<u>VERSIONE PER WINDOWS</u>

CONFIGURAZIONE DI ADOBE ACROBAT READER DC

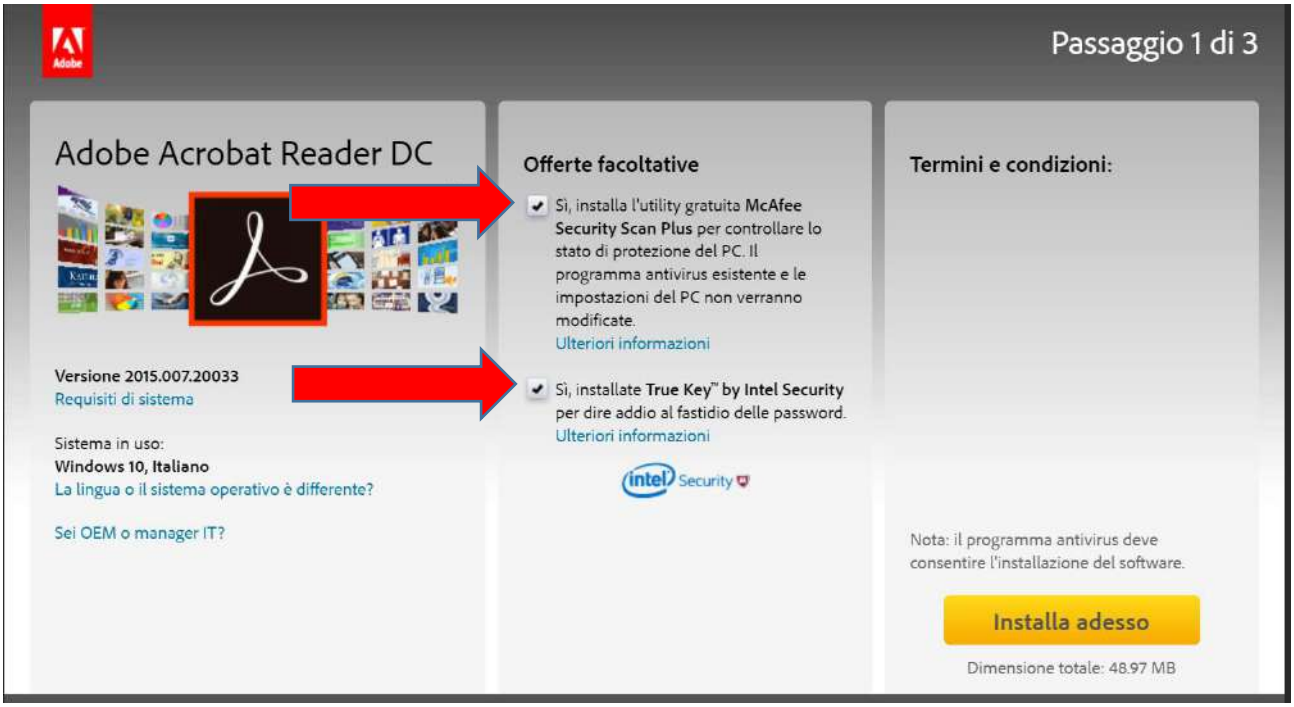
PER L'UTILIZZO CORRETTO NEL PROCESSO AMMINISTRATIVO TELEMATICO

- **Apposizione di firma digitale PAdES BES con algoritmo SHA-256 –**

Versione	Paragrafo o pagina	Descrizione della variazione	Data rilascio
V1	Tutto il documento	Versione iniziale del documento	28/03/2016
V2	Pagina 13	Aggiunta nota	13/04/2016

Introduzione

Per utilizzare i **Moduli** del **Processo Amministrativo Telematico** è necessario disporre del prodotto software **Adobe Acrobat Reader DC**, scaricabile gratuitamente da questo link: https://get.adobe.com/it/reader (si consiglia si togliere il segno di spunta proposto di default nelle **Offerte Facoltative** indicato dalle frecce in figura**)**.



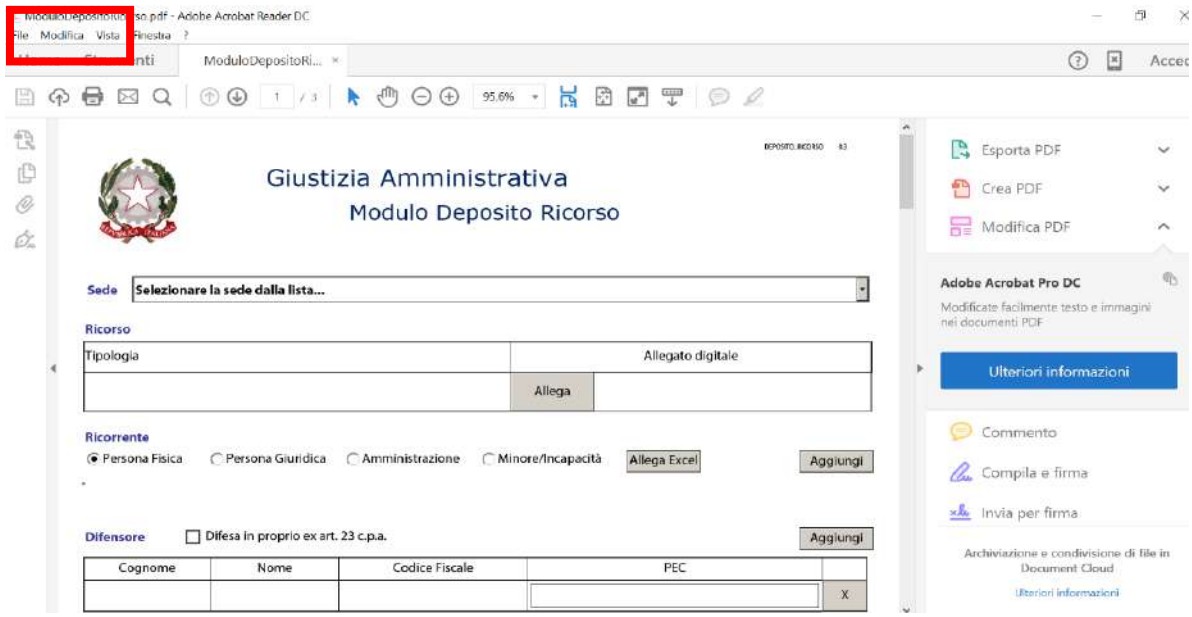
Per poter utilizzare correttamente il software Adobe Acrobat Reader DC nel Processo Amministrativo Telematico è necessario effettuare alcune **operazioni preliminari**.

Le firme valide, infatti, devono essere realizzate utilizzando **l'algoritmo di firma SHA-256** mentre le funzionalità standard di Adobe Acrobat Reader DC realizzano una firma basata sull'algoritmo SHA-1, obsoleto dal 30 giugno 2011.

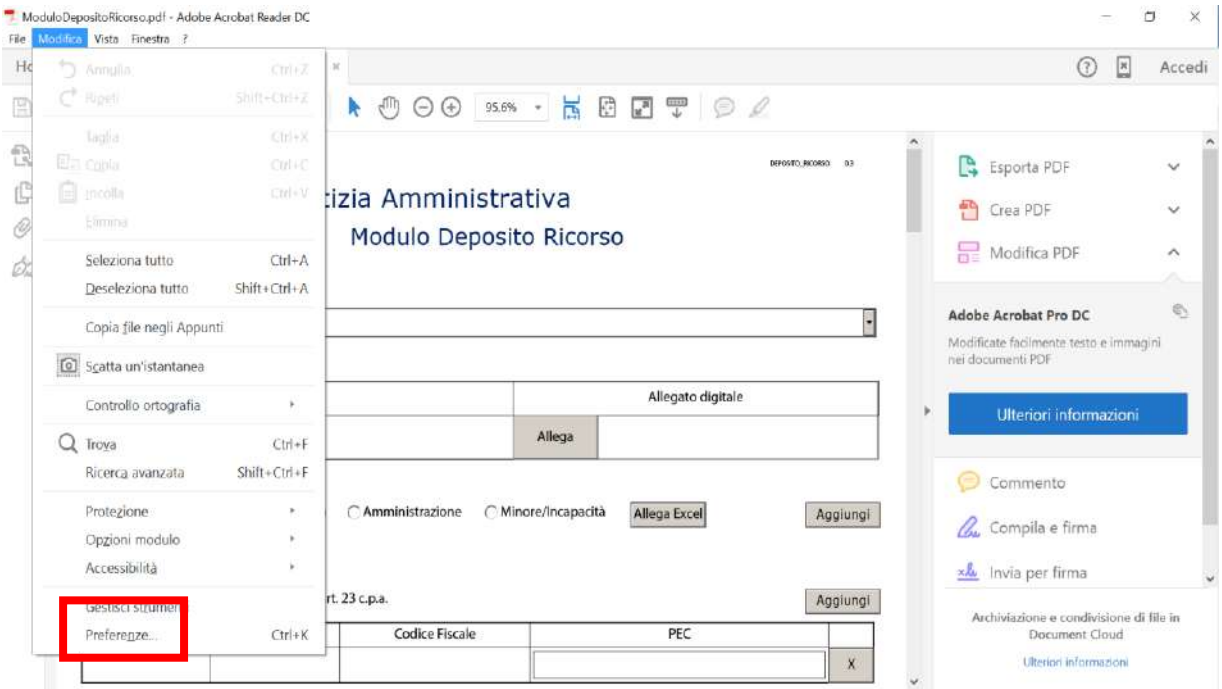
Configurazione del modulo CSP (Crypto Service Provider)

Inserire il proprio dispositivo di firma digitale nel PC, installarlo come da istruzioni (non occorre l'installazione se si è già firmato con quel dispositivo dal PC che si sta utilizzando), aprire Adobe Acrobat Reader DC e procedere come segue:

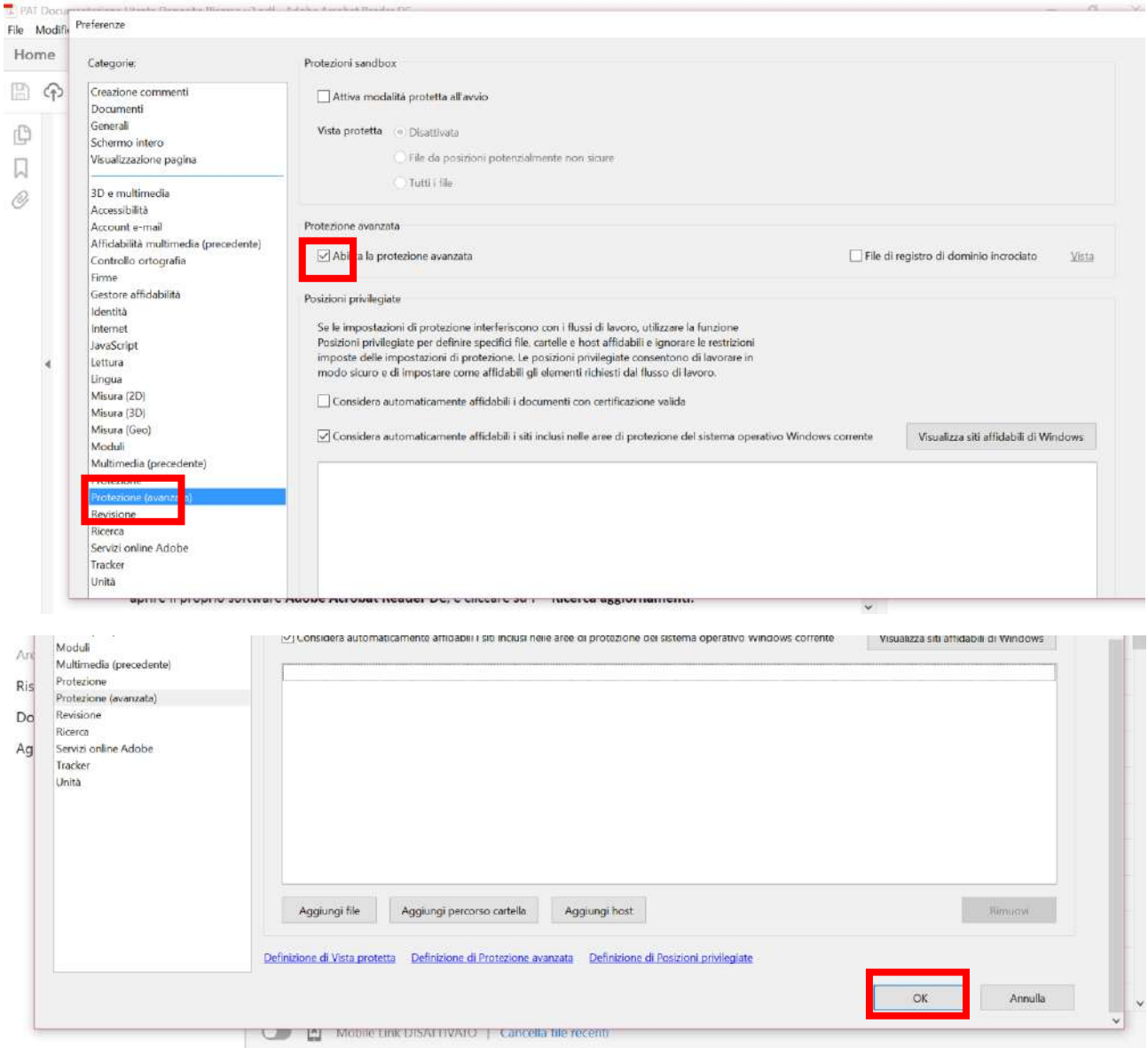
1. Cliccare sul menù **Modifica**



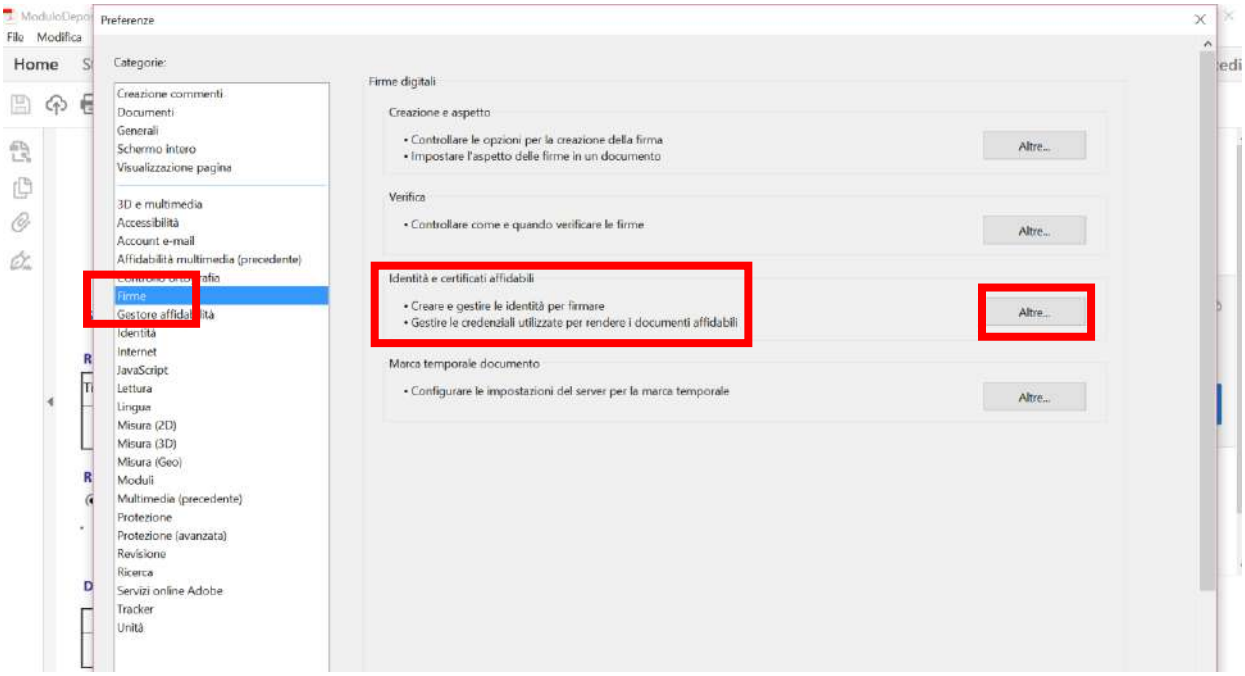
2. Selezionare **Preferenze**



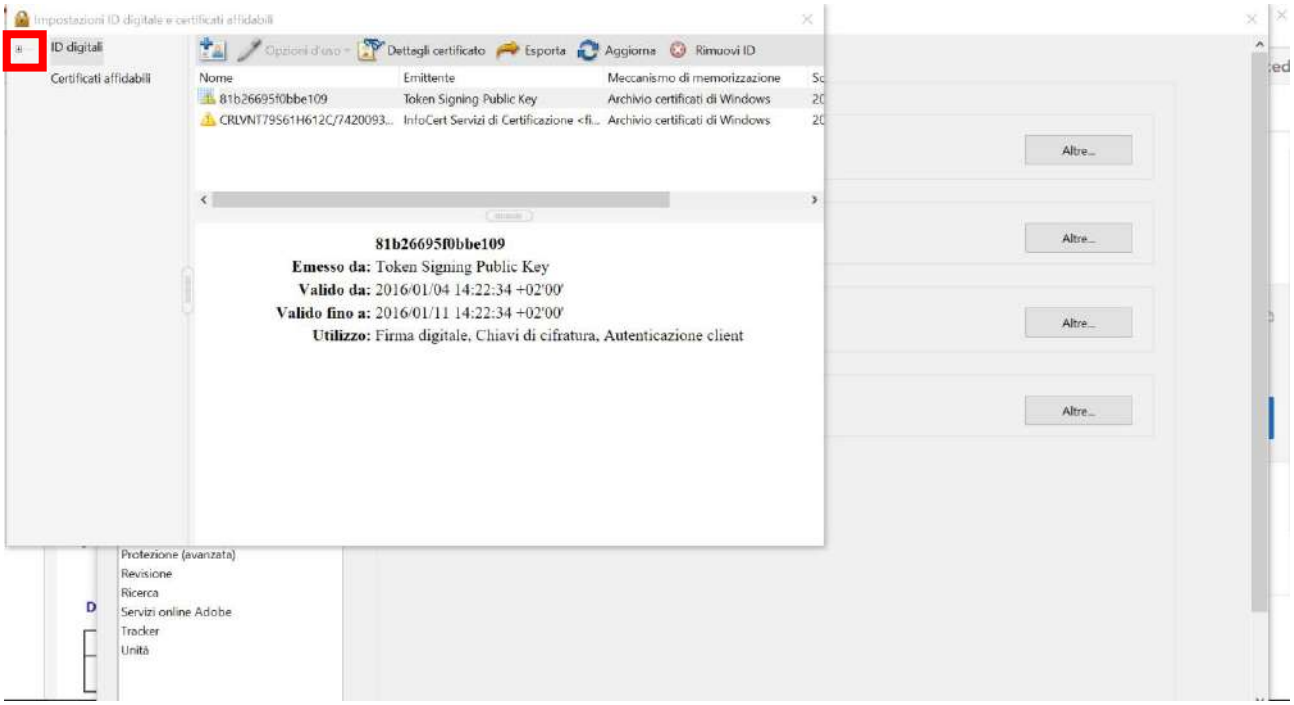
3. Selezionare **Protezione (avanzate)** e <u>togliere</u>, laddove presente, il segno di spunta su **Abilita la protezione avanzata,** scorrere verso il basso la pagina e confermare cliccando su **OK** in fondo alla pagina



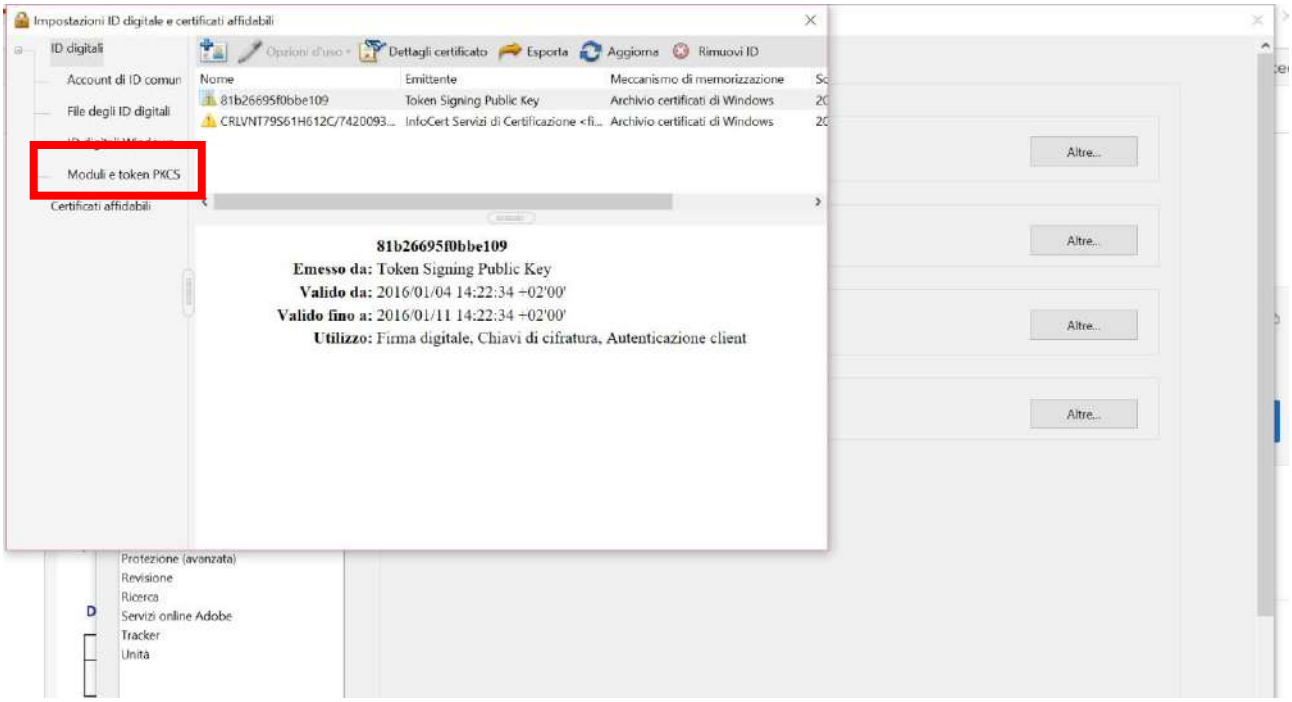
4. Selezionare quindi **Firme** – **Identità e certificati affidabili** e cliccare su **Altre…**



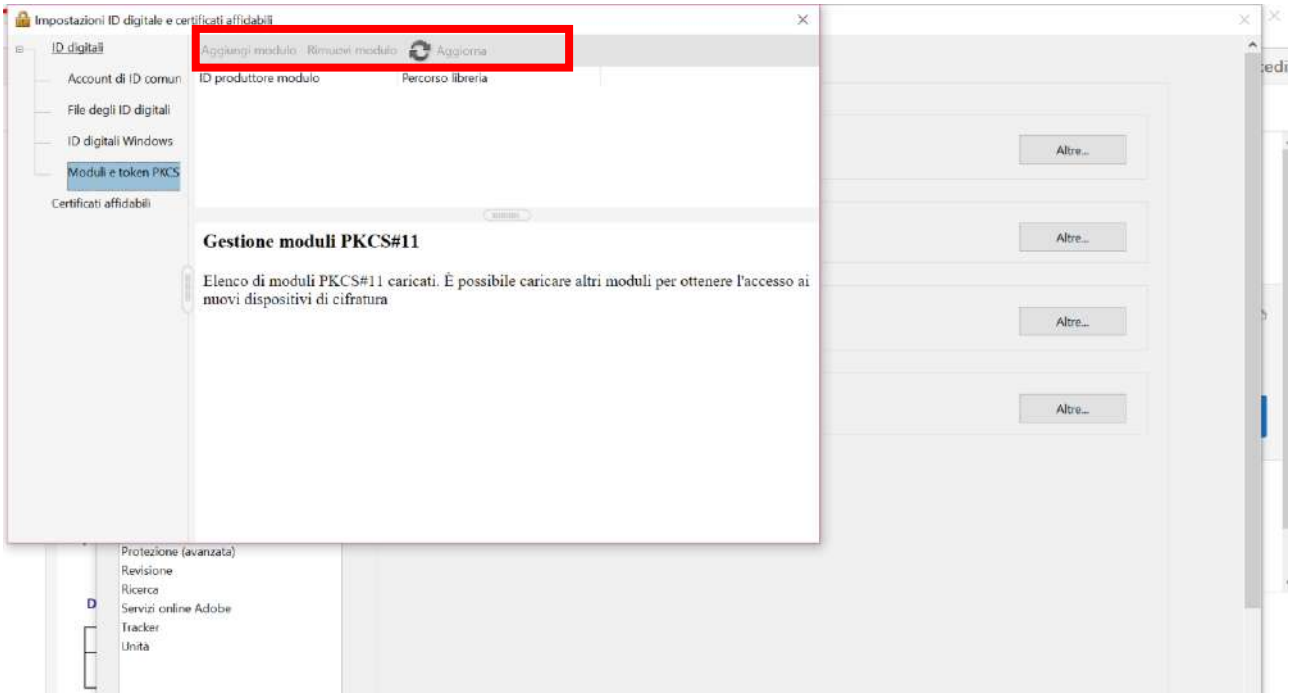
5. A questo punto si aprirà la schermata di Impostazioni ID digitale e certificati affidabili, cliccare sul segno **+** alla sinistra di **ID digitali**



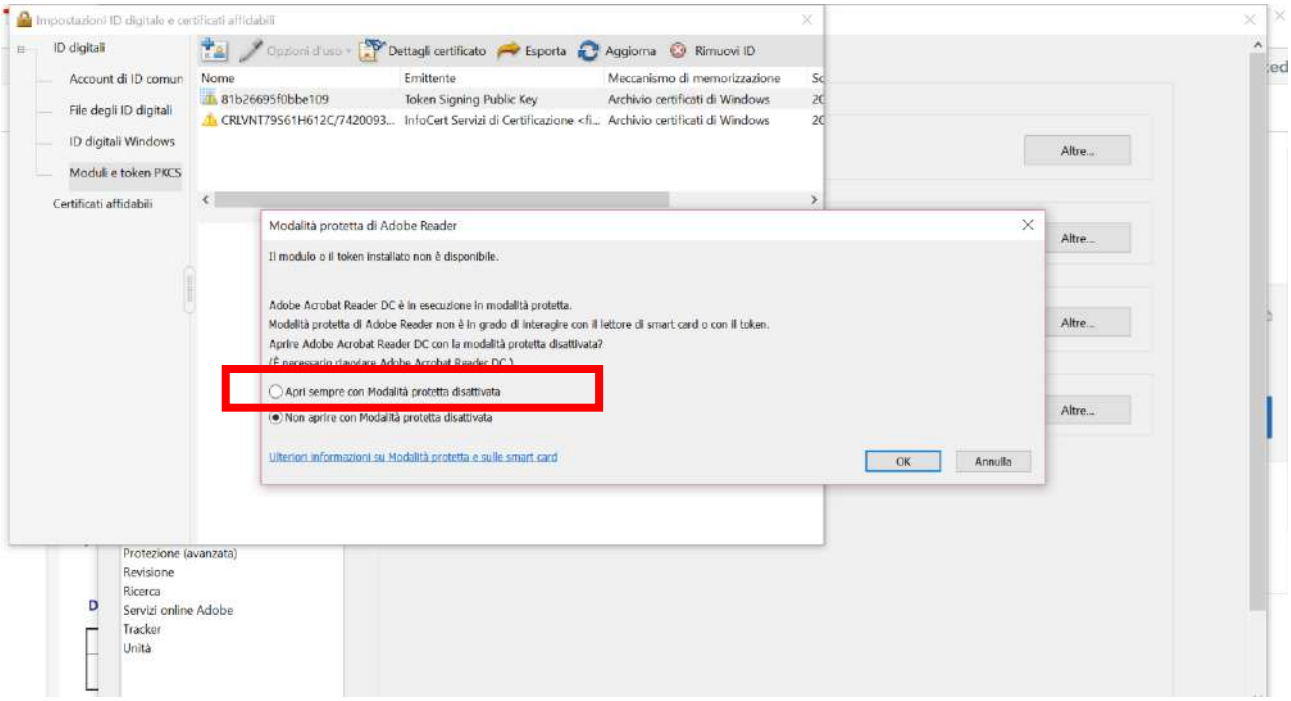
6. Si aprirà quindi un menù sulla sinistra dove occorre selezionare **Moduli e token PKCS**



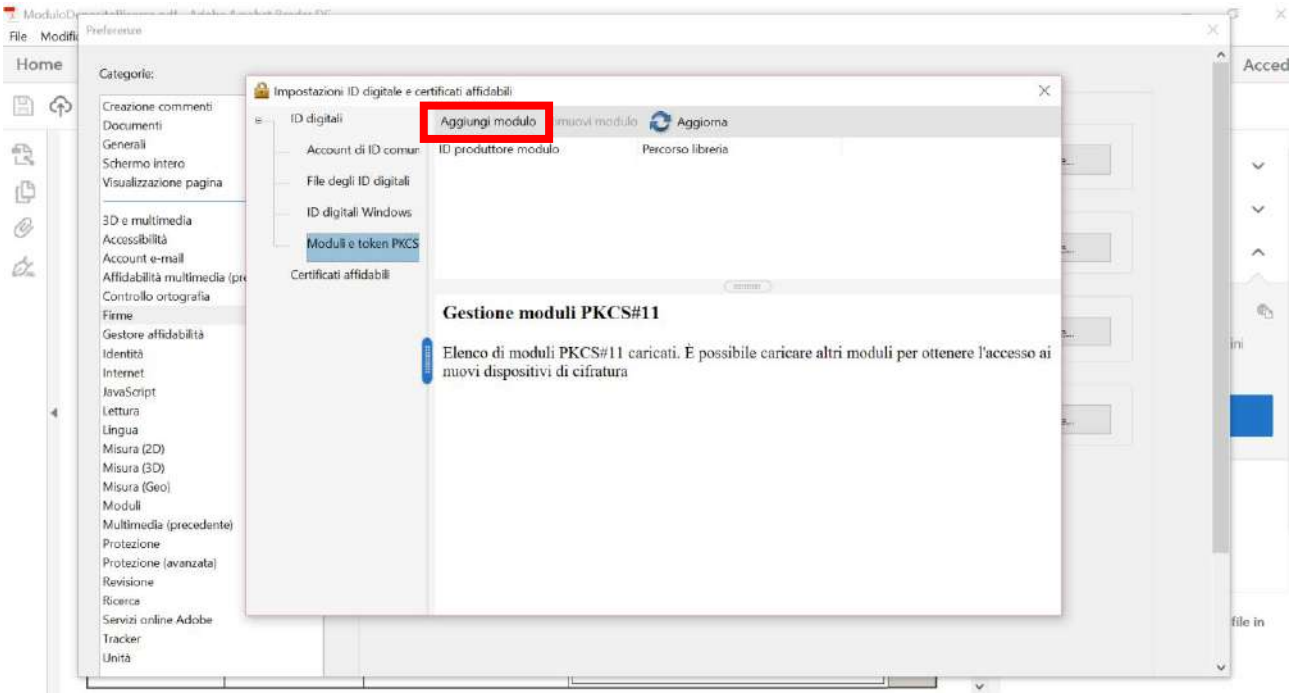
7. A destra dello schermo le voci **Aggiungi modulo** – **Rimuovi modulo** e **Aggiorna** devono essere abilitate – se non lo sono come in figura è possibile che non sia stato eseguito correttamente il passaggio n. 3: togliere il segno di spunta su **Abilita la protezione avanzata** nel menù **Protezione (avanzata)**



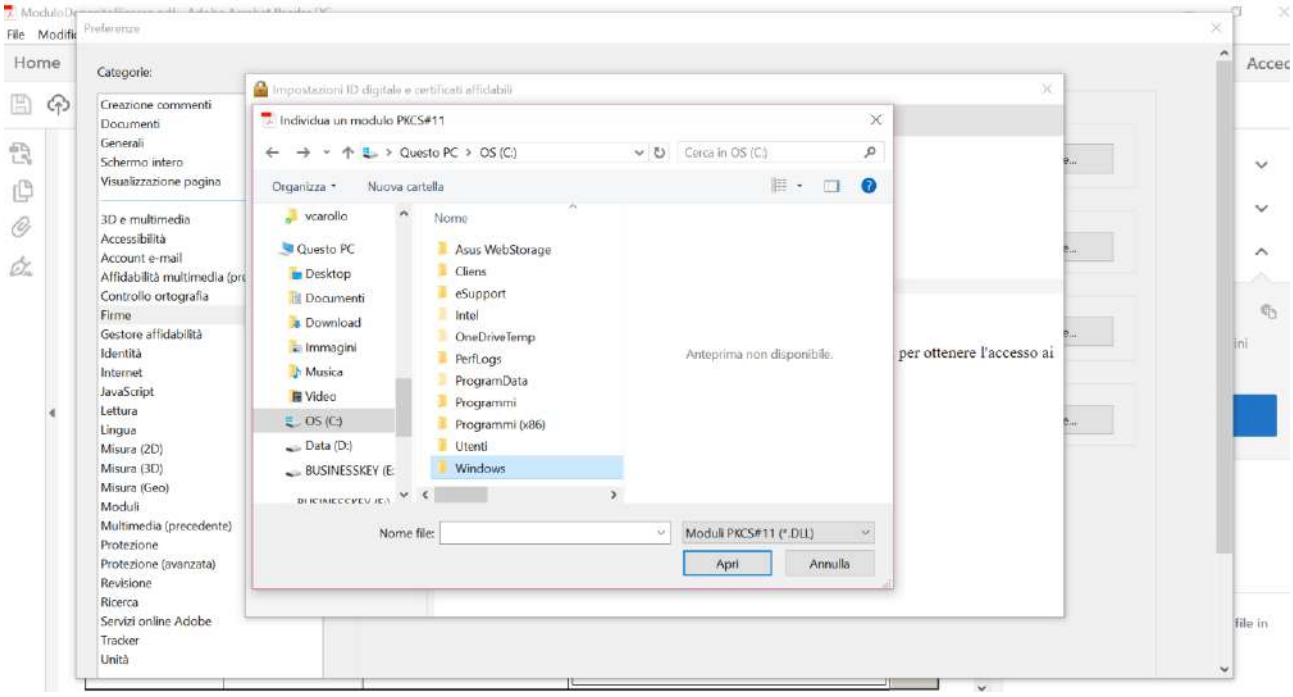
8. Potrebbe aprirsi una schermata che avvisa che Adobe Acrobat è in modalità protetta, nel caso selezionare **Aprire sempre con Modalità protetta disattivata**

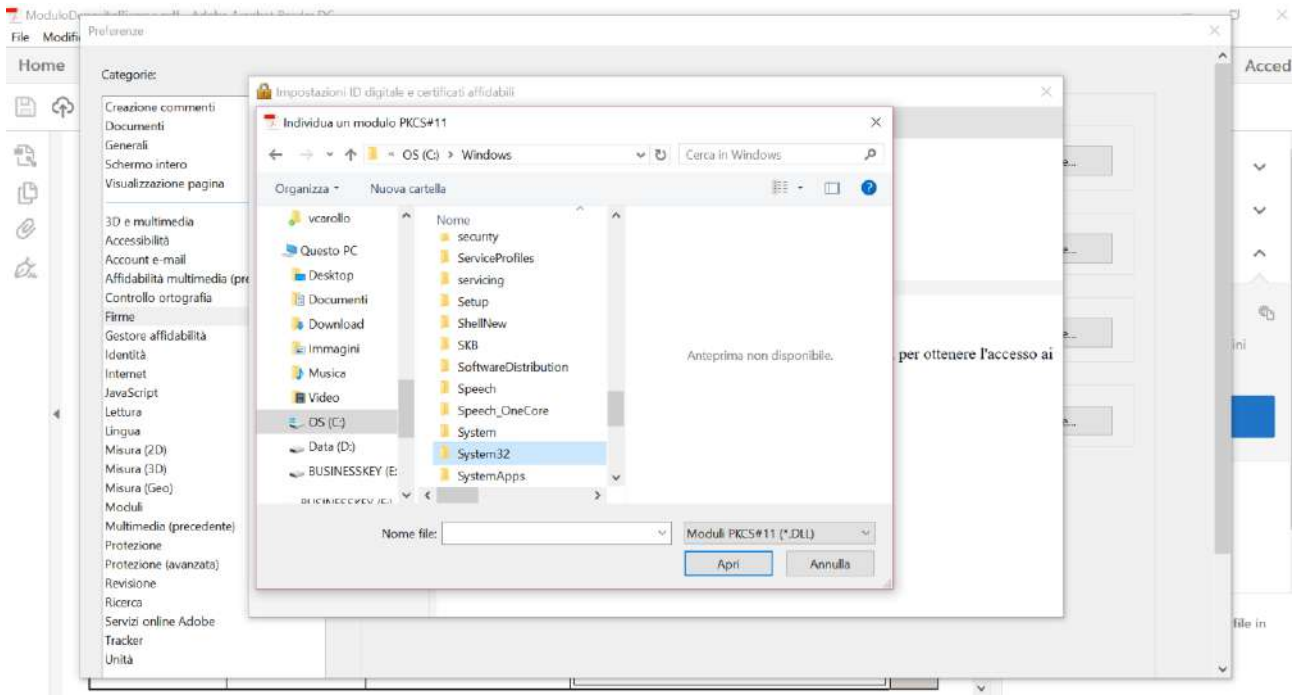


9. Abilitate le voci di destra, cliccare su **Aggiungi modulo**

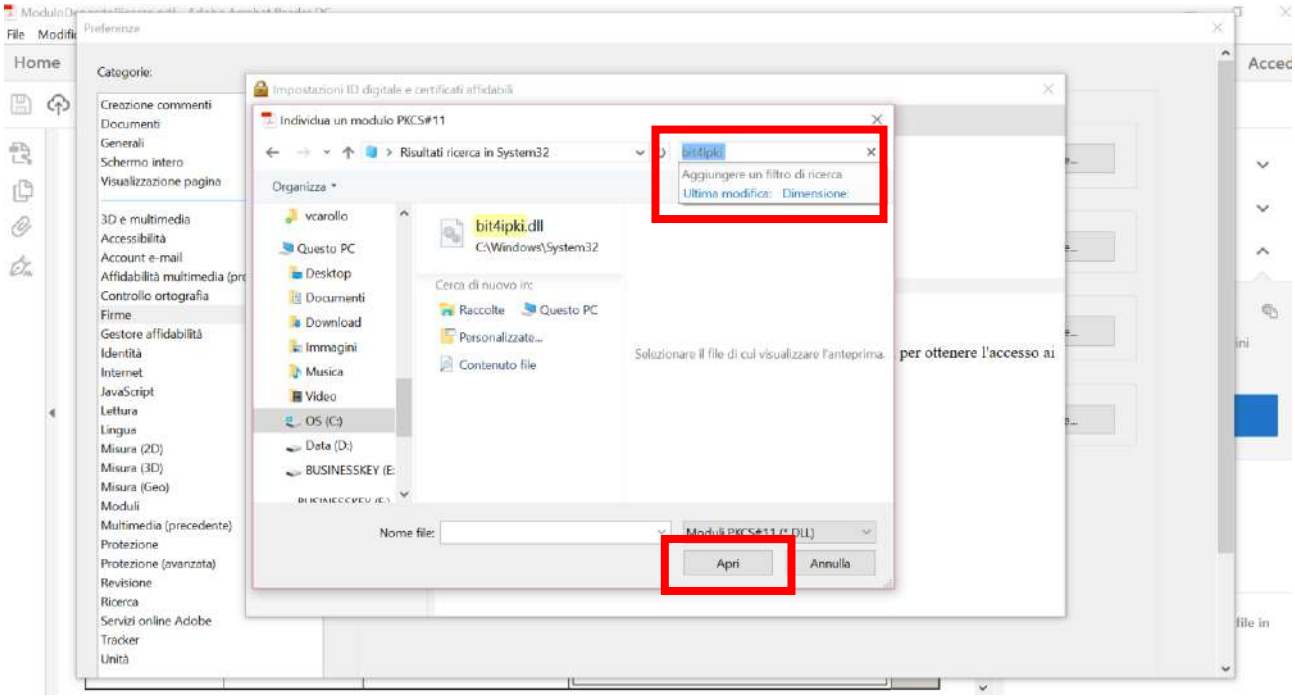


10. Esplorare le cartelle del computer per cercare la libreria della smart card caricata al momento dell'installazione del kit di firma acquistato. Queste librerie si trovano normalmente nella cartella **C:\Windows\System32** come in figura.

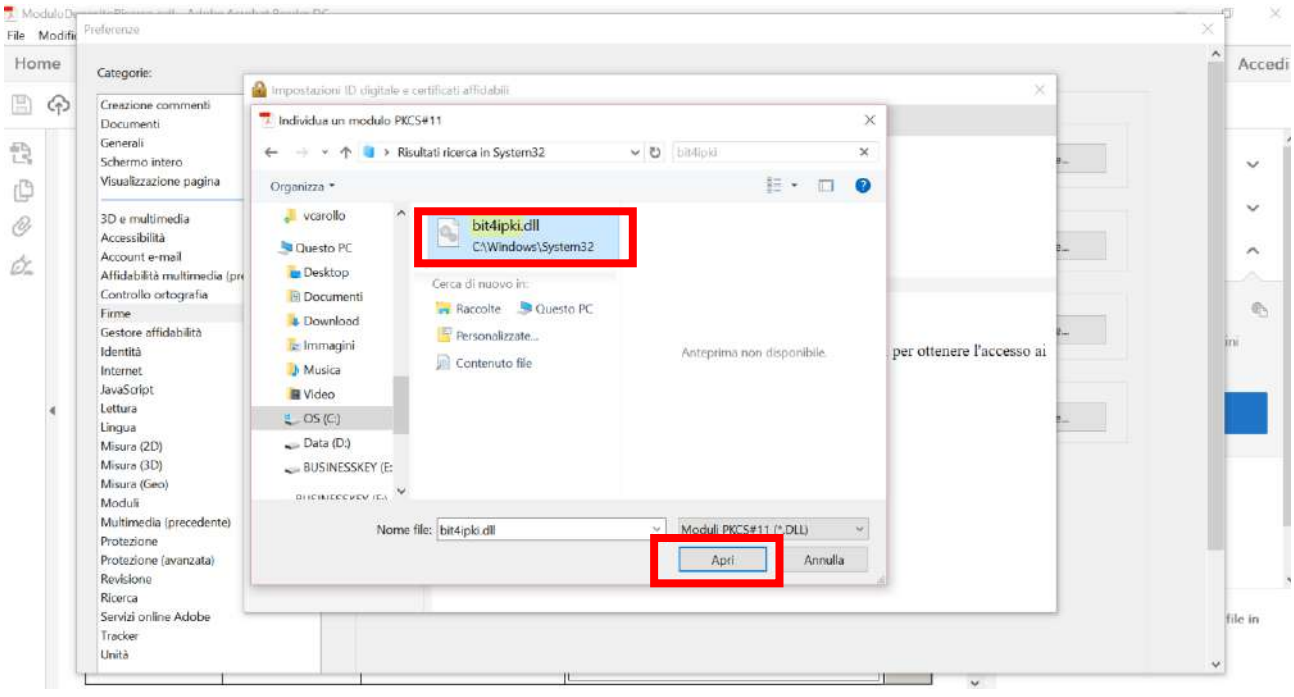




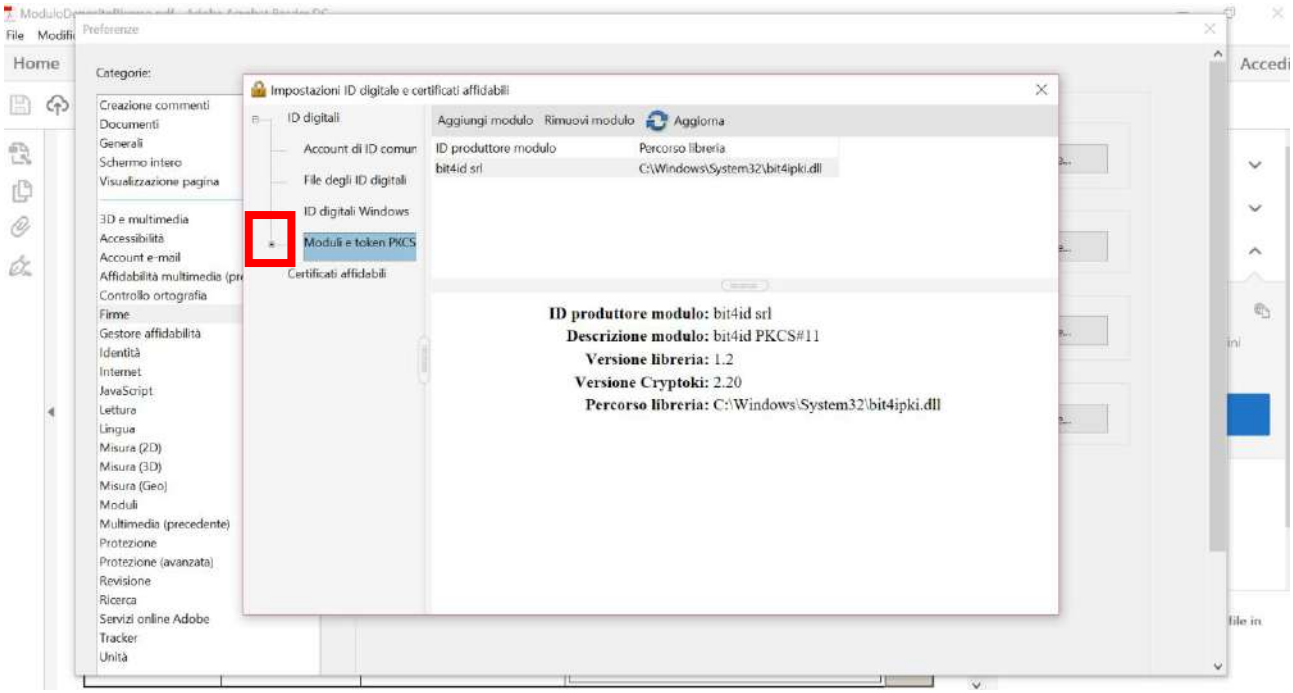
11. Cercare quindi il file **bit4ipki.dll** per le carte ST-Incard (es. chiavetta Infocert) oppure **bit4opki.dll** per le carte Obenthur (es. Arubakey)



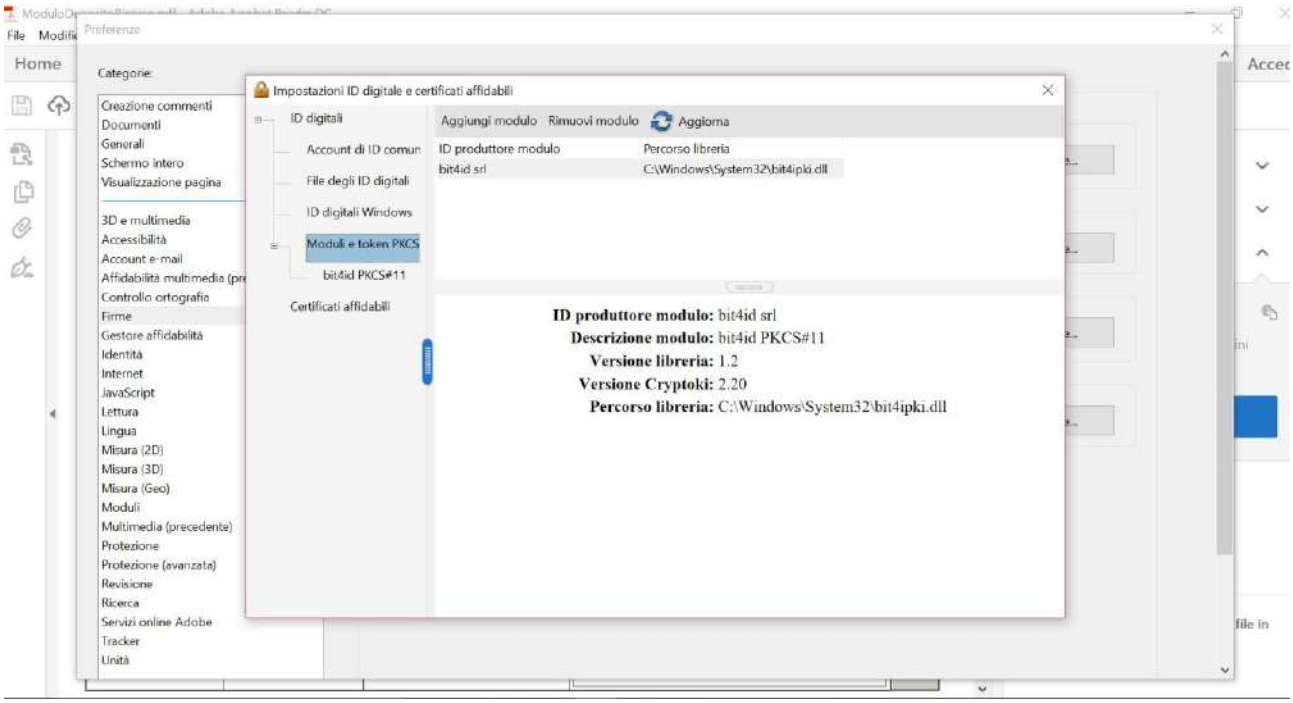
12. Selezionare il file e cliccare su **Apri**:



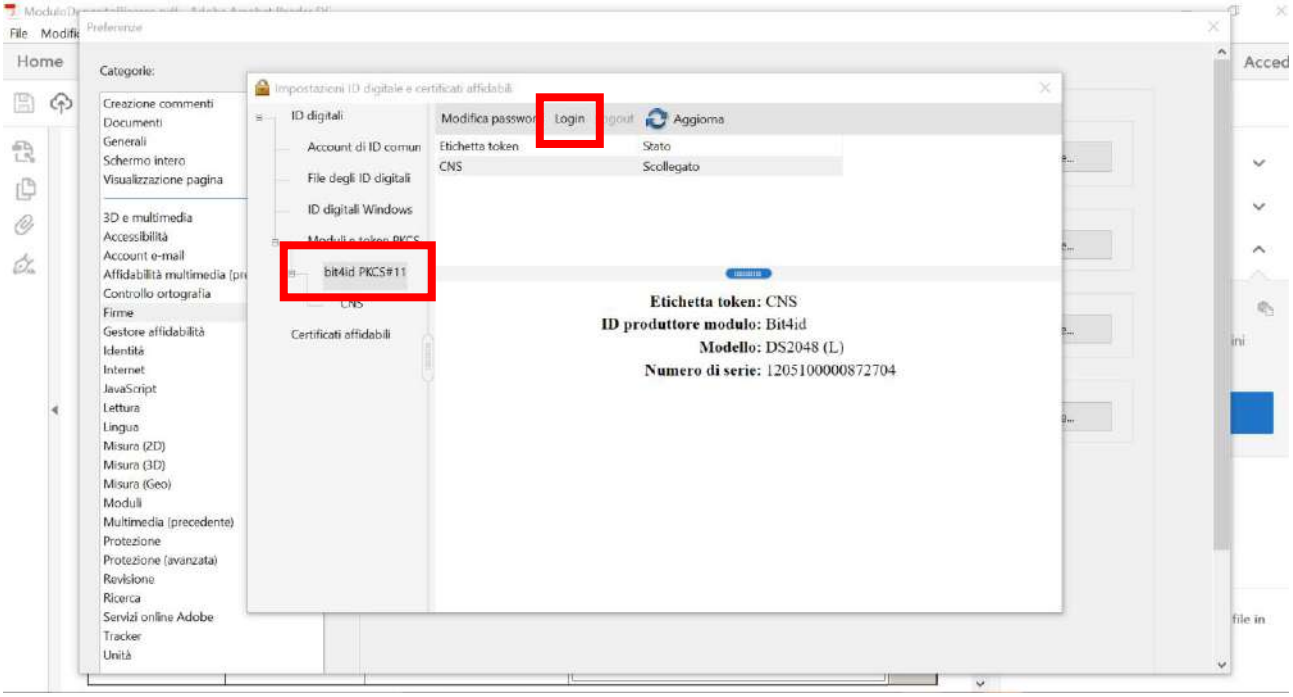
13. A questo punto a fianco a **Moduli e token PKCS** appare un segno **+** che va cliccato perché si espanda il relativo menù.



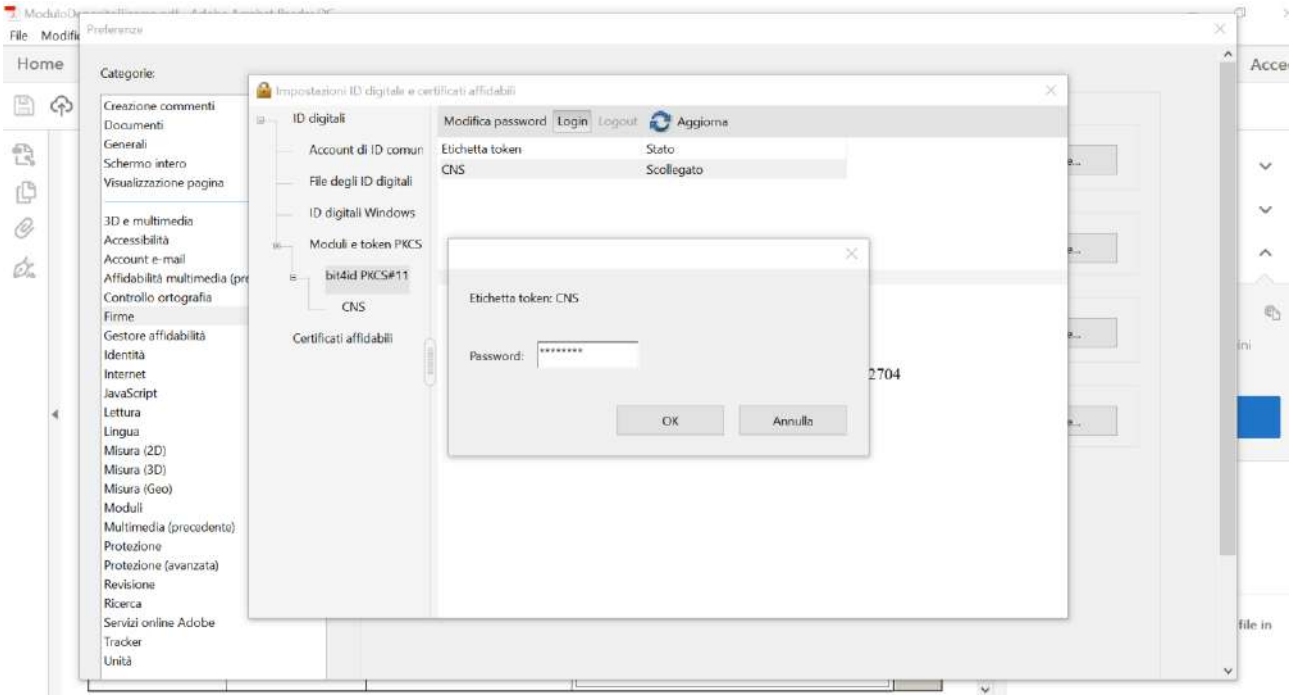
14. anche a fianco a **bit4id PKCS#11** appare un segno **+** che può essere cliccato perché si espanda il relativo menù, <u>se non appare come in figura, chiudere Adobe, estrarre e reinserire il dispositivo di firma digitale e tornare alla schermata</u>.



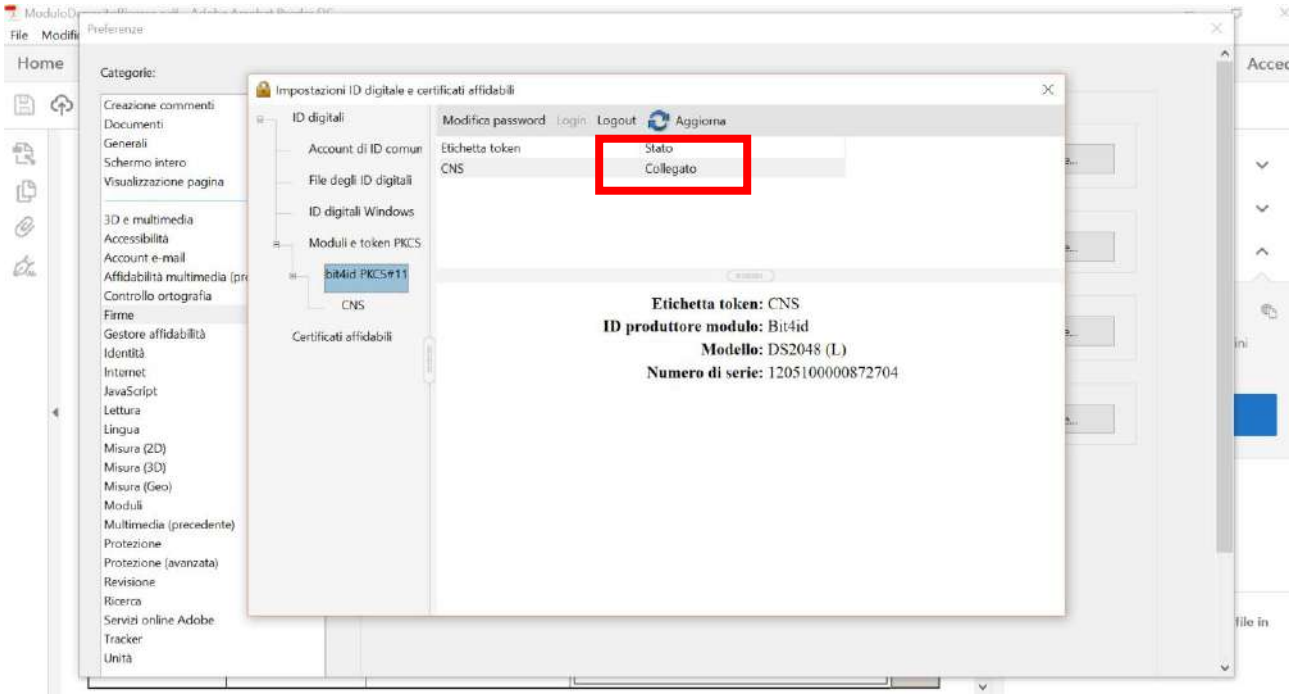
15. Selezionare quindi **bit4id PKCS#11** e nella parte destra selezionare **Login**



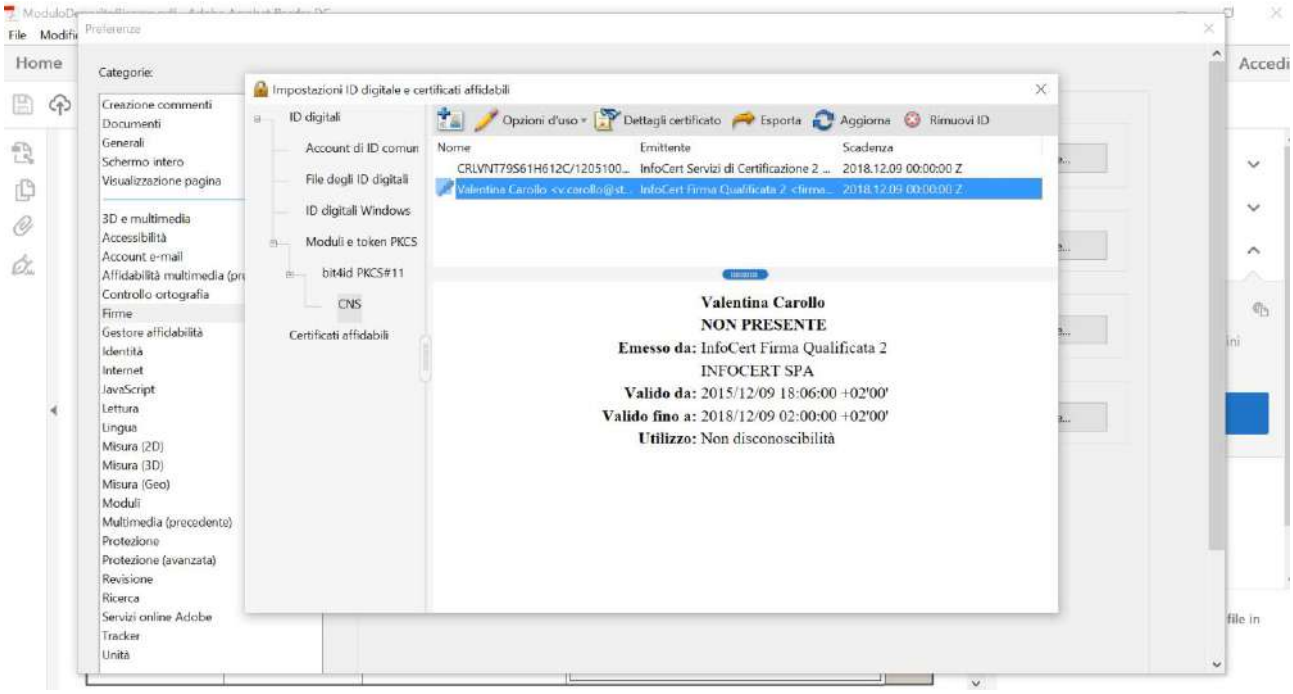
16. Inserire quindi la password associata al dispositivo di firma digitale



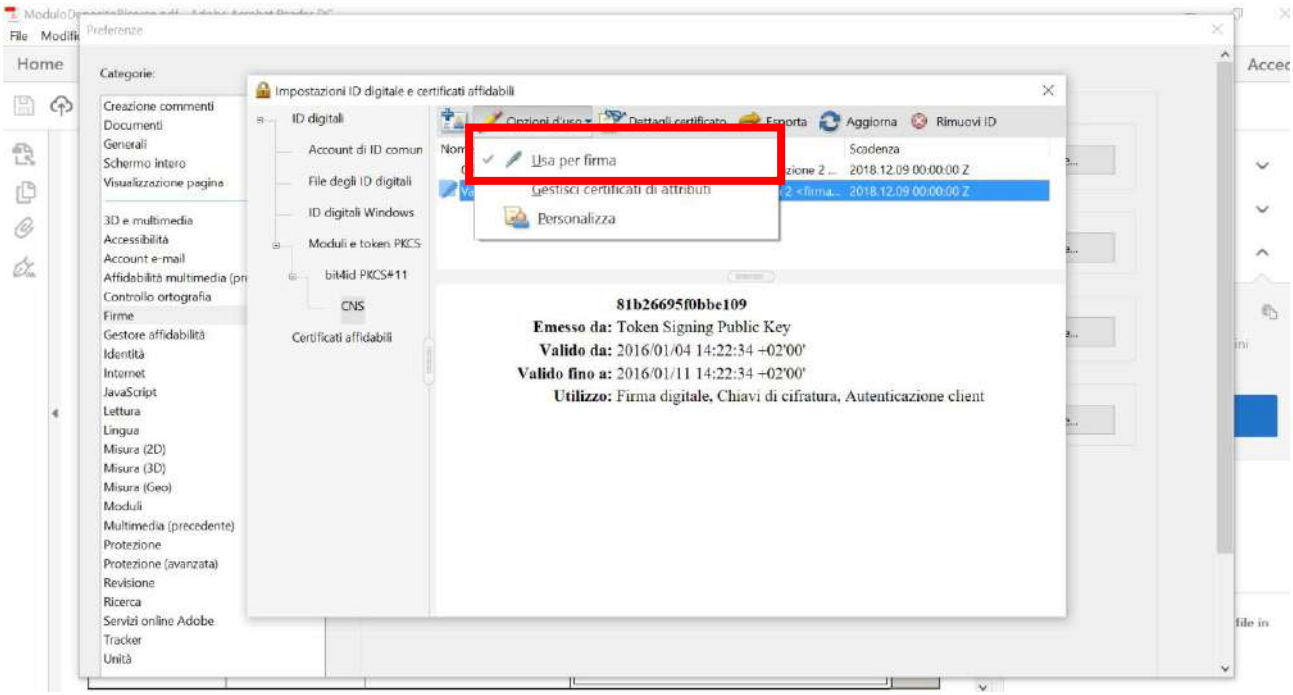
17. A questo punto il dispositivo CNS appare nello stato **Collegato**



18. Selezionare ora **CNS** a sinistra, quindi selezionare a destra la riga contenente il NOME e COGNOME del proprietario della firma digitale (<u>non</u> il CODICE FISCALE)



19. Da **Opzioni d'uso** selezionare **Usa per firma**

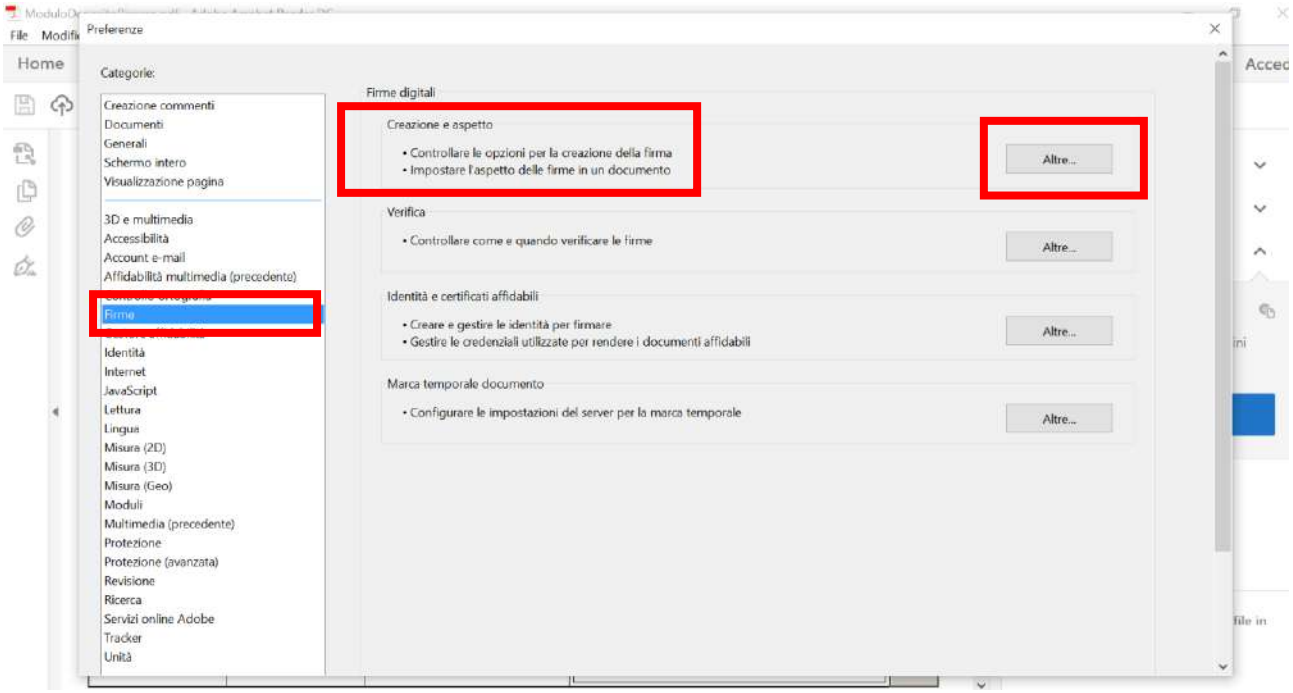


NOTA PER ARUBAKEY e LEXTEL (NAMIRIAL): sembra che I recenti aggiornamenti installino un file dll denominato **bit4xpki.dll** (da notare la x dopo la dicitura bit4) che deve essere utilizzato sia da coloro che posseggono chip di tipo Incard (al posto del bit4ipki.dll) sia da coloro che possiedono chip di tipo Oberthur (al posto del bit4opki.dll)

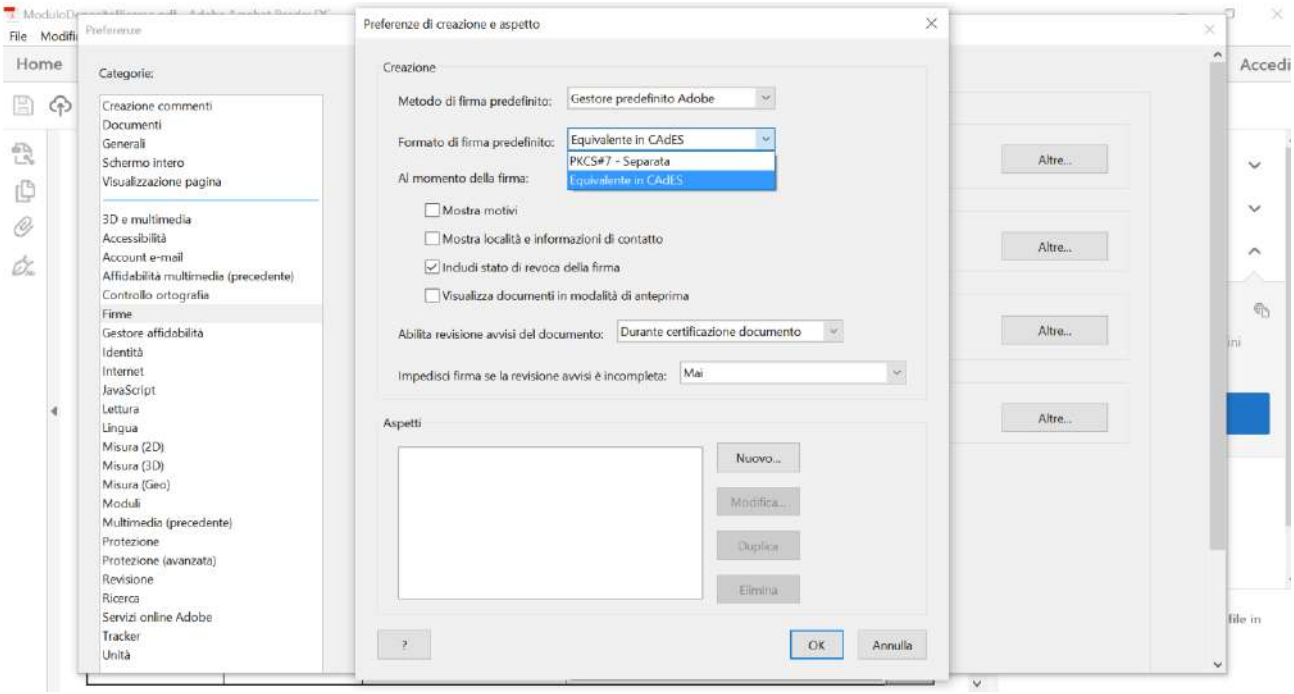
Esistono comunque numerose altre librerie, per i dispositivi non menzionati si consiglia di fare riferimento al sito del fornitore, dove sarà possibile rinvenire i driver specifici.

Configurazione del formato di firma (PAdES BES)

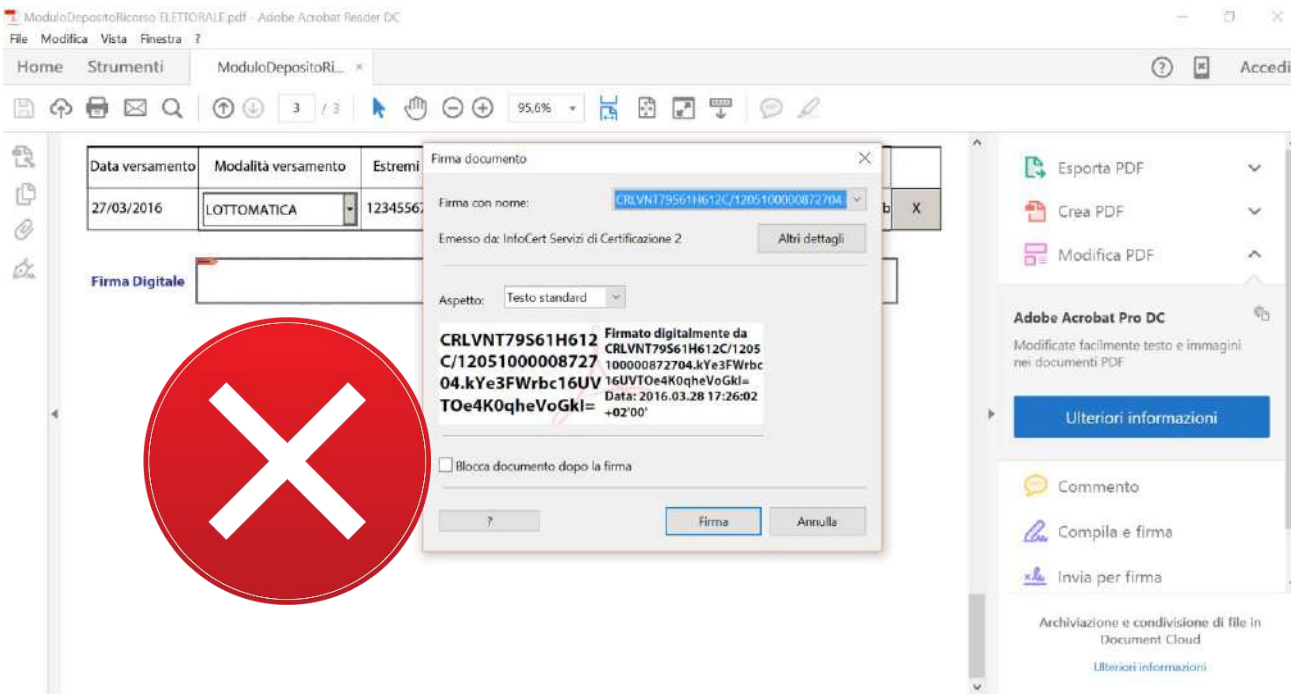
20. Chiudere con X in alto a destra la schermata e tornare su quella precedente dove è selezionato **Firme** e selezionare **Creazione e aspetto – Altre…**



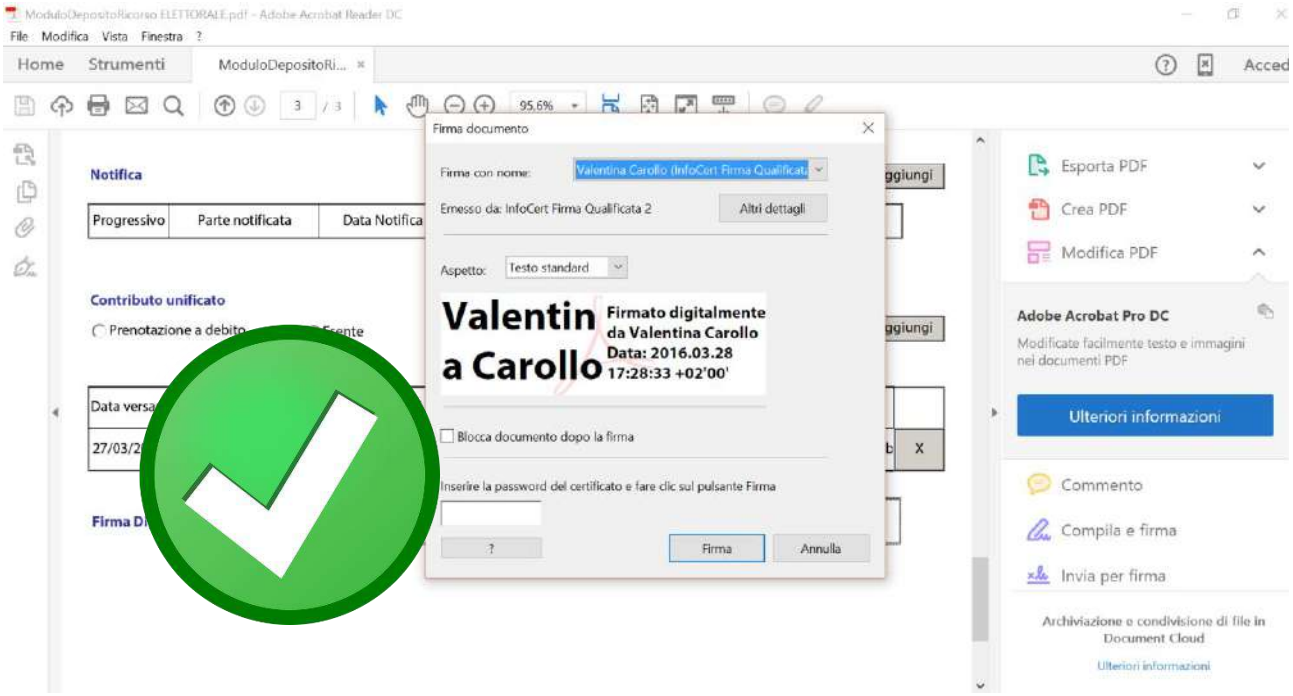
21. A fianco alla dicitura **Formato di firma** predefinito aprire il menù a tendina e selezionare **Equivalente in CAdES**



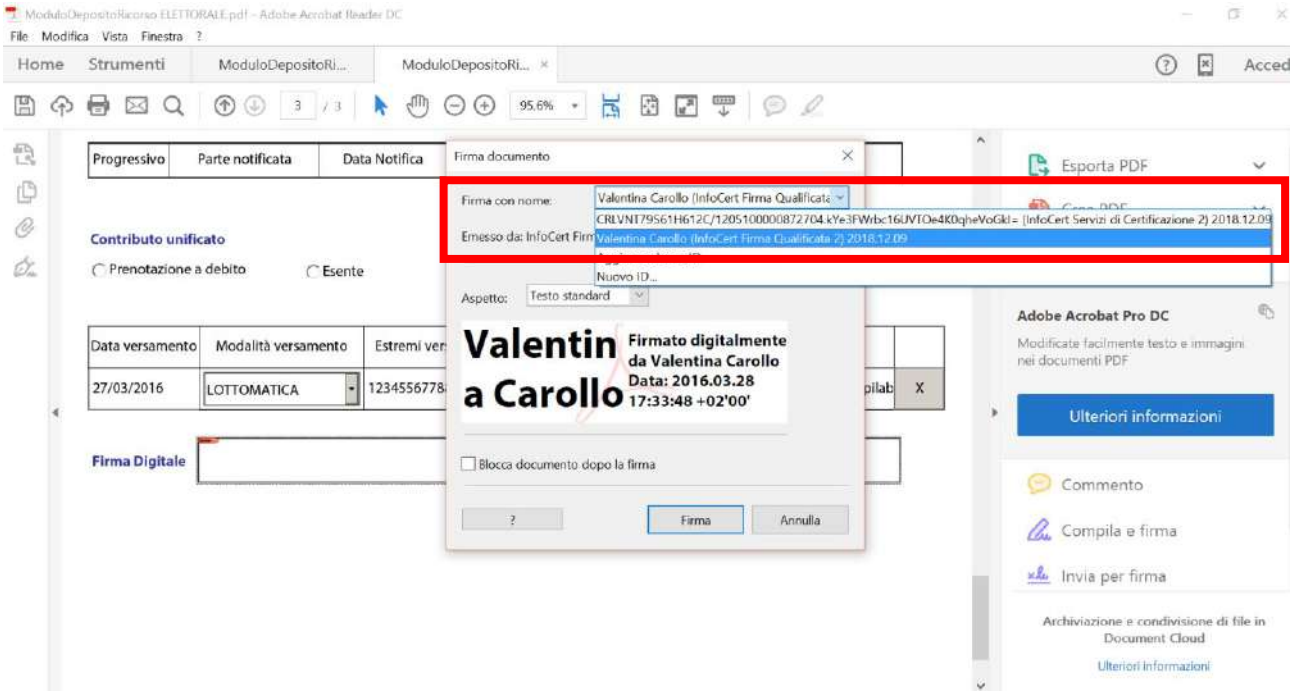
22. A questo punto il software è configurato correttamente e <u>non</u> occorrerà ripetere la procedura indicata da 1 a 22. Può accadere che occorra ripetere la procedura in caso di importanti aggiornamenti di versione del programma o del computer. In ogni caso, ogni volta che si firma un documento <u>NON</u> dovrebbe apparire il codice fiscale come in figura:



23. <u>Se la procedura di firma è corretta apparirà il NOME e COGNOME del firmatario</u>



24. Eventualmente verificare dal menù a tendina apposto accanto a Firma con nome che sia presente il corretto certificato caratterizzato da NOME e COGNOME



Guida predisposta da: avv. Valentina Carollo – avv. Andrea Pontecorvo

V2 – nota aggiunta da Stefano Baldoni