

MUDE Piemonte

Configurazione di Adobe Reader per l'apposizione di firma digitale con algoritmo SHA-256

STATO DELLE VARIAZIONI

Versione	Paragrafo o Pagina	Descrizione della variazione
V01	Tutto il documento	Versione iniziale del documento
V02	Paragrafo 2	Aggiornamento della descrizione della configurazione
V03	Aggiornamento documento	Aggiunti dettagli e chiarimenti specifici
V04	Aggiornamento documento	Aggiunto riferimento a Adobe DC e dettagli su configurazione firma

Sommario

1. INTRODUZIONE.....	2
2. PASSO 1 : CONFIGURARE IL CORRETTO MODULO CSP	2
2.1 Adobe Reader versione XI e Adobe DC.....	2
2.2 Altre versioni di Reader e Acrobat.....	8
3. PASSO 2: CONFIGURAZIONE DEL FORMATO DI FIRMA	8
3.1 Adobe Reader versione XI e Adobe DC.....	8
3.2 Altre versioni di Reader e Acrobat.....	9
4. ULTERIORI VERIFICHE	10

1. Introduzione

Per poter utilizzare i software di Adobe, Acrobat e Reader, per apporre una firma digitale a norma, è necessario effettuare alcune operazioni preliminari.

Ricordiamo che le firme valide devono essere realizzate con il calcolo dell'impronta realizzato con l'algoritmo di hash SHA-256.

Se non si configurano gli strumenti Adobe con il corretto modulo CSP (Crypto Service Provider), ossia con lo stesso CSP utilizzato dalla business key, nel momento in cui viene applicata una firma digitale attraverso le funzionalità offerte da Adobe, si otterrà una firma non valida in quanto conterrà un'impronta eseguita con l'algoritmo SHA-1, ormai obsoleto.

Prima di iniziare, se non è già stato fatto, eseguire la configurazione della propria Business Key seguendo le istruzioni riportate nel documento [Modalità di attivazione e configurazione](#).

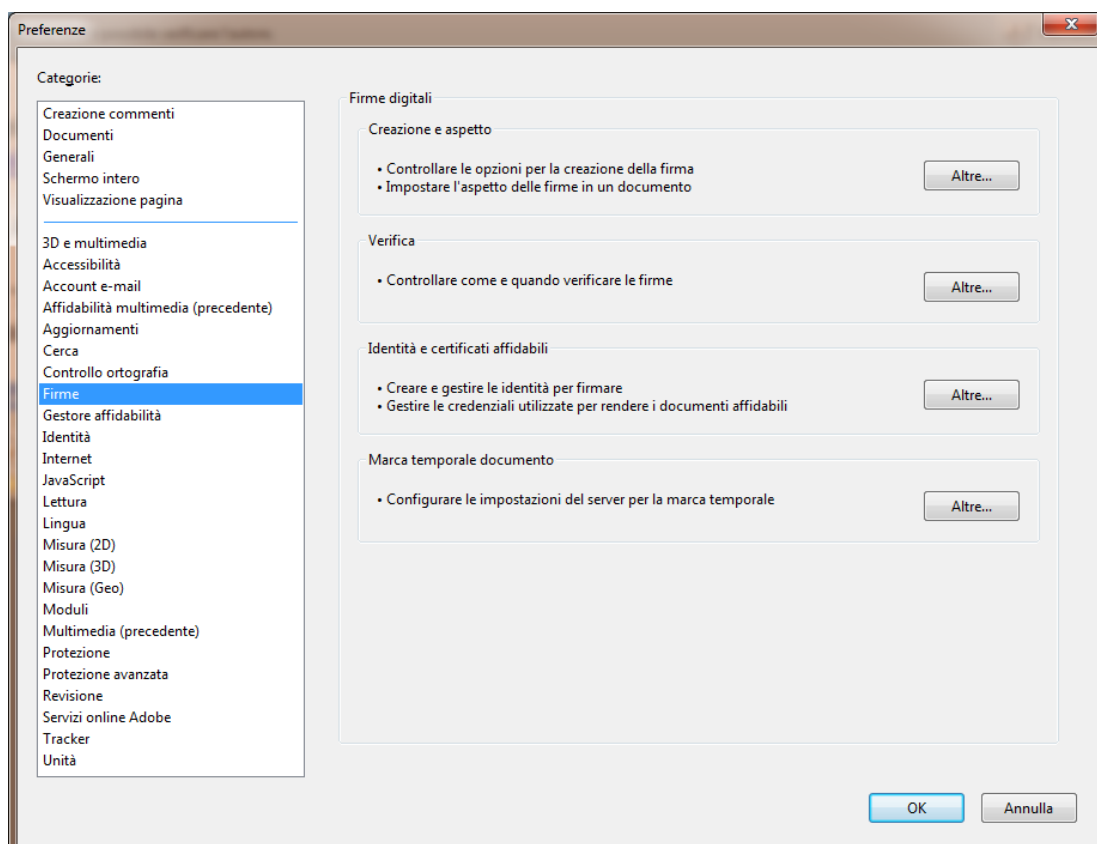
2. PASSO 1 : Configurare il corretto modulo CSP

Prima di iniziare la procedura di configurazione inserire il dispositivo di firma nel proprio pc.

2.1 Adobe Reader versione XI e Adobe DC

Apertura del pannello di configurazione

Aprire Reader, selezionare dalla Barra Menù (F9) la voce “Modifica” → “Preferenze”, quindi all'interno dell'elenco delle categorie indicate, selezionare la voce “Firme”



Nella finestra cliccare il pulsante “Altre” del riquadro “Identità e certificati affidabili”

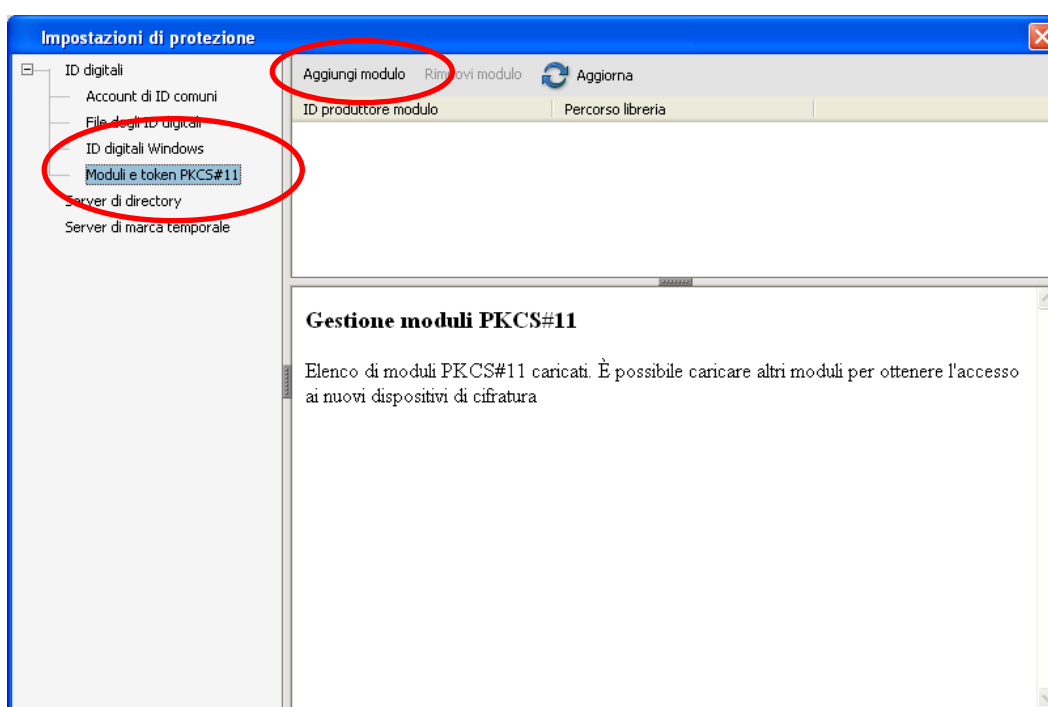
Configurazione del modulo CSP

A questo punto occorre aprire la sezione “Moduli e token PKCS#11”, espandendo la sezione “ID digitali”, e cliccare sulla voce menù “Aggiungi modulo”.

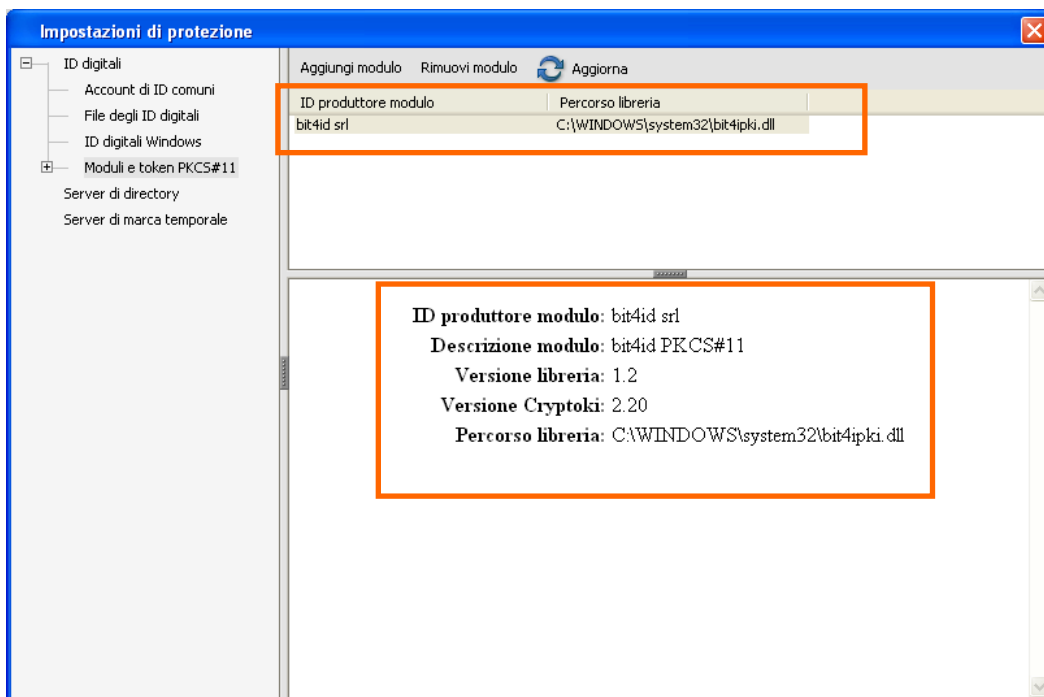
N.B. Se il pulsante “Aggiungi Modulo” non è attivo effettuare la seguente operazione:

- cliccare sul menù Modifica di Adobe
- selezionare la voce Preferenze avanzate
- togliere il visto da Abilita la protezione avanzata

Nella finestra che si apre, occorre cercare il driver di accesso alla Business Key, che è il medesimo installato durante la configurazione della Business Key: cartella \\windows\system32 e selezionare, secondo i casi, il file “bit4ipki.dll” oppure “bit4opki.dll”.



La finestra verrà aggiornata, come raffigurato nell’immagine sottostante.



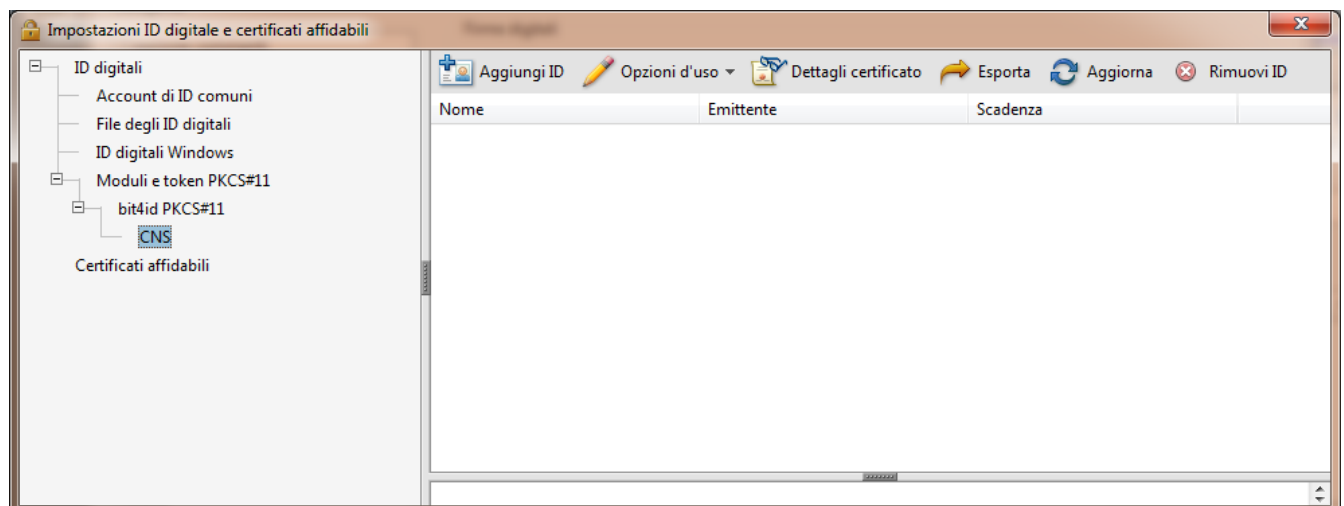
Configurazione del certificato di firma

A questo punto se avevate già inserito il dispositivo di firma procedere con i seguenti passi. Nel caso in cui non abbiate ancora inserito il dispositivo di firma, chiudete la finestra “Impostazioni ID digitale e certificati affidabili”, quindi chiudere la finestra “Preferenze” e chiudere Adobe Reader. Quindi inserite il dispositivo di firma nel pc e ripetete i passi descritti nel paragrafo 2.1 **Apertura del pannello di configurazione.**

Passo 1 di 5

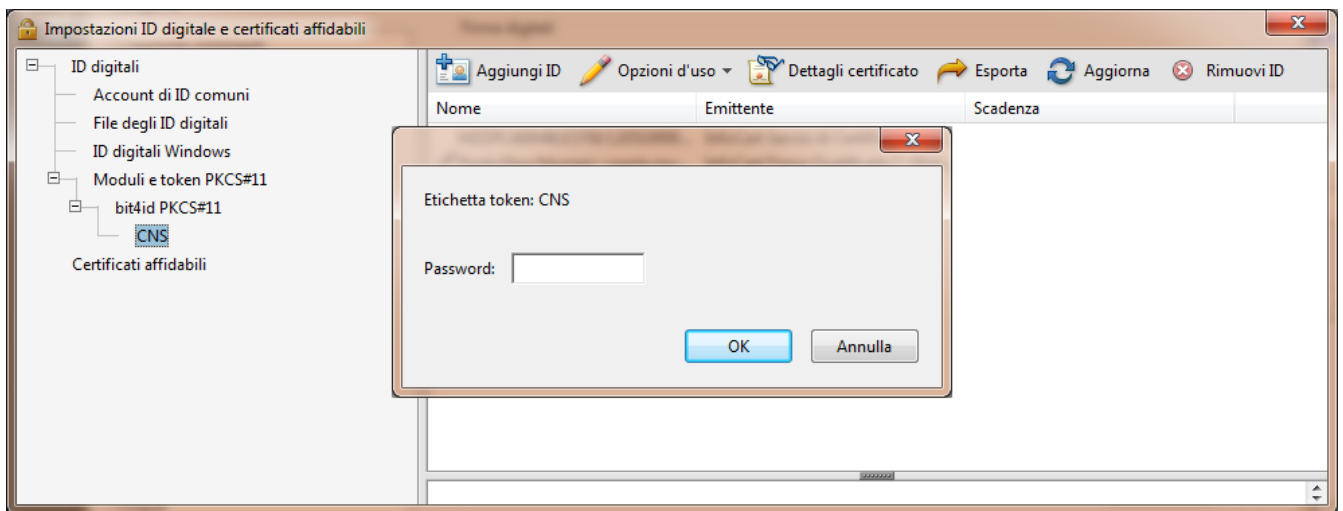
Utilizzando l’elenco delle voci presenti nella parte sinistra della pagina, aprire (cliccando sull’icona raffigurante un +) la voce “Moduli e token PKCS#11” e quindi selezionare la voce CNS.

Nella parte di sinistra devono visualizzarsi alcuni pulsanti specifici per poter leggere i certificati presenti nel dispositivo di firma. Cliccare sul pulsante “Aggiungi ID”



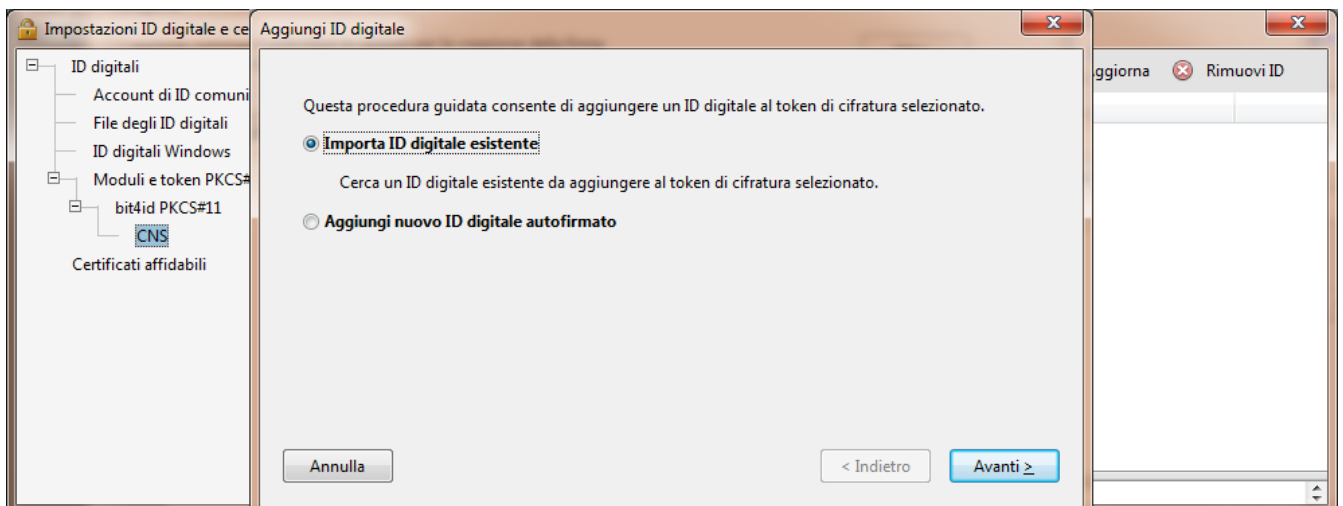
Passo 2 di 5

Inserite il vostro PIN con cui è protetto l'accesso al dispositivo di firma



Passo 3 di 5

Adobe procederà con la lettura dei certificati. Sul nuovo pannello cliccare sul pulsante “Annulla”



Passo 4 di 5

Se compaiono due certificati, selezionare quello che riporta come dettaglio, nella parte sottostante, l'utilizzo come certificato di firma **che dev'essere quello contraddistinto da cognome e nome e non codice fiscale**

Impostazioni ID digitale e certificati affidabili

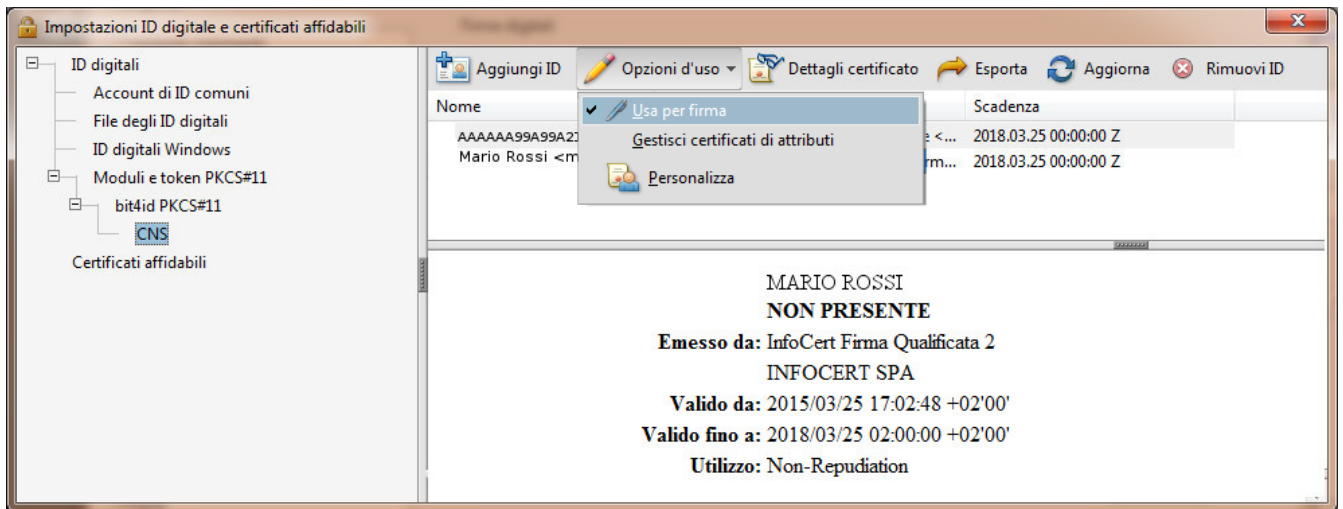
+ Aggiungi ID Opzioni d'uso Dettagli certificato Esporta Aggiorna Rimuovi ID

Nome	Emittente	Scadenza
AAAAAA99A99A219A/120510000...	InfoCert Servizi di Certificazione <...	2018.03.25 00:00:00 Z
Mario Rossi <mario.rossi@	InfoCert Firma Qualificata 2 <firm...	2018.03.25 00:00:00 Z

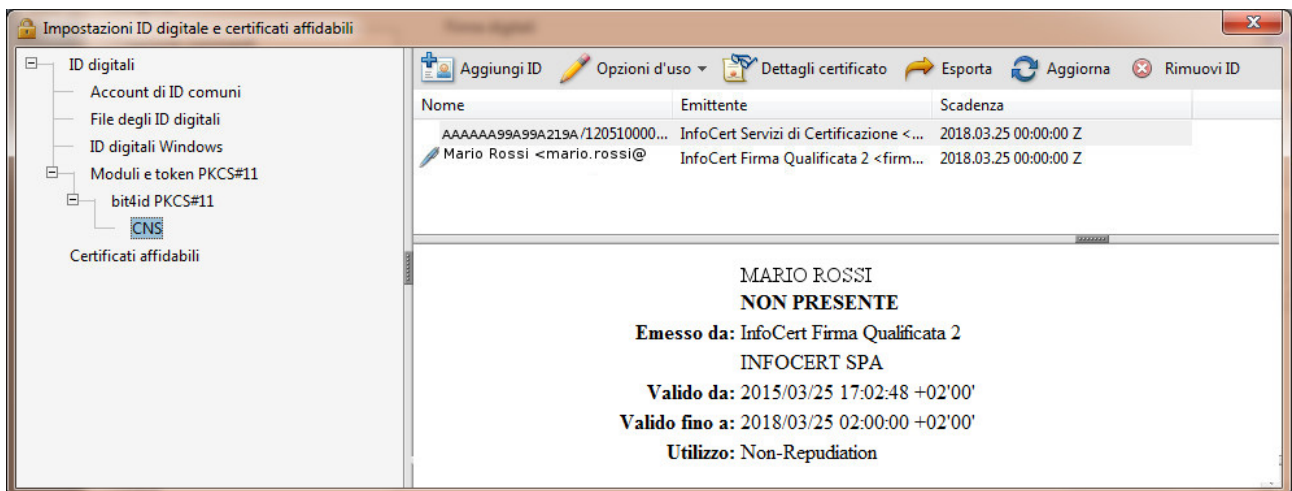
MARIO ROSSI
NON PRESENTE
Emesso da: InfoCert Firma Qualificata 2
 INFOCERT SPA
Valido da: 2015/03/25 17:02:48 +02'00'
Valido fino a: 2018/03/25 02:00:00 +02'00'
Utilizzo: Non-Repudiation

Passo 5 di 5

Una volta selezionato il certificato da utilizzare per la firma, cliccare sul pulsante “Opzioni d’uso” e selezionare la voce “Usa per firma”



Accanto al certificato comparirà l’immagine di una penna stilografica



La procedura di configurazione del certificato è terminata. Chiudere la finestra e confermare col pulsante “OK”, quindi chiudere Adobe Reader.

2.2 Altre versioni di Reader e Acrobat

Altre versioni di Reader e Acrobat potrebbero differenziare dalle indicazioni date in precedenza unicamente per le voci dei menù, necessarie per arrivare alla gestione dei Moduli.

Su Acrobat X, andare su:

Modifica - protezione - Impostazioni di protezione

Su Acrobat Professional, cliccare su

Avanzate → Impostazioni di protezione (Security Settings)

Reader versione IX e X cliccare su

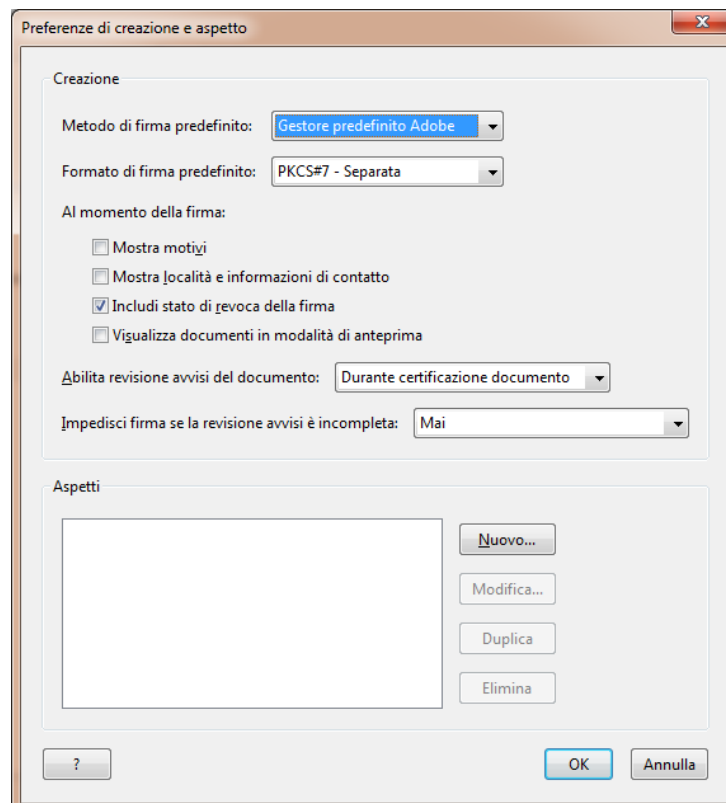
Documento → Impostazioni di protezione (Security Settings)

3. PASSO 2: Configurazione del formato di firma

3.1 Adobe Reader versione XI e Adobe DC

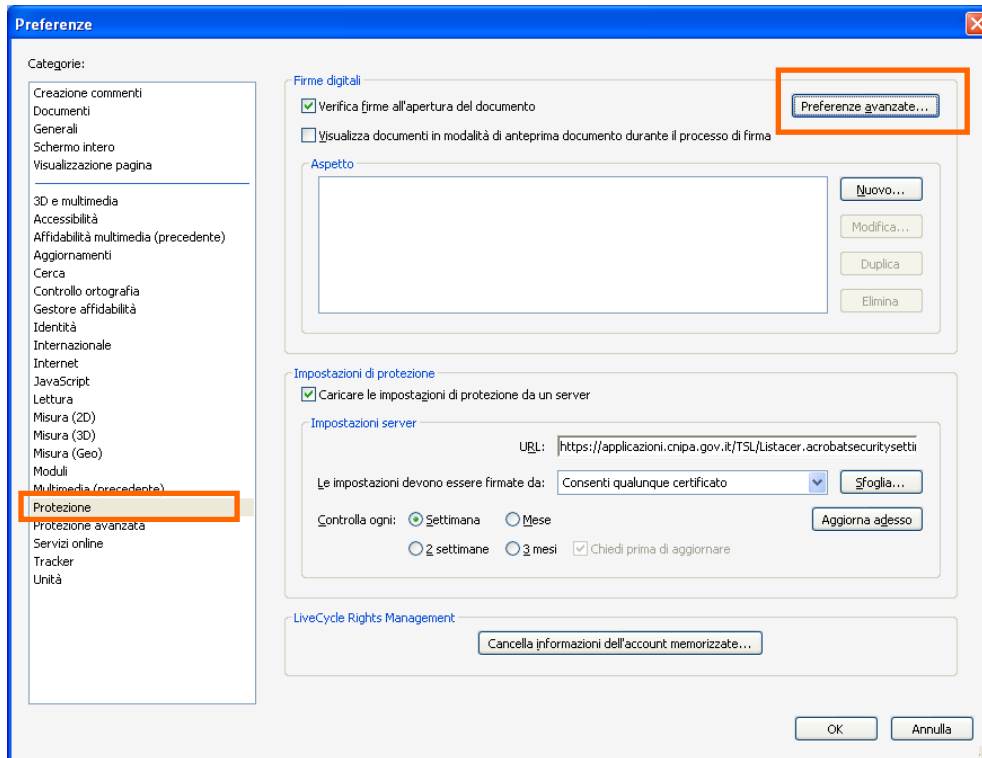
Aprire Reader, selezionare dalla Barra Menù (F9) la voce “*Modifica*” → “*Preferenze*”, quindi all’interno dell’elenco delle categorie indicate, selezionare la voce “*Firme*” e quindi cliccare il pulsante “*Altre*” del riquadro “*Creazione e aspetto*”.

Nella casella denominata “*Formato di firma predefinito*”, selezionare la voce “**PKCS#7 separata**” che identifica il formato di firma **PADES part 2**.

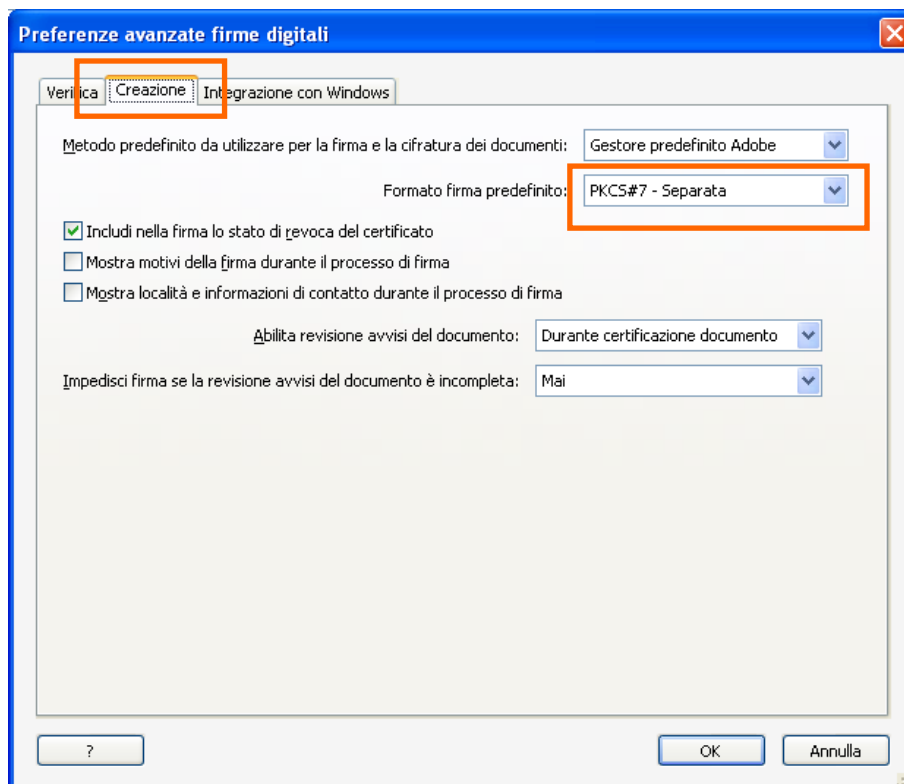


3.2 Altre versioni di Reader e Acrobat

In Reader/Acrobat X e Reader IX selezionare dal menu “Modifica” → “Preferenze” quindi in “Protezione” cliccare sul pulsante “Preferenze avanzate”



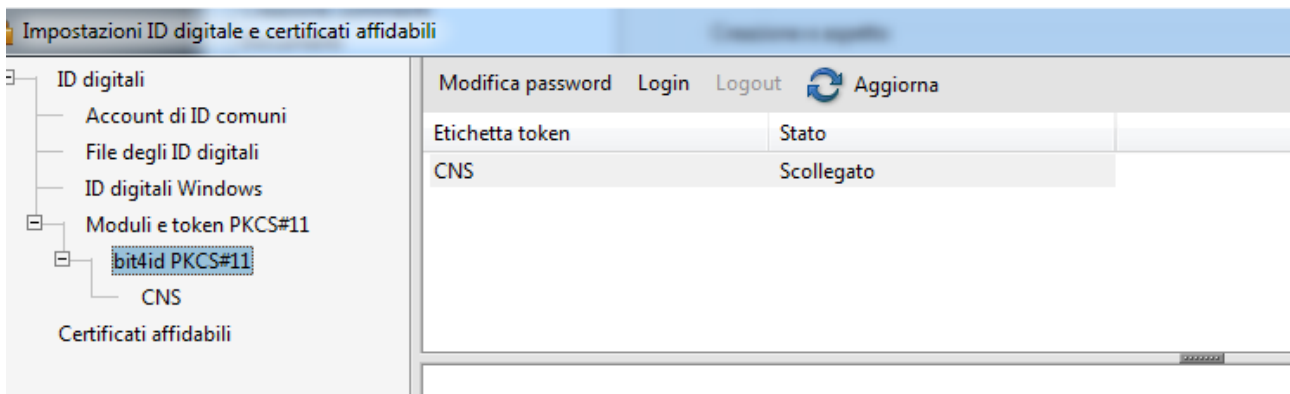
Quindi nella cartella Creazione selezionare il Formato firma predefinito come PKCS#7-Separata.



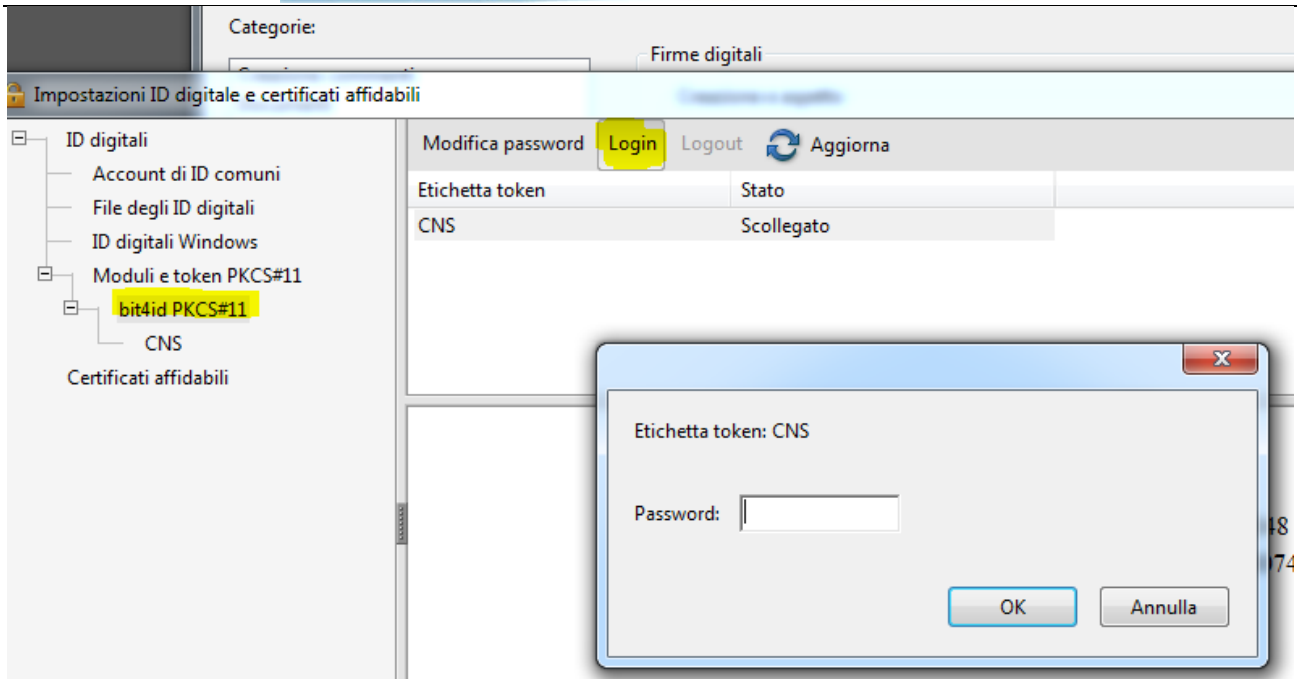
4. ULTERIORI VERIFICHE

Se dopo aver seguito la configurazione descritta precedentemente si dovesse ancora visualizzare il messaggio **“errore, firma non valida”** in fase di firma dell’istanza su Mude, occorre effettuare un’ulteriore verifica.

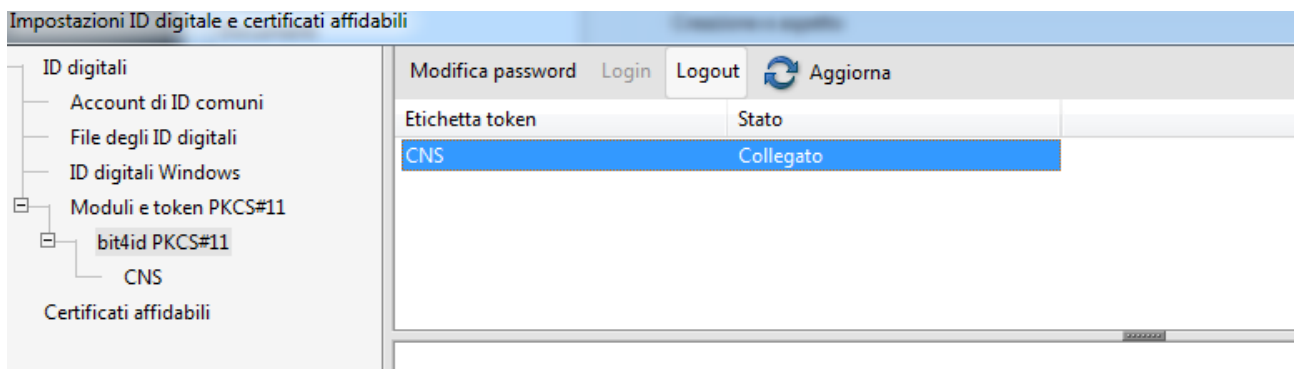
- Aprire Reader, selezionare dalla Barra Menù (F9) la voce “Modifica” / “Preferenze”, quindi all’interno dell’elenco delle categorie indicate, selezionare la voce “Firme”
- Nella finestra cliccare il pulsante “Altre” del riquadro “Identità e certificati affidabili”
- A questo punto occorre aprire la sezione “Moduli e token PKCS#11”, espandendo la sezione “ID digitali” e posizionarsi, come da immagine, sulla dicitura **“bit4id PKCS#11”**



- Se compare sulla parte destra della videata la riga (come descritto nell’immagine sopra) con lo STATO = Scollegato è necessario selezionare il pulsante LOGIN posto in alto



- Nella finestra che compare inserire il proprio PIN della business key e dare OK



- Dopo questa operazione lo STATO sarà COLLEGATO