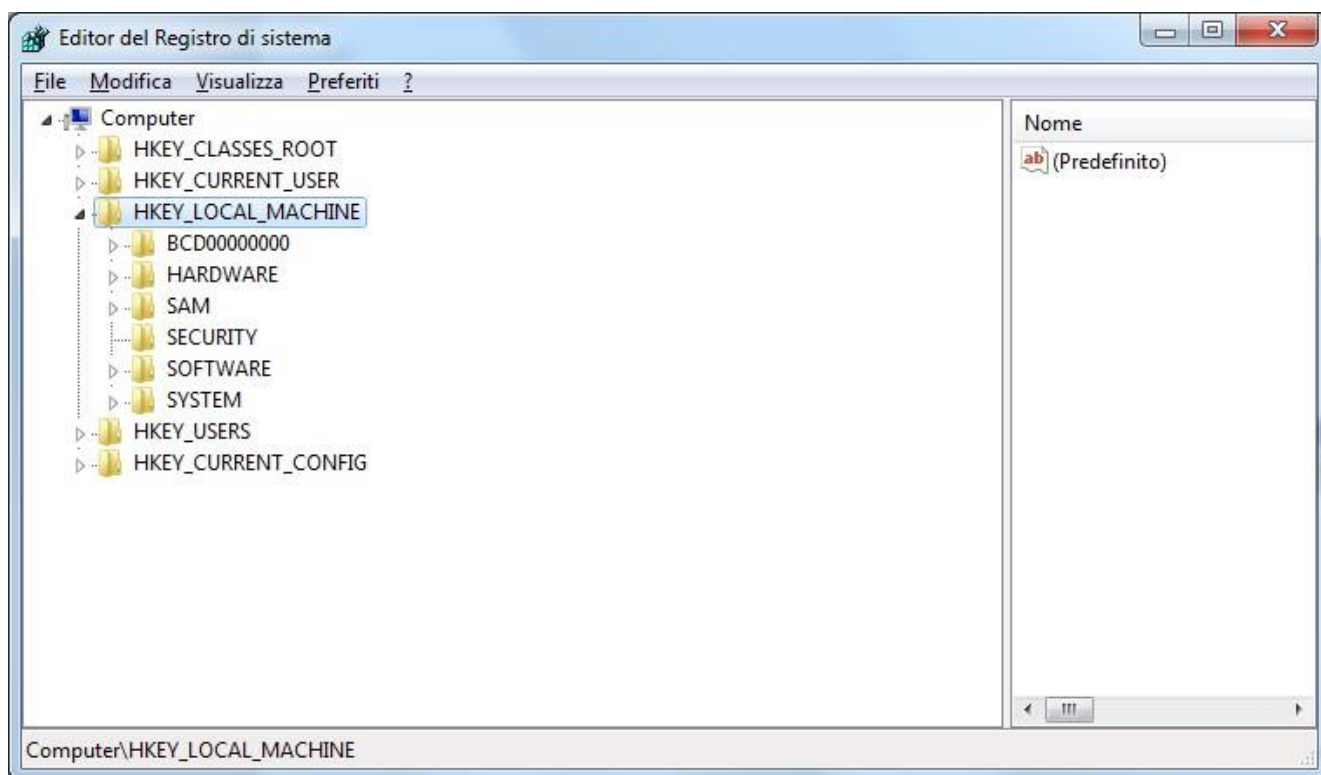
Nel caso in cui l'utente utilizzi anche una user-id e una password per il collegamento ad Internet è necessario impostare anche:

"**ProxyUser**"="User"

"**ProxyPassword**"="password"

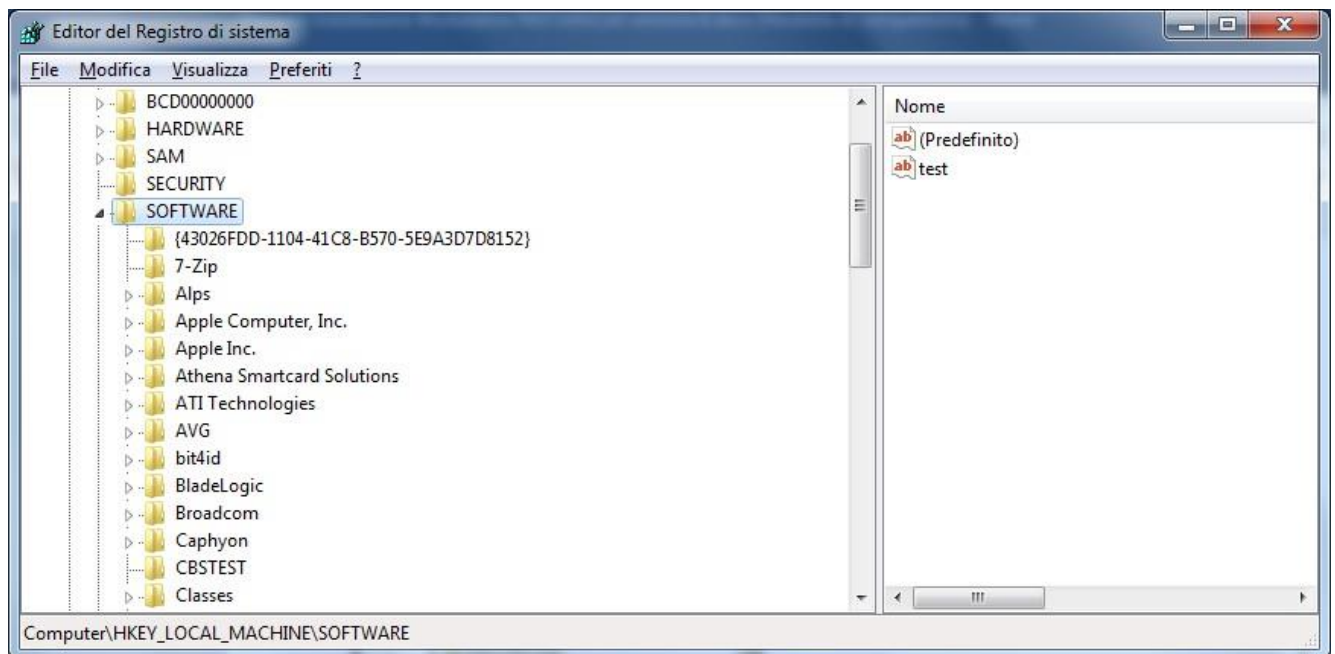
Per valorizzare delle entry nei registry di Windows è necessario utilizzare il comando **regedit** che permette di entrare nei registri di Windows.

Quindi dal Menu **Avvio** si digita **regedit**.

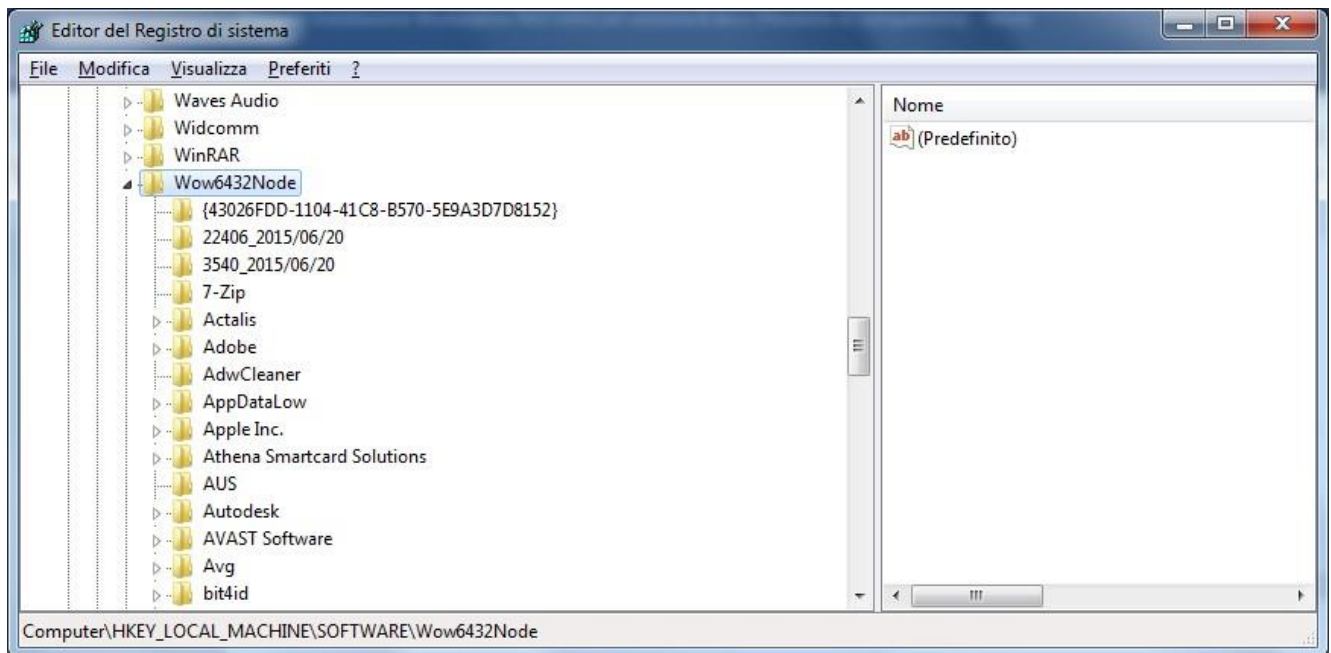


si clicca sul + di **HKEY\_LOCAL\_MACHINE**

poi sul + di **SOFTWARE**

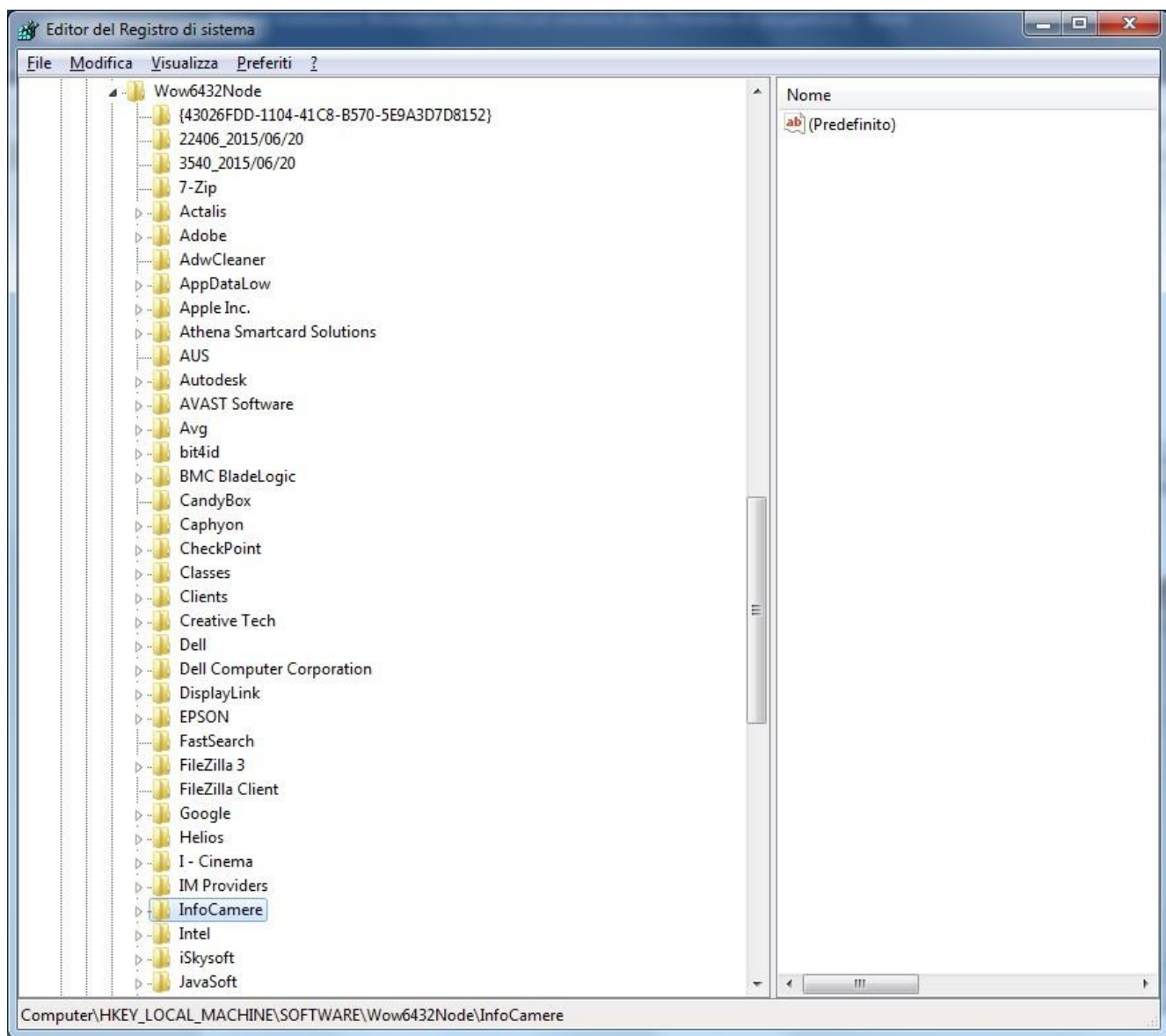


e quindi sul nodo Wow6432Node

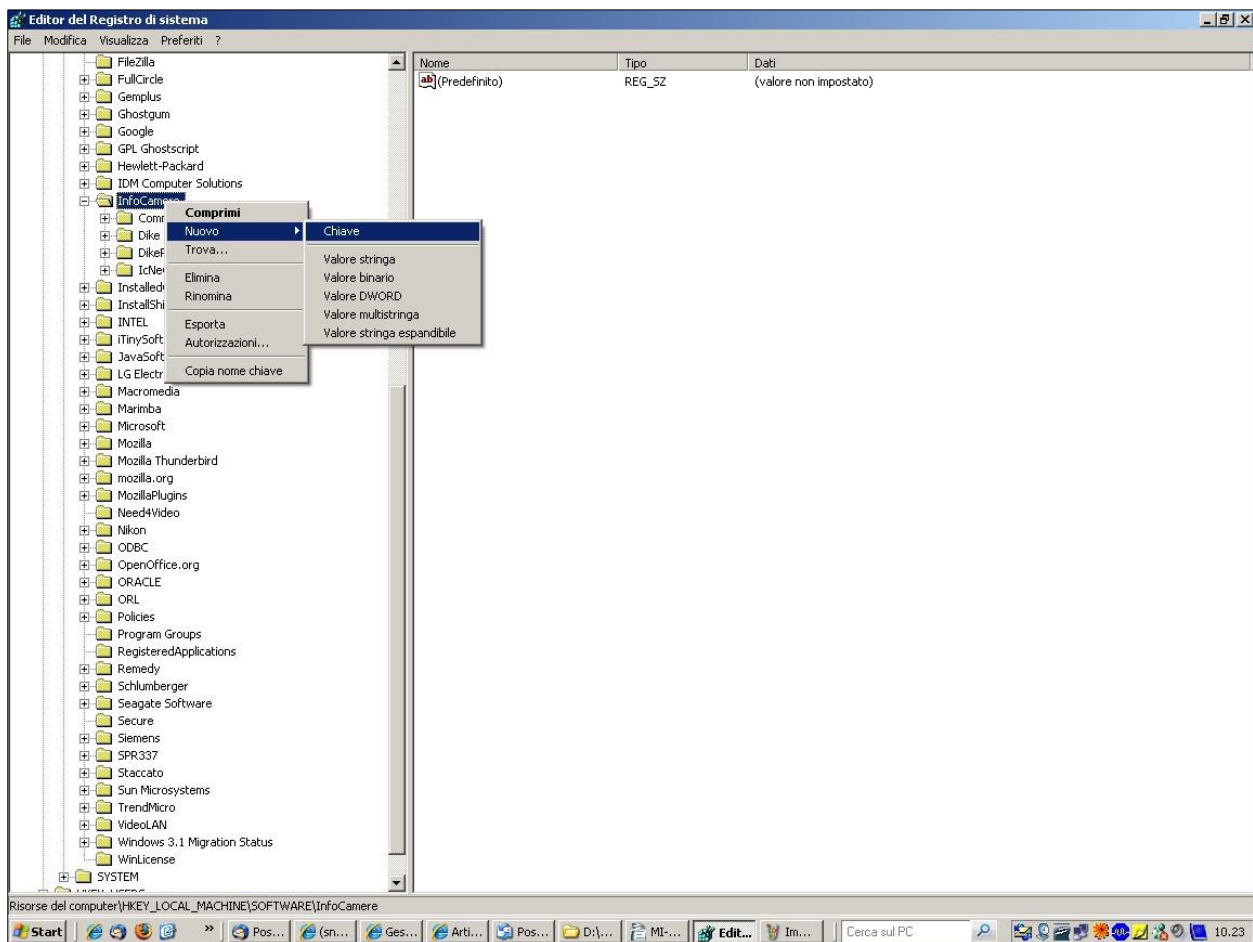


Poi si cerca la voce **InfoCamere** (se non esiste va creata):

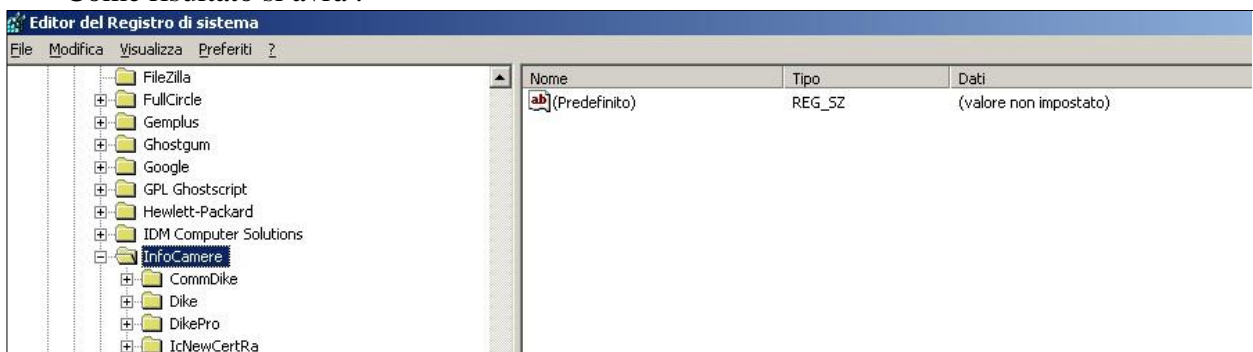




A questo punto per inserire i dati del Proxy è necessario creare la chiave **IcNewCertRa**.  
Tasto DX del Mouse su **InfoCamere – Nuovo – Chiave** e si digita **IcNewCertRa**

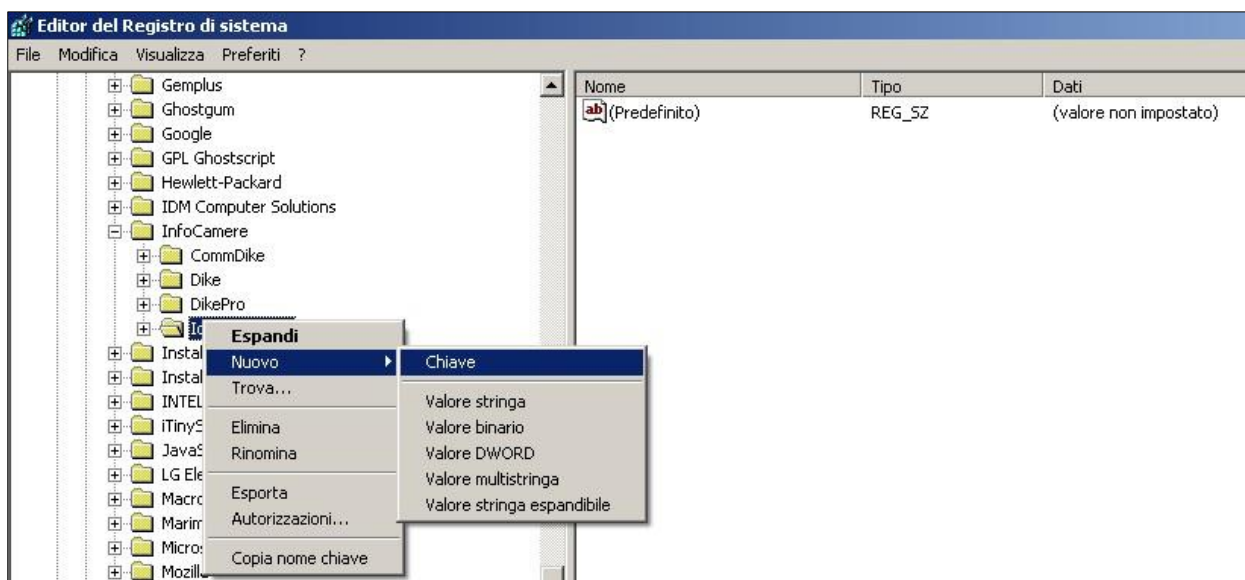


Come risultato si avrà :



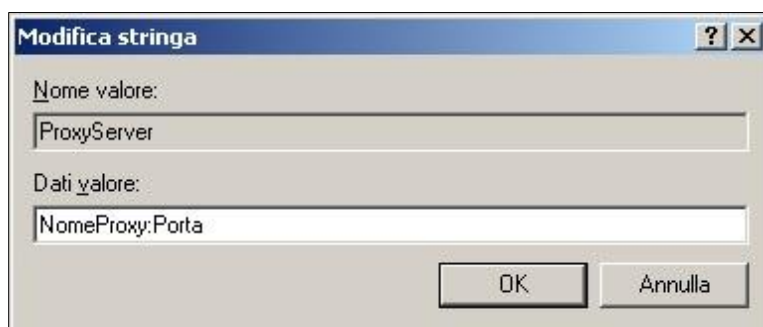
Quindi nuovamente tasto DX del Mouse su **IcNewCertRa** – **Nuovo** – **Valore stringa** :



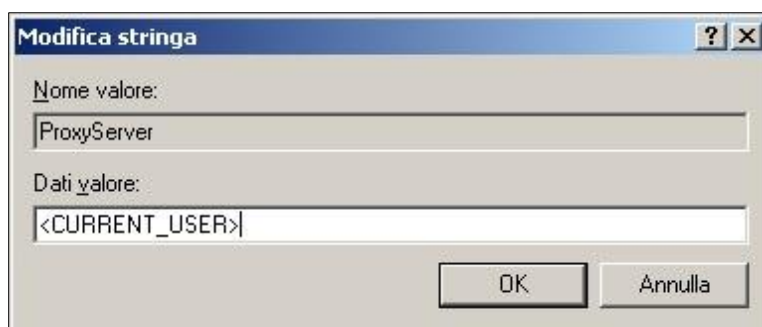


si denomina la Stringa con '**ProxyServer**'.

Una volta creata questa Stringa ci si clicca sopra col tasto DX del Mouse – **modifica** si inseriscono i parametri del Proxy



oppure



Si consiglia di utilizzare questo secondo tipo configurazione perchè ha l'autenticazione integrata e non è necessario inserire **ProxyUser** e **ProxyPassord**

Qualora fosse necessario inserire anche la user e la password per il Proxy bisogna creare altre due Stringhe denominate **ProxyUser** e **ProxyPassword** nella stessa modalità di come abbiamo

fatto per la Stringa **ProxyServer**, inserendo come valore delle stringhe la user-id e la password di accesso ad Internet.

## 2.4 Test postazione client

Nella pagina di emissione della smart card, è presente una funzione dedicata esclusivamente al test della postazione RAO. Tale funzione, selezionabile attraverso il link “**Rilascio smart card**” contenuto nella parte superiore della pagina stessa, attiva una serie di controlli che possiamo riassumere in:

- verifica parametri di colloquio con il server •
  - installazione di tutte le componenti client •
  - test della comunicazione con la parte server della CA
- Se tutto è OK verrà visualizzato un Popup del tipo:



Ovviamente si clicca su “**OK**”

Nel caso di errori, questi verranno segnalati direttamente all’utente tramite MessageBox e scritti sul file di log (vedi anche il Manuale Utente Ufficio di Registrazione).

Si consiglia di effettuare questo test prima di iniziare a fare le emissioni soprattutto se è trascorso un certo periodo di tempo dall’ultima effettuata.

## 3. Workstation IR informatizzato

### 3.1 Prerequisiti

L’Incaricato della Registrazione informatizzato, per poter svolgere la sua attività deve utilizzare un computer con sistema operativo aggiornato Microsoft Windows.

Per utilizzare il browser di Microsoft per la navigazione SSL (autenticazione sicura, firma su moduli online...), è necessario installare i moduli CSP (Cryptographic Service Provider), i software indispensabili per l’importazione del certificato di autenticazione nello store Microsoft.

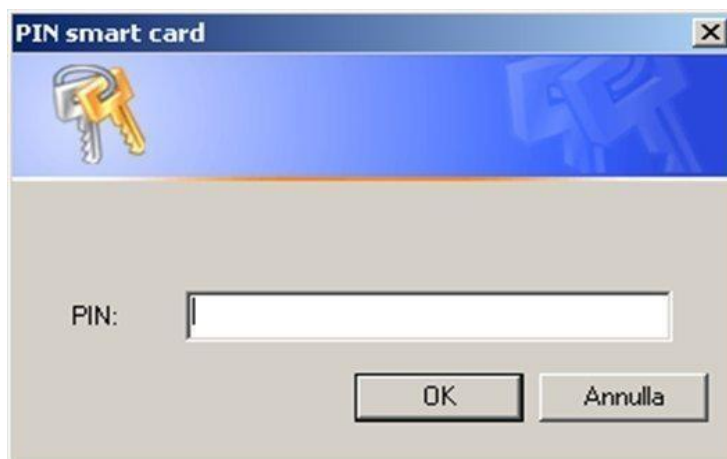
Per installare i CSP è necessario collegarsi a queste url:

- [www.firma.infocert.it/software/bit4id\\_xpki\\_1.4-ccid.zip](http://www.firma.infocert.it/software/bit4id_xpki_1.4-ccid.zip) ○
- [www.firma.infocert.it/software/SafeDive2\\_setup.zip](http://www.firma.infocert.it/software/SafeDive2_setup.zip)

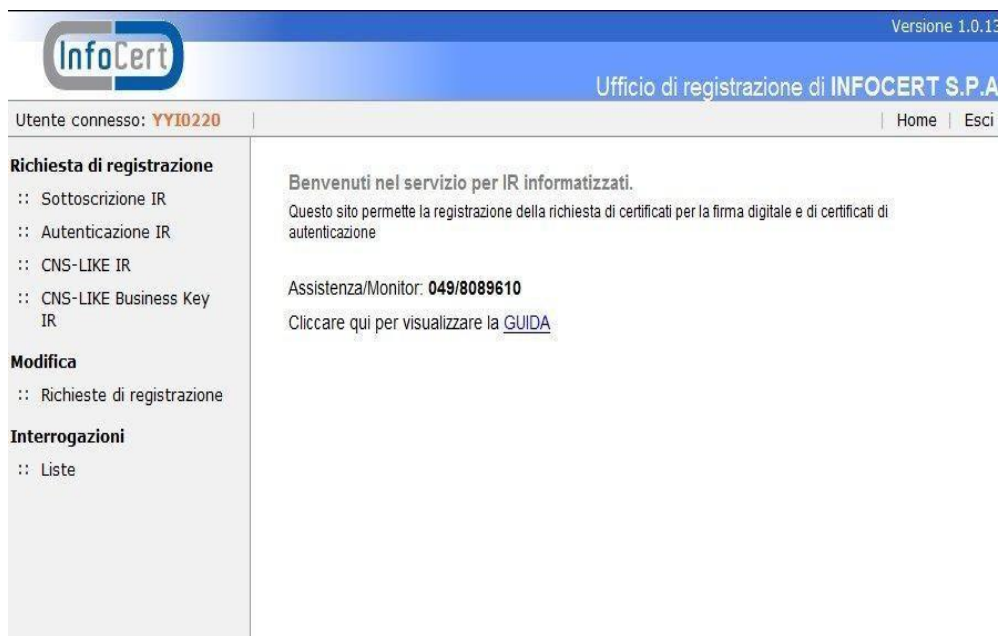
e, dopo aver letto le istruzioni, scaricare il CSP relativo al dispositivo in possesso dell’IR, che contiene un certificato di autenticazione o di tipo CNS, rilasciato dall’Ente Certificatore Infocert.

### 3.2 Collegamento al modulo online

L'Incaricato della Registrazione informatizzato, dopo aver verificato i prerequisiti di cui sopra e dopo aver inserito nel lettore la propria smartcard, si dovrà collegare all'url: <https://ncarir.infocert.it> e alla relativa richiesta inserire il pin, come nell' immagine:



Dopo aver inserito il pin, sarà consentito l'accesso alla pagina iniziale per le registrazioni delle richieste di certificato, (vedi immagine)



e proseguire con la normale attività di registrazione.