

MUDE Piemonte

Modalità operative di configurazione e accesso al sistema MUDE

STATO DELLE VARIAZIONI

Versione	Paragrafo o Pagina	Descrizione della variazione
V01	Tutto il documento	Versione iniziale del documento
V02	Paragrafo 2.2	
V03	Paragrafo 1.1.2 Paragrafo 2.2	Le novità sono evidenziate in giallo .

Sommario

1. CERTIFICATI DIGITALI	2
1.1 Kit di firma digitale	4
1.1.1 Smart card	4
1.1.2 Business Key.....	4
2. CONFIGURAZIONE DEGLI STRUMENTI UTILIZZATI	8
2.1 Firma digitale.....	8
2.2 Browser e sistemi operativi	9
2.3 Adobe Reader.....	12
2.3.1 Modulo aggiuntivo per Adobe Reader	12
2.3.2 Configurazione Reader versione 9	14
2.3.3 Configurazione Reader versione 10	16
2.4 Adobe Flash Player (plugin per browser).....	17
3. ACCESSO APPLICATIVO MUDE.....	18
3.1 Accreditamento	18
3.2 Autenticazione.....	19
4. ALLEGATO: ELENCO ENTI CERTIFICATORI	20

1. Certificati digitali

Di seguito vengono fornite alcune indicazioni di carattere generale utili e in alcuni casi da eseguire per poter accedere al servizio MUDE 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 MUDE Piemonte aderisce alla normativa vigente di CNIPA in merito all'autenticazione applicativa, pertanto accetta come certificato di autenticazione i certificati della Carta Nazionale dei Servizi (CNS).

Sul sistema non sono caricati di default tutti i tracciati degli Enti Certificatori CNS compliant, ma solamente quelli che fino ad oggi hanno effettuato accessi verso il sistema.

IMPORTANTE: se il sistema non riconosce il vostro certificato digitale ma il certificatore rientra fra quelli presenti nell'elenco di seguito riportato, comunicatelo via mail a:
edilizia.privata@csi.it
affinché si possa provvedere alla necessaria configurazione a sistema e permettere l'accesso alle procedure.

In allegato al fondo del documento trovate l'elenco degli enti certificatori.

I kit di firma digitale devono necessariamente contenere al loro interno due certificati:

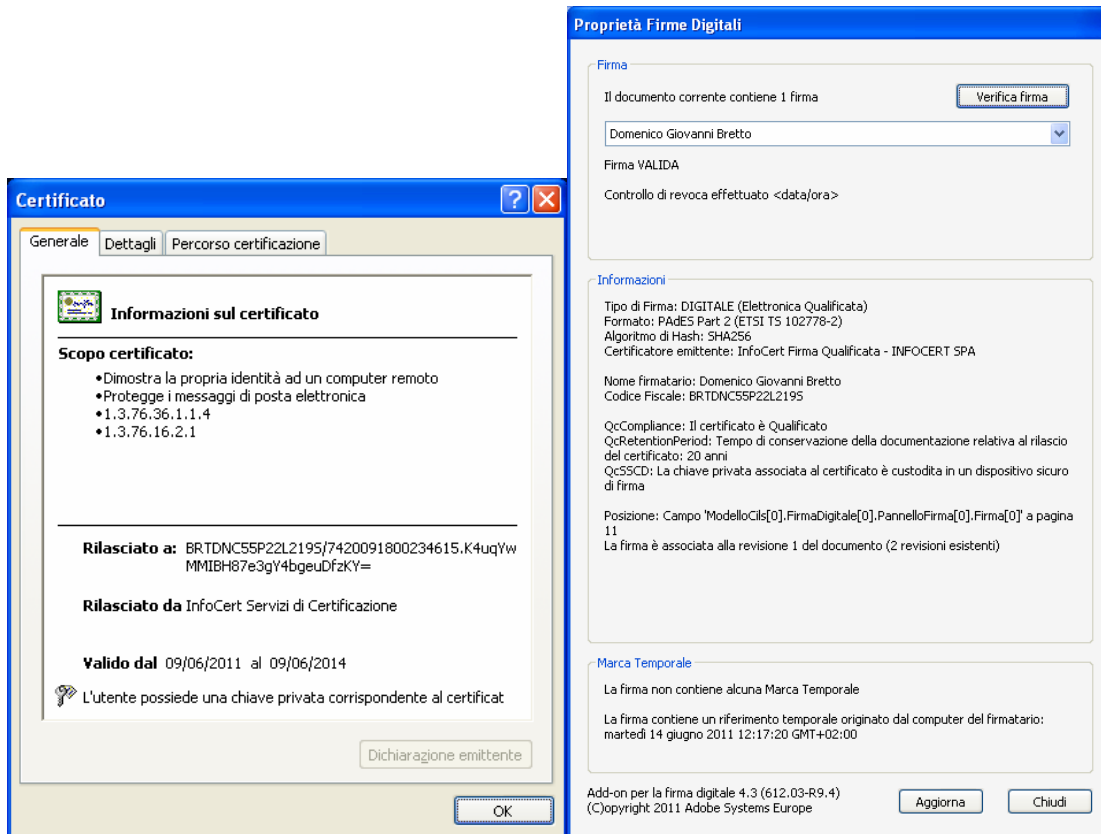
- certificato di autenticazione necessario per essere riconosciuti dal sistema;
- certificato di firma per firmare digitalmente i documenti

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

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

Nel manuale del vendor 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.

Esempio di certificato di autenticazione e certificato di firma rilasciato da Infocert.



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



1.1 Kit di firma digitale

1.1.1 Smart card

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

- ✓ Explorer: menu Strumenti => Opzioni => Contenuto => Certificati => Personale => Importa certificato.
- ✓ Firefox: menu Strumenti => Opzioni => Avanzate => Cifratura => Mostra certificati => Personali => Importa
- ✓ 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 viene riconosciuto automaticamente ad ogni accesso al sistema MUDE. Se sul browser persistono più certificati, il browser presenta una finestra di dialogo per la scelta del certificato opportuno.

Quindi viene richiesto il PIN e si accede al sistema.

1.1.2 Business Key

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 l'autorun che permette la visualizzazione dei menu operativi.

Autorun di Aruba



Autorun di Infocamere

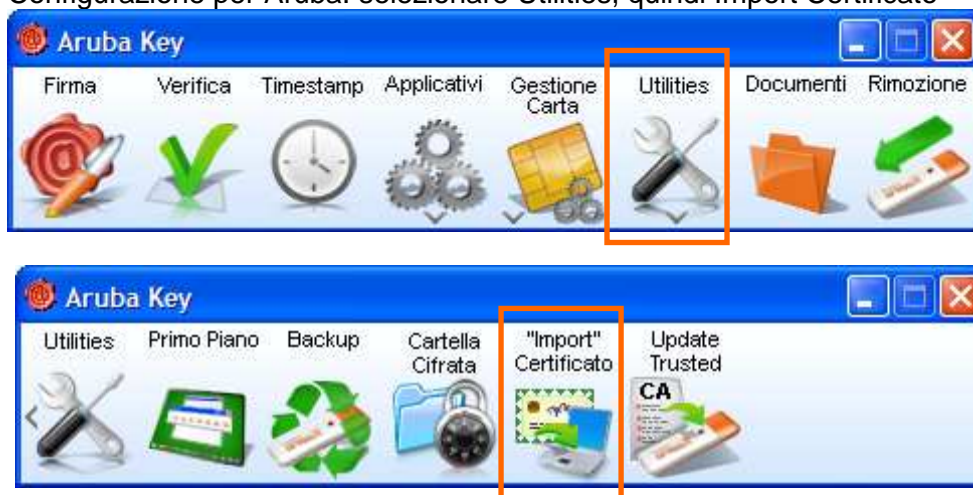


Nel caso in cui l'autorun NON attivi il menu operativo, utilizzare le risorse del computer per visualizzare il contenuto della chiavetta ed eseguire manualmente il file Autorun.exe che si trova nella radice principale della chiavetta.

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 directory \\windows\system32 un file che, a seconda del tipo di certificato utilizzato, può chiamarsi "bit4ipki.dll" oppure "bit4opki.dll".

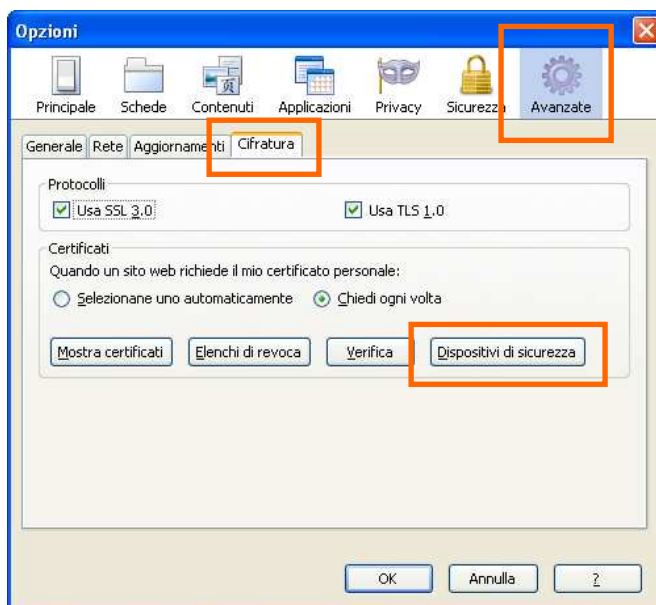


Il file installato permette ai browser presenti sul computer di individuare i certificati digitali presenti nella chiavetta.

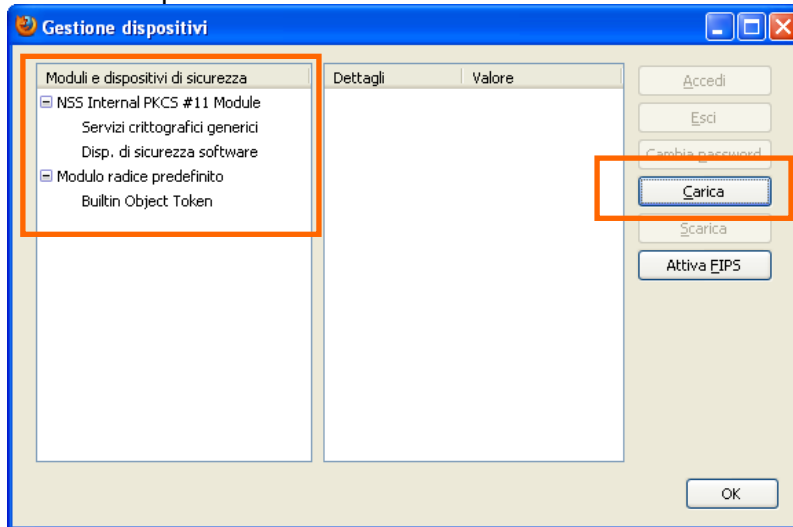
Tuttavia esistono comportamenti diversi a seconda del browser: Explorer e Chrome identificano automaticamente il file installato e quindi il posizionamento dei certificati sulla chiavetta; mentre per FireFox è necessario procedere con l'installazione manuale del file.

Configurazione di FireFox residente sul proprio computer.

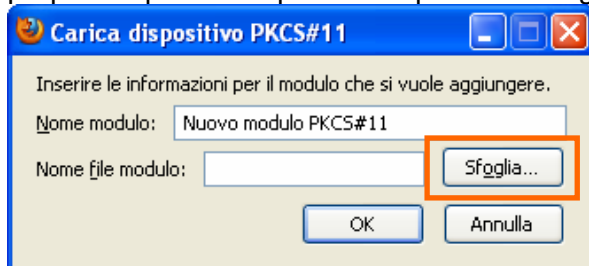
Eseguire FireFox, quindi dal menu Strumenti selezionare Opzioni => Avanzate => Cifratura E selezionare il pulsante Dispositivi di sicurezza



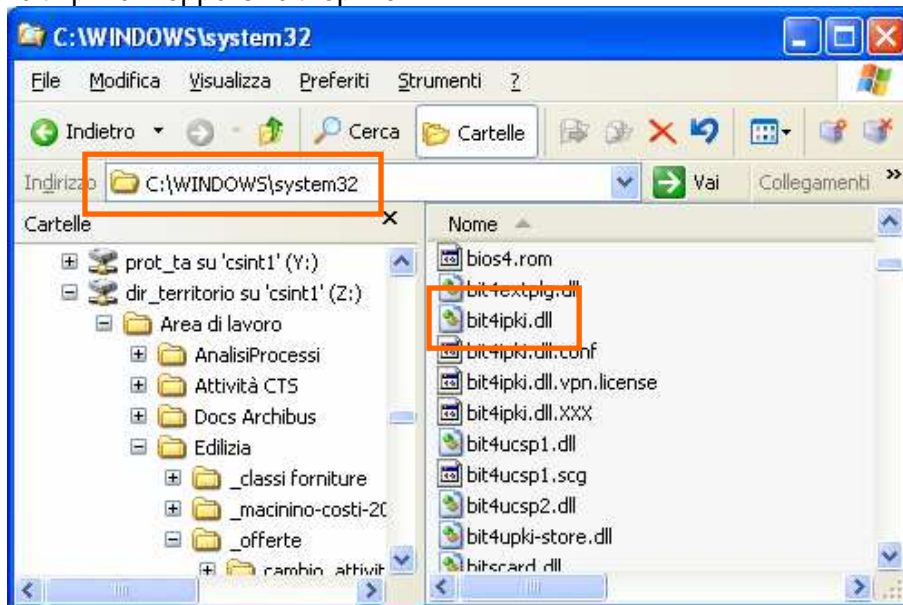
Tipicamente vengono visualizzati solo due dispositivi, per aggiungere quello di interesse cliccare sul pulsante Carica.



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



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. Configurazione degli strumenti utilizzati

L'esecuzione sul lato client della soluzione MUDE richiede l'uso di alcuni strumenti software. La parte applicativa è una soluzione di tipo web quindi è richiesto l'uso di un browser, mentre per la compilazione della modulistica è richiesto il software AdobeReader.

Sulla propria postazione di lavoro gli strumenti necessari per operare ai fini del sistema MUDE sono tre:

- modulo per apporre la firma digitale
- un browser per l'accesso a internet
- il prodotto Adobe Reader nella versione 9 o successive
- Adobe Flash Player (plugin per browser)

Tutti questi moduli sono gratuiti, scaricabili da Internet o forniti con il kit di firma digitale.

2.1 Firma digitale

Si considera in questo caso la firma digitale da apporre in locale ai file (PDF) che saranno allegati alle istanze MUDE 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 menu Firma Digitale.



2.2 Browser e sistemi operativi

I browser sui quali sono stati effettuati sufficienti test sono quelli maggiormente diffusi: Explorer, Mozilla Firefox, Google Chrome.

Browser supportati:

- Internet Explorer 6 e superiori (sufficientemente garantito da test interni su sistema windows XP SP3)
- Mozilla Firefox 3.6 e superiori (sufficientemente garantito da test interni su sistema windows XP SP3)

Browser potenzialmente supportabili:

- Google Chrome (disponibile per alcuni sistemi Windows, Mac OS e Linux); tuttavia questo prodotto ~~NON~~ permette una visualizzazione corretta della componente cartografica.
- Google Chrome è stato provato, ma non ancora sufficientemente testato, con sistema operativo Windows XP.

Il sistema operativo Windows7 è stato provato, ma non ancora sufficientemente testato, con i browser Explorer7 e FireFox5. Durante le prove è stato possibile navigare la parte applicativa web ed effettuare la compilazione del modello e firmarlo digitalmente.

Il sistema operativo Windows Vista è stato testato con Explorer 9 e con FireFox Portable contenuto nella chiavetta di firma digitale. In particolare per funzionare correttamente con Explorer 9 è necessario attivare la "Visualizzazione compatibilità", come descritto di seguito, in questo modo si rendono operative le funzionalità del browser previste dal sistema (visualizzazione della cartografia e attivazione delle tendine per la scelta di Provincia e Comune). Mentre con FireFox Portable tutto funziona correttamente, comprese le attività relative all'apposizione della firma digitale sul modello, senza dover effettuare alcuna operazione sul browser.

Il sistema operativo Macintosh (Mac OS X) versione 10.6 è stato provato nell'unico modo previsto dal sistema Mac è cioè con il browser FireFox Portable contenuto nella chiavetta di firma digitale, in quanto non è possibile eseguire l'Autorun per configurare i browser presenti sul computer. Per effettuare una configurazione corretta è necessario scaricare dal sito del vendor, qualora lo avesse previsto, la necessaria configurazione.

Ad esempio per InfoCert collegandosi al sito <http://www.businesskey.it/bkpermac.htm> e seguire i passi suggeriti.

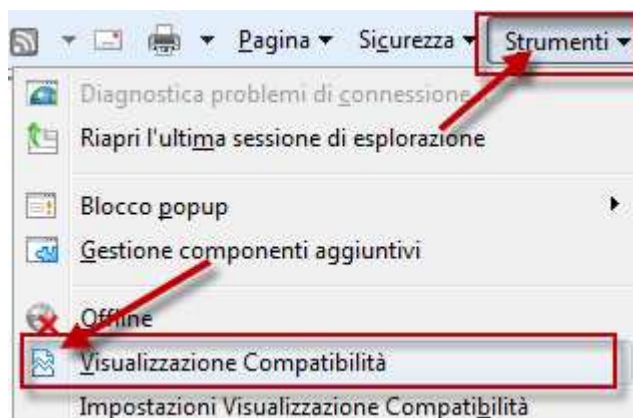
I risultati delle prove effettuate non sono confortanti: è possibile accedere al sistema e navigare le pagine, mentre si sono riscontrate grosse difficoltà nell'apertura della modulistica. Pertanto l'utilizzo di questo sistema operativo è al momento sconsigliato.

Il browser Explorer nelle versioni 8 e 9 deve essere configurato in modo che sia attiva la visualizzazione di compatibilità per i siti web specifici. L'attivazione si ottiene facendo clic sul pulsante "Visualizzazione compatibilità" situato sul lato destro della barra degli indirizzi accanto al



pulsante "Aggiorna",

oppure dal menu Strumenti selezionare l'opzione "Visualizzazione compatibilità".



Inoltre nella sezione Impostazioni Visualizzazione Compatibilità inserire fra i siti compatibili www.piemonte.it.

Effettuate queste impostazioni procedere all'aggiornamento della pagina premendo il tasto F5.

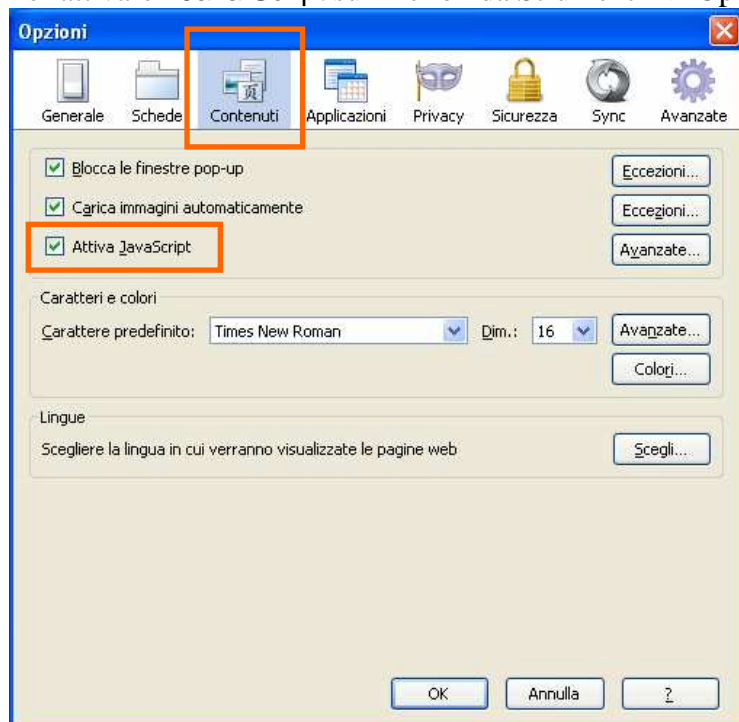
Trovate ulteriori dettagli al seguente link <http://support.microsoft.com/kb/956197/it>

Si suggerisce l'utilizzo del tasto **F5** qualora il browser e/o l'Adobe Reader risultino bloccati.

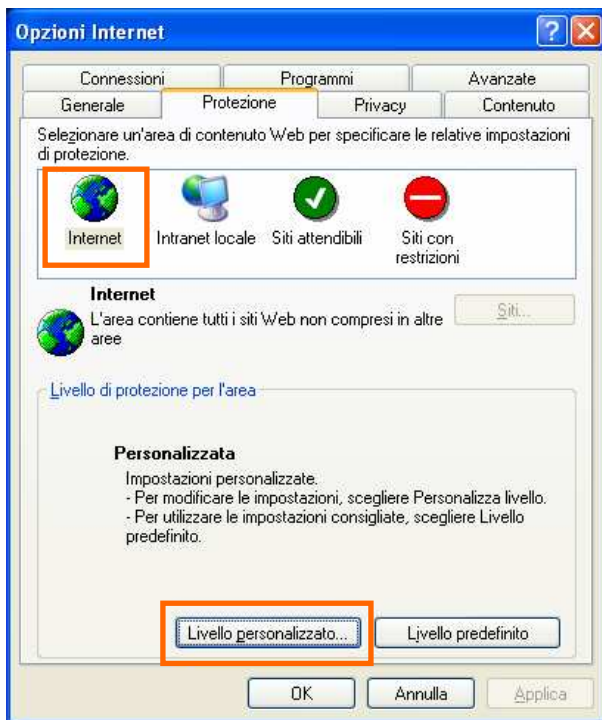
L'utilizzo di **monitor da 19"** o superiori possono provocare difficoltà di visualizzazione delle funzionalità del browser se utilizzati a pieno schermo (ad esempio sulla componente cartografica); pertanto si consiglia di ridurre la finestra di visualizzazione.

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

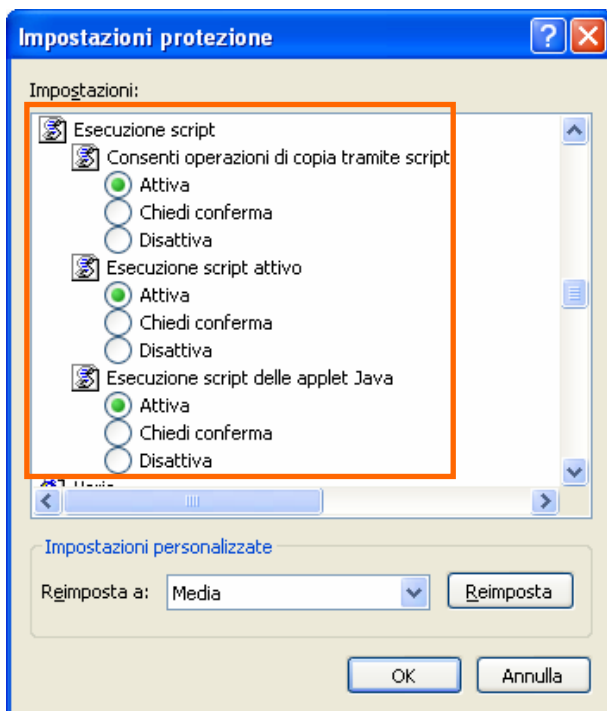
Per attivare i Java Script su FireFox da Strumenti => Opzioni => Contenuti



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

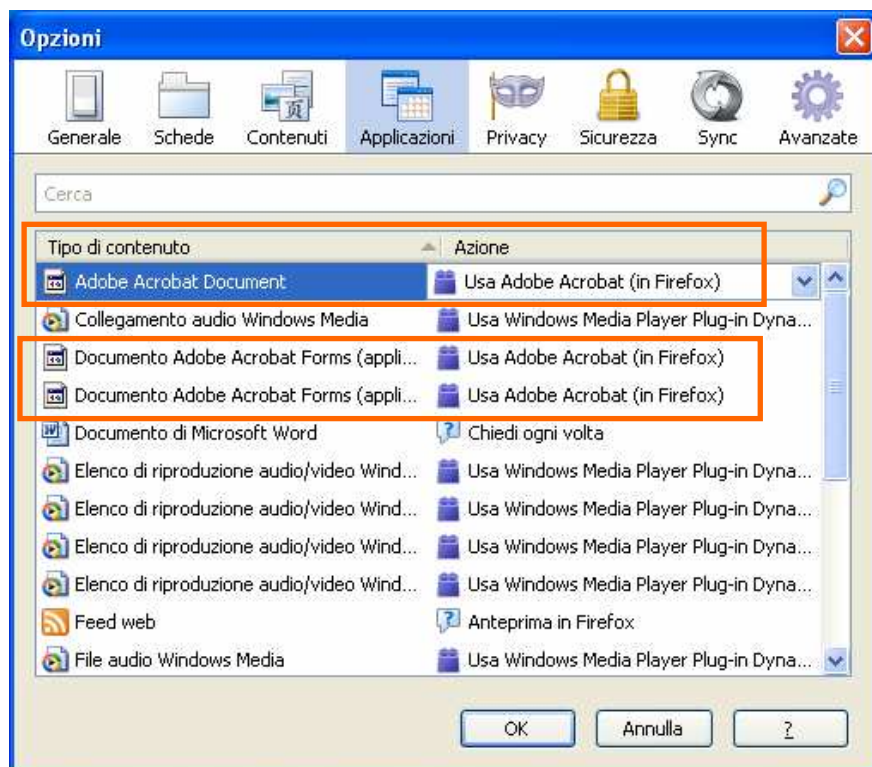


Nella finestra delle Impostazioni di protezione, circa a metà dell'elenco, attivare tutte le esecuzioni script proposte.



Quindi confermare e chiudere con Ok tutte le finestre aperte.

Nel caso si utilizzasse Mozilla Firefox verificare da Strumenti => Opzioni => Applicazioni che per ogni tipo di documento Adobe Acrobat l'azione sia sempre "Usa Adobe Acrobat (in Firefox)".



2.3 Adobe Reader

Il sistema MUDE necessita che sia presente sulla postazione di lavoro il software Adobe Reader (nella versione 9 o successiva), al fine di consentire la compilazione dei modelli MUDE e apporre la firma digitale on line.

NB: la presenza contestuale di AdobePRO e AdobeReader9 sulla stessa postazione può causare conflitti all'atto della firma dei modelli. Nel caso si suggerisce di eseguire AdobeReader9 e dal menu Modifica => Preferenze scegliere fra le Categorie quella Generali e indicare quale programma predefinito l'AdobeReader9.

2.3.1 Modulo aggiuntivo per Adobe Reader

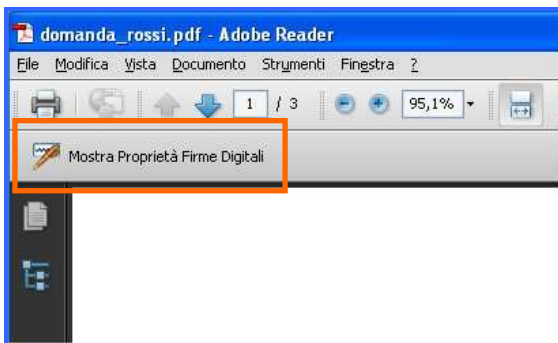
IMPORTANTE: E' richiesta l'installazione dell'add-on per la firma digitale. Questo modulo permette di verificare se la firma digitale apposta ai documenti è quella riconosciuta legalmente.

Compatibile con Adobe Acrobat e Adobe Reader versioni 9 e 10 è uno strumento aggiuntivo, gratuito per Adobe Acrobat e Adobe Reader, offerto da Adobe Systems Italia. Semplifica la messa a punto delle funzioni di firma digitale e rende più immediate le operazioni di verifica, nel rispetto dei requisiti della normativa vigente in Italia e nell'Unione Europea. Installa l'Elenco Pubblico dei Certificatori Accreditati a DigitPA e permette di mantenerlo aggiornato nel tempo.

L'add-on è scaricabile al seguente indirizzo: <http://www.adobe.com/it/security/software/form.html>

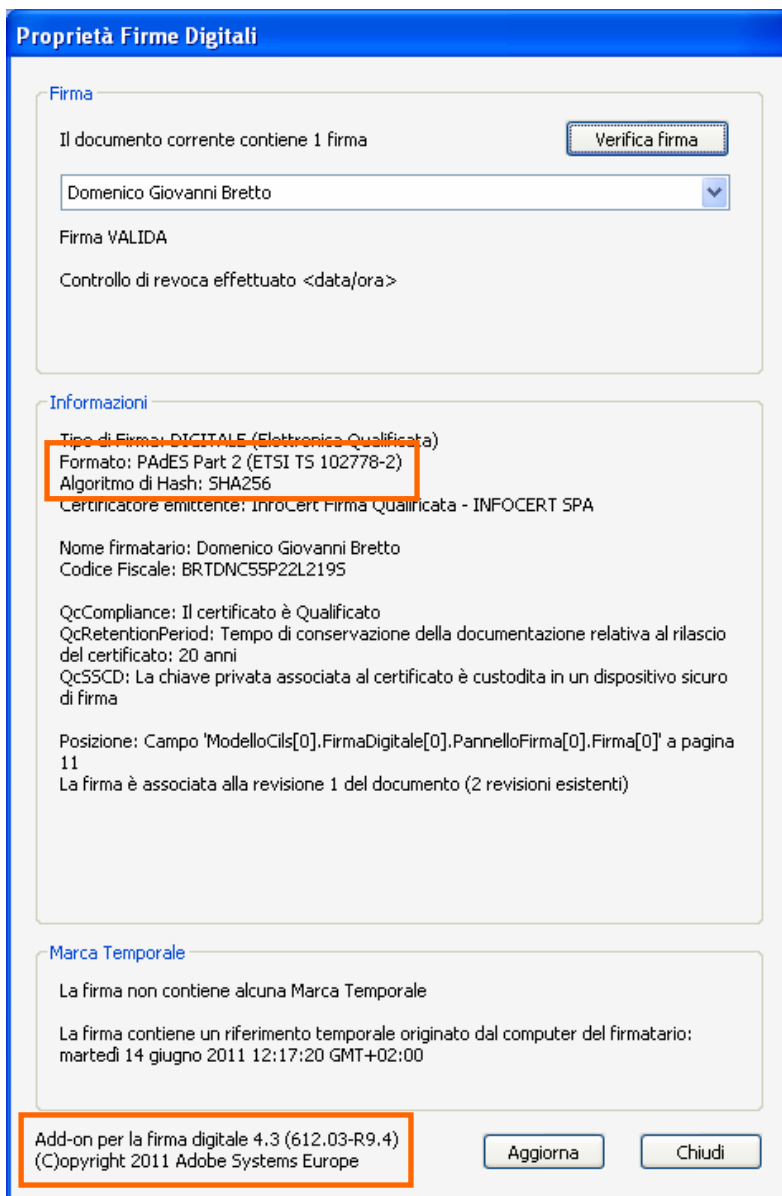
Il download è gratuito previa una semplice registrazione di alcuni dati anagrafici.

Dopo l'apposizione della firma digitale al modello MUDE in PDF, verificare le caratteristiche della firma prodotta selezionando il tab "Mostra proprietà firme digitali" (funzionalità offerta dall'add-on) dello strumento Adobe Reader.



Viene quindi presentata la proprietà di firma che deve avere quale formato il **PADES part 2 (ETSI TS 102778)** e come algoritmo di hash lo **SHA256**.

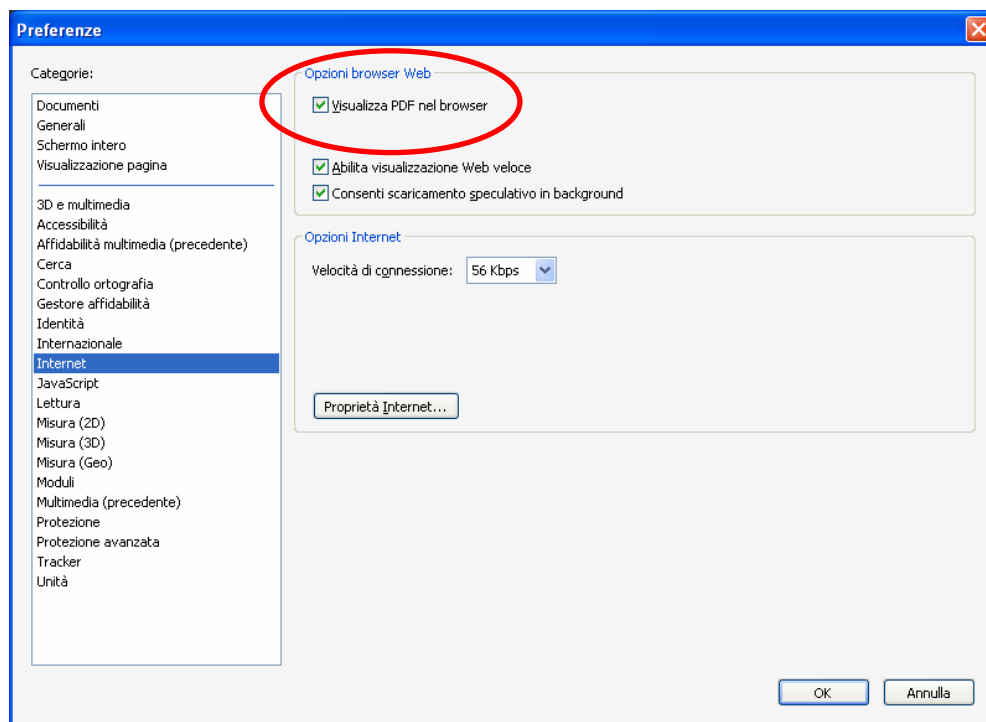
Da notare in calce viene riportata la presenza dell'add-on.



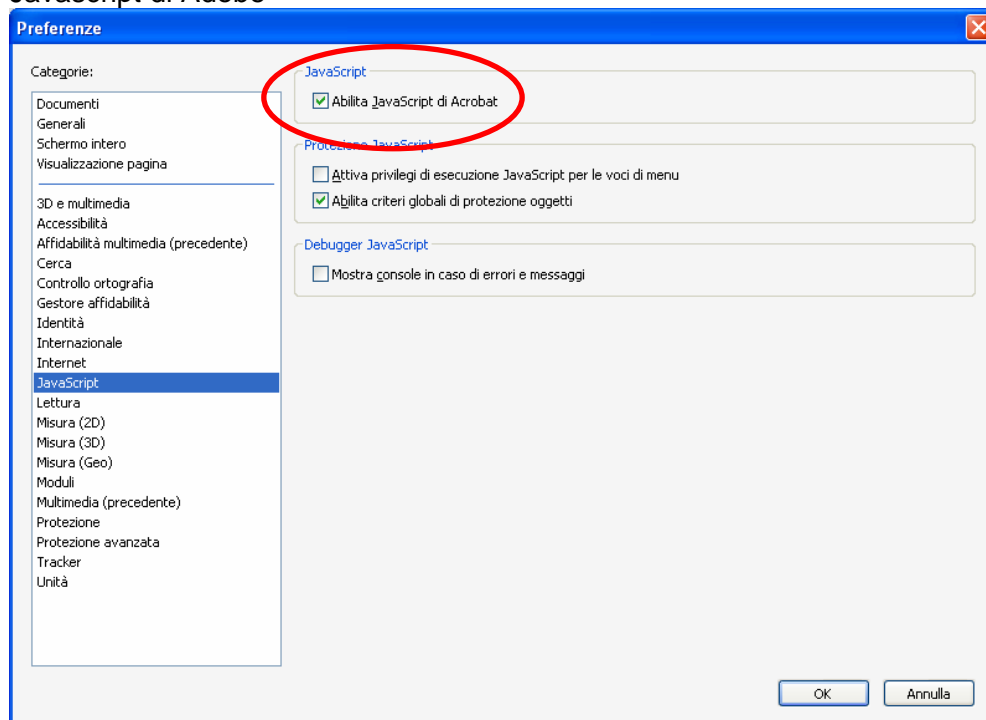
2.3.2 Configurazione Reader versione 9

Impostare l'opzione sul Reader che abilita la visualizzazione del modulo PDF all'interno del Browser; per l'impostazione dell'opzione seguire il percorso Modifica > Preferenze > Internet, selezionare l'opzione "visualizza PDF nel Browser".

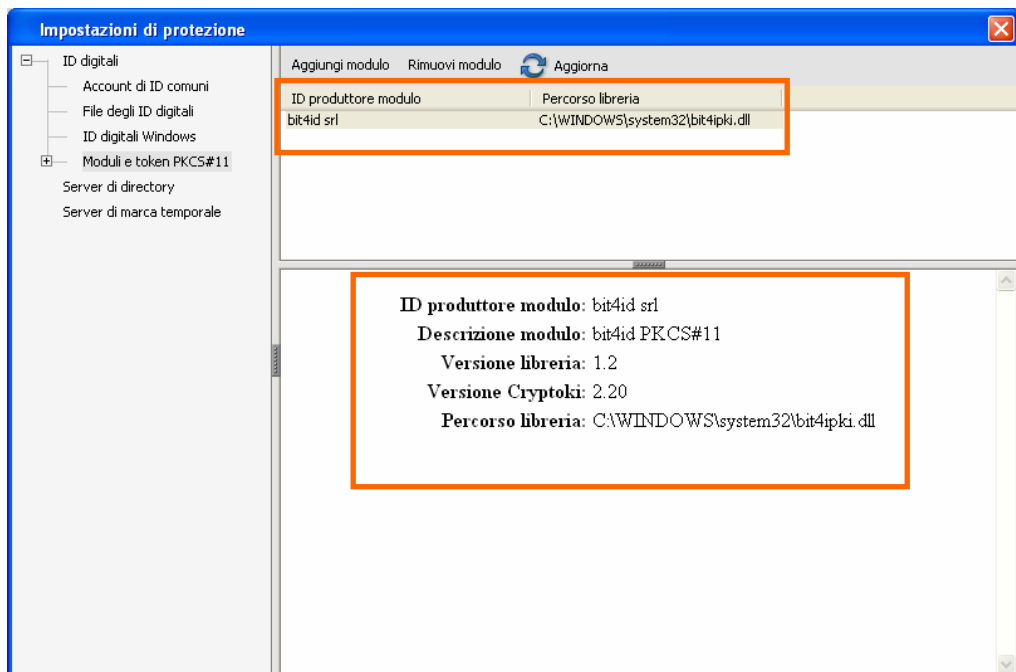
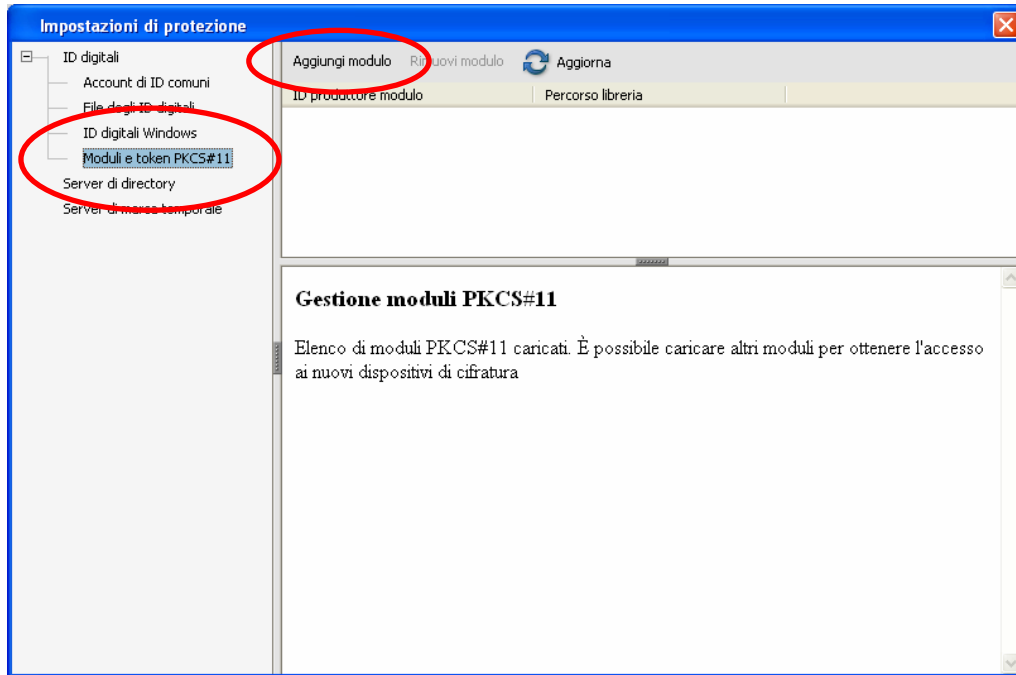
La compilazione in locale del modello non permette di inoltrare le istanze.



Impostare l'opzione sul Reader che abilita il JavaScript del modulo PDF ; per l'impostazione dell'opzione seguire il percorso Modifica > Preferenze > Javascript, selezionare l'opzione "abilita Javascript di Adobe"



Per l'apposizione della firma digitale, il Reader deve agganciare la Business Key al fine di poter usare il certificato di firma ivi residente; per l'impostazione occorre seguire il percorso Documento => Impostazioni di protezione, selezionare "moduli e token PKCS#11" ed aggiungere (se mancante), dal menu Aggiungi modulo, il modulo che aggancia il driver di accesso alla Business Key. Questo modulo è il medesimo installato in precedenza: cartella \\windows\system32 e selezionare, secondo i casi, il file "bit4ipki.dll" oppure "bit4opki.dll".

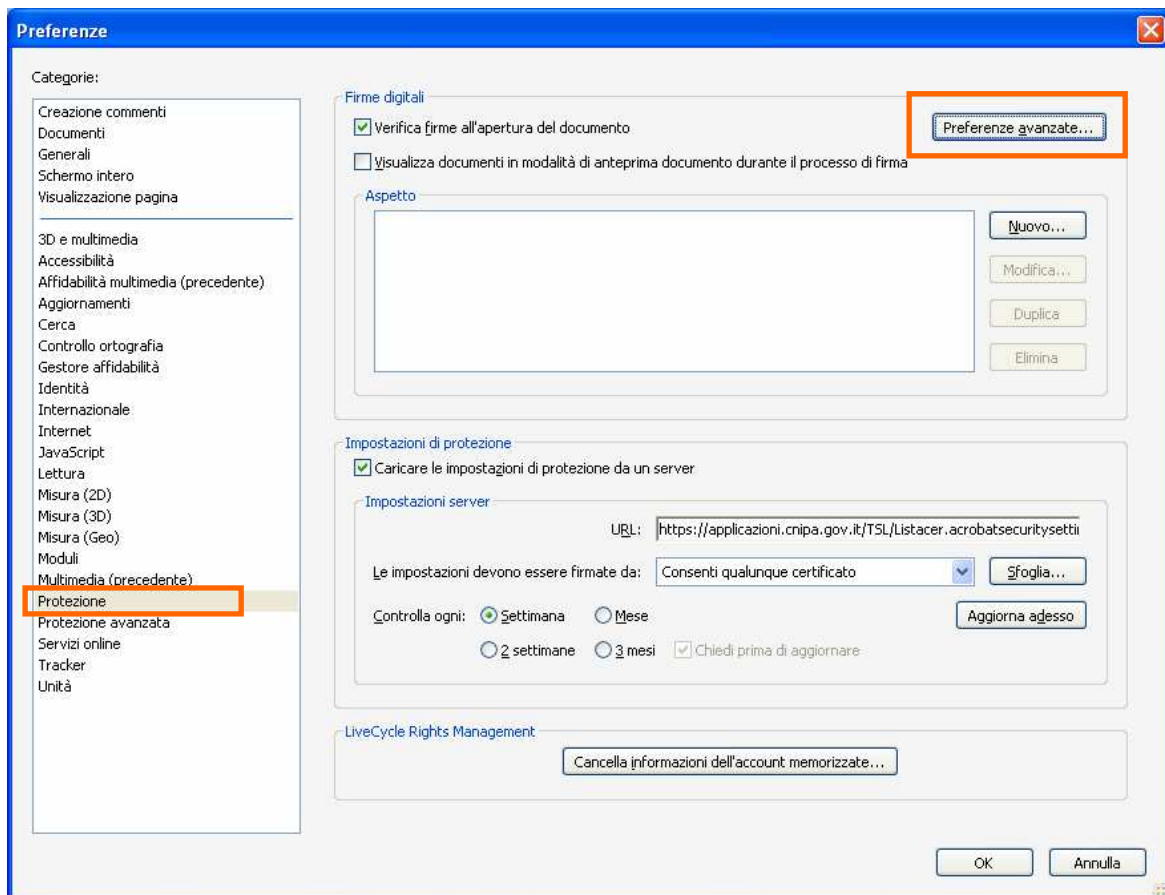


2.3.3 Configurazione Reader versione 10

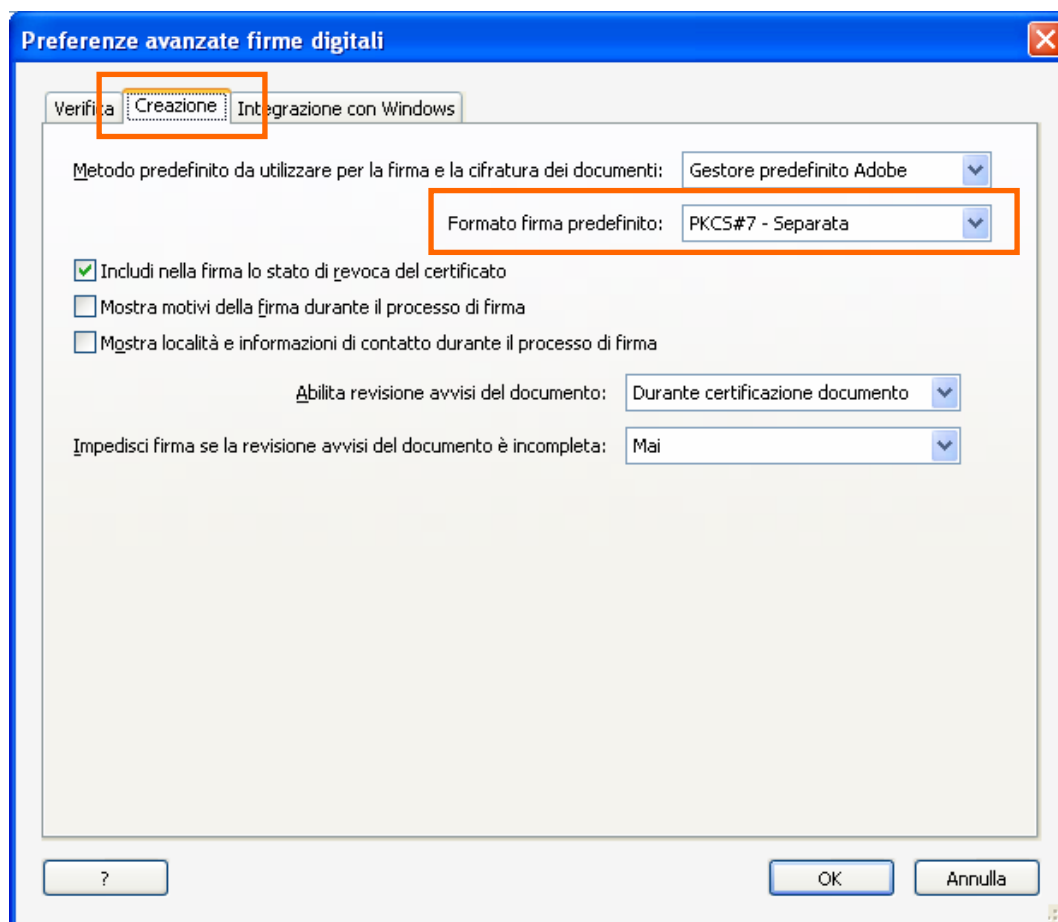
Le impostazioni descritte per la versione 9 sono valide anche per la versione 10.

Il formato di firma applicato di default dalla versione 10 è il PAdES part 3; è pertanto richiesta l'impostazione esplicita del formato di firma **PAdES part 2** che il Reader identifica come **"PKCS#7 separata"**.

Per impostare eseguire il Reader 10 quindi selezionare dal menu Modifica => Preferenze quindi in Protezione selezionare Preferenze avanzate



Quindi nella cartella Creazione selezionare il Formato firma predefinito come PKCS#7-Separata.



2.4 Adobe Flash Player (plugin per browser)

Il plugin è necessario per eseguire l'upload dei documenti elettronici allegati alle istanze MUDE.

La distribuzione e l'utilizzo di Adobe Flash Player non sono vincolati all'installazione di licenze.

Si raccomanda l'installazione della versione più recente; la versione minimale supportata è la 9.

Qualora il player non fosse installato localmente, la pagina web del front office che utilizza la componente Flash rimanda ad una pagina di download del player sul sito web della Adobe. La sua distribuzione è in funzione del sistema operativo presente sulla postazione e del browser usato.

N.B.: qualora sulla postazione sia presente una versione anteriore alla 9, la funzionalità di upload non viene caricata nella pagina (l'area di upload presenta una regione bianca). In questo caso procedere con l'installazione del plugin.

3. Accesso applicativo MUDE

Avviate il browser presente sul vostro PC e inserite l'indirizzo www.mude.piemonte.it

Sul sito, nella sezione "Per i professionisti", è presente il link "Accedi al servizio MUDE".

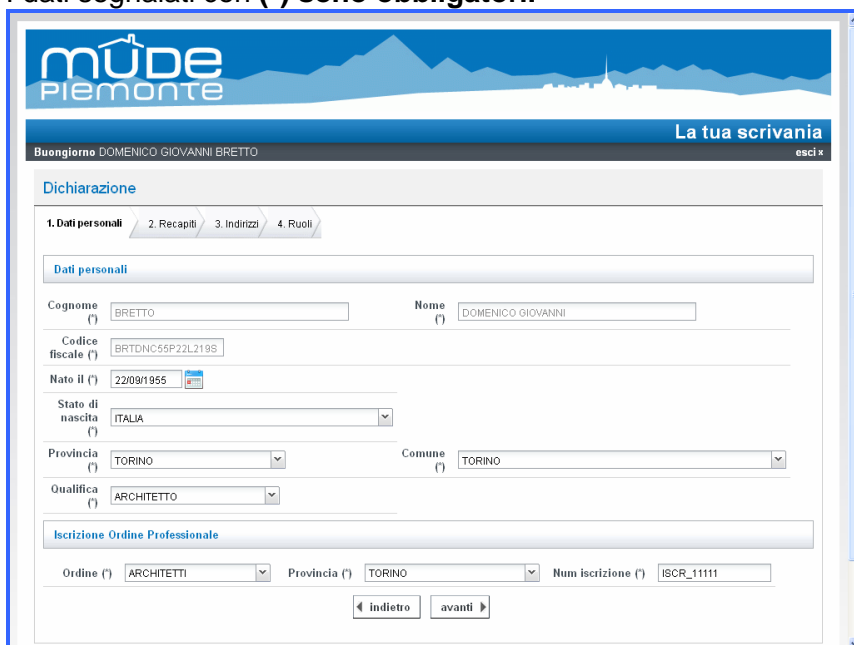
IMPORTANTE: prima di attivare il link inserire il kit di firma digitale

3.1 Accredittamento

Al primo accesso il sistema vi chiede di accreditarvi.

L'accREDITamento consiste nel compilare una serie di cartelle con i vostri dati personali.

I dati segnalati con (*) sono obbligatori.



The screenshot shows the 'Dati personali' section of the 'Dichiarazione' form. It includes fields for:

- Cognome (*): BRETTA
- Nome (*): DOMENICO GIOVANNI
- Codice fiscale (*): BRTDNC55P22L219S
- Nato il (*): 22/09/1955
- Stato di nascita (*): ITALIA
- Provincia (*): TORINO
- Comune (*): TORINO
- Qualifica (*): ARCHITETTO
- Iscrizione Ordine Professionale: Ordine (*): ARCHITETTI, Provincia (*): TORINO, Num iscrizione (*): ISCR_11111

 Navigation buttons 'indietro' and 'avanti' are at the bottom.

La cartella Ruoli contiene anche l'informativa per il consenso al trattamento dei dati personali.



The screenshot shows the 'Ruoli' section of the 'Dichiarazione' form. It contains a table of roles with checkboxes:

Ruolo	Selezionato
Collaudatore	<input checked="" type="checkbox"/>
Direttore Lavori	<input checked="" type="checkbox"/>
Direttore lavori CA	<input checked="" type="checkbox"/>
Progettista	<input checked="" type="checkbox"/>
Progettista strutture	<input checked="" type="checkbox"/>

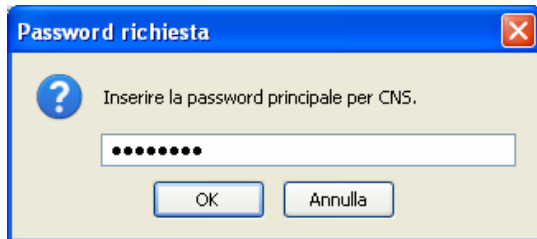
 Below the table are links for 'scarica in Excel' and 'scarica in PDF'. A red box highlights a privacy notice:

INFORMATIVA AI SENSI DELL'ART.13 D. LGS. 196/2003(Codice in materia di protezione dei dati personali)Ai sensi e per gli effetti di cui all'art.13 del D.Lgs.196/2003 ("Codice in materia di protezione dei dati personali"), La informiamo che la Regione Piemonte procede al trattamento dei dati personali da Lei forniti (di seguito Dati) nel rispetto della normativa vigente e secondo quanto di seguito riportato: - La Regione Piemonte può utilizzare i dati forniti in occasione della registrazione nel rispetto dei diritti e delle libertà fondamentali ed esclusivamente al fine di abilitarla all'utilizzo del servizio MUDE. Il conferimento dei suoi dati ha natura facoltativa ma il mancato o incompleto conferimento non Le consentirà di fruire del servizio in oggetto. - Responsabili del trattamento sono: il Responsabile della Direzione LIVIO DEZZANI domiciliato presso il recapito del Titolare del trattamento sotto indicato ed il CSI Piemonte, quale Responsabile esterno del trattamento, domiciliato in Torino, corso Unione Sovietica 216. - Titolare del trattamento è la Regione Piemonte in qualità di Ente erogatore del Servizio. Per qualsiasi comunicazione inerente il trattamento dei Suoi Dati (incluso l'esercizio dei diritti previsti dall'art. 7 del Codice Privacy) potrà rivolgersi a Direzione Programmazione strategica politiche territoriali ed edilizia C.so Bolzano, 44 - 10121 tel. 011.4321428

 Below the notice is a checkbox: 'Dichiaro di aver preso visione dell'informativa sul trattamento dei dati personali dichiarati.' with a checked box.

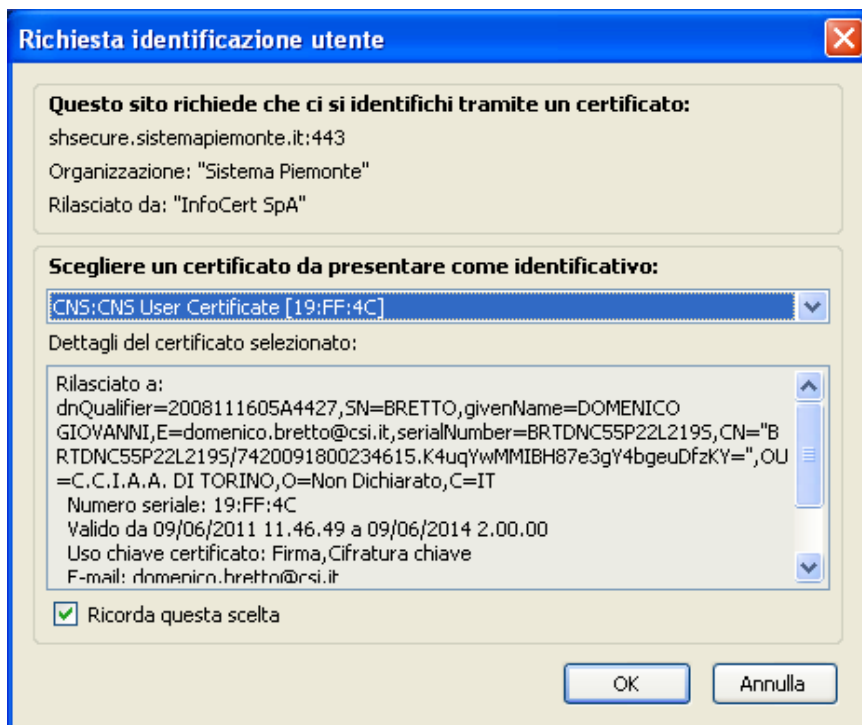
3.2 Autenticazione

Ad ogni accesso al sistema successivo all'accreditamento, il sistema identifica la presenza del certificato e chiede l'inserimento del codice segreto (PIN).

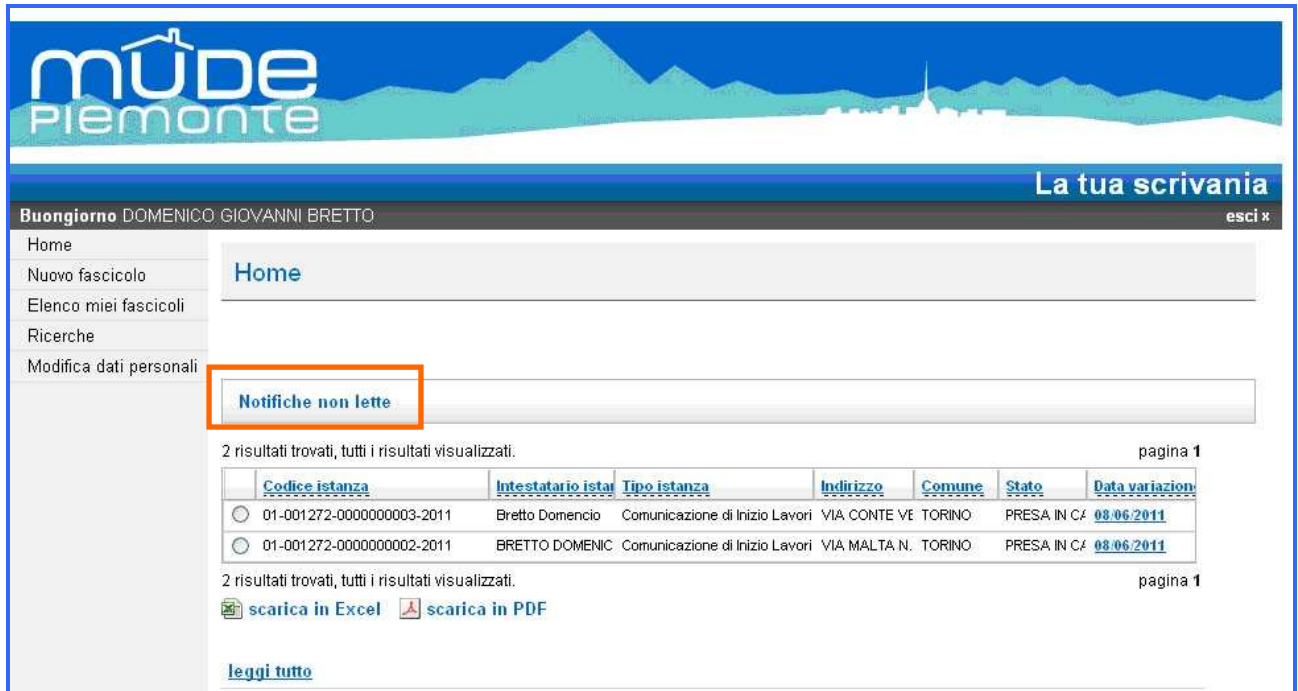


Nel caso in cui il sistema rilevasse la presenza di più di un certificato vi propone di scegliere quello da utilizzare per l'accesso al sistema. Scegliete il certificato e proseguite.

Utilizzate sempre il certificato CNS rilasciato dal vostro certificatore.



Una volta confermato il certificato si accede alla Home della vostra scrivania MUDE.
 Se a sistema sono presenti delle Notifiche da parte della PA non ancora lette, queste vengono sottoposte alla vostra attenzione ogni volta che accedete alla Home. Quelle già lette sono sempre raggiungibili consultando le istanze alle quali fanno riferimento.



La tua scrivania

Buongiorno DOMENICO GIOVANNI BRETTO esci x


- Home
- Nuovo fascicolo
- Elenco miei fascicoli
- Ricerche
- Modifica dati personali

Notifiche non lette

2 risultati trovati, tutti i risultati visualizzati. pagina 1

	<u>Codice istanza</u>	<u>Intestatario ista</u>	<u>Tipo istanza</u>	<u>Indirizzo</u>	<u>Comune</u>	<u>Stato</u>	<u>Data variazion</u>
<input type="radio"/>	01-001272-0000000003-2011	Bretto Domencio	Comunicazione di Inizio Lavori	VIA CONTE VE	TORINO	PRESA IN C/	<u>08.06.2011</u>
<input type="radio"/>	01-001272-0000000002-2011	BRETTO DOMENIC	Comunicazione di Inizio Lavori	VIA MALTA N.	TORINO	PRESA IN C/	<u>08.06.2011</u>

2 risultati trovati, tutti i risultati visualizzati. pagina 1

 [scarica in Excel](#)  [scarica in PDF](#)

[leggi tutto](#)

4. Allegato: elenco enti certificatori

Certification Authority
<i>Actalis CA per Autenticazione CNS</i>
<i>Actalis CA per certificati CNS 2</i>
<i>Actalis Class A Secure Client CA</i>
<i>Actalis Class A Secure Client CA</i>
<i>Actalis Client Authentication CA</i>
<i>Actalis Qualified Certificates CA</i>
<i>Actalis Qualified Certificates CA</i>
<i>Actalis Qualified Certificates CA</i>
<i>Actalis Qualified Certificates CA</i>
<i>Actalis S.p.A. – Autenticazione</i>
<i>ArubaPEC per Arma dei Carabinieri CA 1</i>
<i>ArubaPEC S.p.A. NG CA 1</i>
<i>ArubaPEC S.p.A. NG CA 2</i>
<i>Bancaintesa Production Identrus Certification Authority</i>
<i>bancaroma Production Identrus Certification Authority</i>
<i>bancaroma Production Identrus Certification Authority</i>
<i>Cedacricert</i>
<i>Cedacricert Old</i>
<i>CedacricertCATS</i>
<i>Certicomm CNDCEC</i>
<i>Certificatore Saritel</i>
<i>CIE ROOTCA</i>
<i>CNIPA CA1</i>
<i>Consiglio Nazionale Forense - Autenticazione</i>
<i>CT RUPA CA1</i>
<i>Esercito Italiano</i>
<i>I.T. Telecom Firma Qualificata CA</i>
<i>I.T. Telecom per il Ministero dell'Interno CA</i>
<i>I.T. Telecom per il Ministero dell'Interno CA</i>
<i>Identrus Root Certificate Authority</i>
<i>In.Te.S.A. - Certification Authority</i>
<i>IN.TE.S.A. Certification Authority</i>
<i>InfoCamere Servizi di Certificazione</i>
<i>InfoCamere Servizi di Certificazione 2</i>

<i>InfoCert Servizi di Certificazione</i>
<i>InfoCert Servizi di Certificazione CL</i>
<i>Intesa Sanpaolo Production Identrust Certification Authority</i>
<i>Intesa Sanpaolo S.p.A. - Certification Authority Principale</i>
<i>Ministero della Difesa</i>
<i>MPS Production Identrus Certification Authority</i>
<i>MPS Production Identrus Certification Authority</i>
<i>MPS Root Certification Authority</i>
<i>Namirial CA Autenticazione</i>
<i>Postecert per Regione Emilia-Romagna</i>
<i>Postecom CA1 – New</i>
<i>Postecom CA2</i>
<i>Postecom CS2</i>
<i>Regione Autonoma Friuli Venezia Giulia - CA Cittadini</i>
<i>Regione Lombardia Certification Authority Cittadini</i>
<i>Regione Lombardia Certification Authority Cittadini 2</i>
<i>Regione Lombardia Certification Authority Cittadini 3</i>
<i>Regione Lombardia Certification Authority Cittadini 4</i>
<i>Regione Siciliana Certification Authority Cittadini</i>
<i>Root CA CIE 2</i>
<i>ROOT CA SICUREZZA CNSD</i>
<i>sanpaoloimi Production Identrus Certification Authority</i>
<i>sanpaoloimi Production Identrus Certification Authority</i>
<i>SIA Secure Server CA</i>
<i>Sistema Piemonte CA</i>
<i>SubCA-01 CIE</i>
<i>SubCA-02 CIE</i>
<i>SubCA-03 CIE</i>
<i>SUBCA-EMISSIONE1-MI</i>
<i>SUBCA-EMISSIONE2-MI</i>
<i>SUBCA-EMISSIONE4-MI</i>
<i>SUBCA-EMISSIONE5-MI</i>
<i>SUBCA-EMISSIONE6-MI</i>