VADEMECUM

COME SI INSERISCE L'ATTESTAZIONE DI CONFORMITA' NELLA COPIA INFORMATICA

Premessa

L'attestazione di autenticità dopo l'avvento del PCT ha assunto una importanza centrale nella attività quotidiana dell'avvocato, che tuttavia si ritrova disorientato:

- dalla coesistenza del formato cartaceo (analogico), dei vari tipi di formato digitale (pdf "testuale" e pdf "immagine") e di firma digitale (CAdES e PAdES) sia delle "copie" da autenticare sia dei documenti rispetto ai quali viene attestata la conformità, e dall'intreccio dei casi e delle procedure che regolano il passaggio dall'uno all'altro formato, ed il loro diverso impiego;
- dalla frammentarietà, dalla rapida successione e dalla ridondanza delle norme legislative e regolamentari;
- dal progressivo ampliamento dei casi e delle procedure nelle quali è consentito, ovvero è obbligatorio, ricorrere alla attestazione di autenticità;
- dalle difficoltà di configurazione di hardware e software, causate anche dalla evoluzione delle tecnologie, degli standards e delle scelte tecniche e commerciali dei produttori.

Al momento è difficile pensare a soluzioni "definitive", ma invece possibile ricercare, con un approccio pragmatico, le soluzioni "in questo momento" più aderenti al quadro normativo e più facili da usare.

La **semplicità, stabilità e facilità d'uso** dovrebbero quindi diventare obiettivi primari.

Tralasciando le "normali" modalità di attestazione cartacea in calce alla stampa cartacea della copia informatica (alla quale l'attestazione deve essere "congiunta materialmente"), per l'attestazione di conformità delle sole "copie informatiche" da parte dell'avvocato si può individuare **al momento** un principio "generale", che deriva:

- dal nuovo art. 16-undecies comma 2 il quale in relazione alle disposizioni sul PCT, del CPC e della L.53/94 prescrive che "*quando l'attestazione di conformita' si riferisce ad una copia informatica, l'attestazione stessa* ***e' apposta nel medesimo documento informatico***".

- dall'attuale impossibilità **in concreto** di inserire l' attestazione su di un documento informatico separato **fino alla pubblicazione delle modalità di individuazione tecniche dell'atto di riferimento** da parte del Ministero della Giustizia, come previsto dal comma 3 dello stesso art 16-undecies.

Quindi dal 21 agosto 2015 l'attestazione deve essere apposta – temporaneamente, sino a termine *incertus quando* - nella copia informatica oggetto di autenticazione.

E' così stata **sospesa** l'alternativa, che è rimasta in vigore dal 27 giugno (DL 83/15) alla pubblicazione il 21 agosto della legge di conversione, che tentava di semplificare con la dizione "*contenente l'indicazione dei dati essenziali per individuare univocamente la copia a cui si riferisce*" le più stringenti regole tecniche dell'art. 71 del CAD (Art 6 c.3 II parte DPCM 13.11.14: "*contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico*" (cioè l'UTC e l'hash del file oggetto di autentica)

Ciò non toglie che la attestazione di autenticità debba essere contenuta anche nella relata di notifica via PEC, perché così continua a prevedere lo stesso comma 3 dello stesso art. 16-undecies.

Cerchiamo di analizzare quattro casi:

A) estrazione di copia informatica **dal fascicolo informatico**: il comma 9-bis dell'art. 16-bis della L.221/2012 consente all'avvocato di attestare la **conformita' delle copie da lui estratte ai corrispondenti atti contenuti nel fascicolo informatico.** Attenzione: l'obbligo c'è proprio per l'autenticazione delle "copie informatiche", non per i "duplicati" (=copie identiche bit per bit aventi lo stesso "hash" dell'originale) che non richiedono "autenticazione".

B) estrazione di copia informatica di atto processuale o provvedimento **detenuti in originale o copia conforme**, e cioè di atti cartacei. In sostanza scansioni "fotografiche" (copia per immagine= contenuto e forma identici, CAD art.1 lettera i-ter), o copie identiche del solo contenuto. La legge 132/2015 introducendo l'art. **16-decies** della L. 221/2012 ha qui ampliato il potere di certificazione di conformità dell'avvocato, che adesso è stato esteso alla "*copia informatica* ***anche*** *per immagine, di un* ***atto processuale di parte o di un provvedimento del giudice*** *formato su supporto analogico e* ***detenuto in originale o in copia conforme***" che venga fatta **oggetto di deposito telematico,** a prescindere cioè dal fatto che essa sia state o meno oggetto di notifica. Quindi per questo caso il presupposto per l'esercizio del potere di autentica è la "detenzione" dell'originale o della copia conforme dell'atto processuale di parte o del provvedimento giudiziale di cui si estrae l'immagine.

C) estrazione di copia informatica **del titolo esecutivo, del precetto e del verbale di pignoramento** che devono essere depositati telematicamente nel procedimento esecutivo: per questo caso il **comma 2 dell'art. 16-bis** prevede che "*ai fini del presente comma, il difensore attesta la conformita' delle copie agli originali, anche fuori dai casi previsti dal comma 9-bis e dall'articolo 16-decies*". Anche qui è obbligatorio l'inserimento dell'autentica nella copia per immagine di tali atti.

D) estrazione di copia informatica **per immagine dell'atto cartaceo destinato alla notifica via PEC dell'avvocato** (art. 18 DM 44/2011).
Il nuovo testo del **comma 2 dell'art. 3-bis** della L. 53/94 prevede che: *2. Quando l'atto da notificarsi* ***non*** *consiste in un documento informatico, l'avvocato provvede ad estrarre* ***copia informatica dell'atto formato su supporto analogico, attestandone la conformita' con le modalita' previste dall'articolo 16-undecies*** *del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221. La notifica si esegue mediante*

allegazione dell'atto da notificarsi al messaggio di posta elettronica certificata.

Tuttavia come detto la parte finale del nuovo comma 3 dell'art. 16-undecies prevede poi che "*se la copia informatica e' destinata alla notifica,* ***l'attestazione di conformita' e' inserita nella relazione di notificazione***".

Fermo restando che nella relata deve essere sempre certamente inserita l'attestazione di conformità della copia per immagine, è aperta la discussione se tale attestazione sia ora possibile (visto che le specifiche tecniche ancora non ci sono) e, se si, se essa si aggiunga o sostituisca l'attestazione da inserire nella stessa copia per immagine.

Ragionevolezza e prudenza inducono a ritenere che tale attestazione (e quindi la notifica via PEC) allo stato sia possibile ma sia opportuno anche inserire l'attestazione nella copia informatica (non nel duplicato!) oggetto di notifica.

Poiché le "copia informatiche" viste sopra avranno sempre il formato "pdf" ("portable document format") e dovranno sempre essere digitalmente sottoscritte, analizzeremo due modalità di inserimento e di firma della attestazione di autenticità in un documento "pdf", precedute da alcune ulteriori considerazioni sulle caratteristiche concrete dei documenti informatici scaricabili.

Vedremo che il secondo metodo, ove correttamente configurato, ha un campo di utilizzo assai più esteso di quello della autenticazione, come scoprirà chi avrà la pazienza di sperimentarlo.

Servono naturalmente: un computer (qui con sistema operativo windows); il dispositivo di firma digitale; il software Adobe Reader ver. 11 (GRATUITO scaricabile da internet); il file .pdf da autenticare.

Per prima cosa procuriamoci il documento da autenticare. Scarichiamo dal PST un atto giudiziale, in questo caso una sentenza di Corte d'Appello firmata digitalmente con modalità PADES-BES, ed apriamola con il programma «Adobe reader XI» configurato.

E' possibile scaricare l'atto come

- come «Duplicato informatico»
- come «Copia informatica»

semplicemente selezionando il flag voluto accanto alla relativa voce nella finestra del PST, come segue:



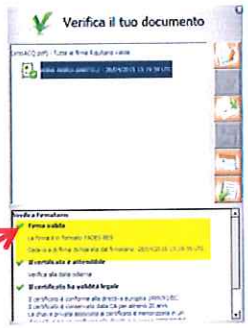


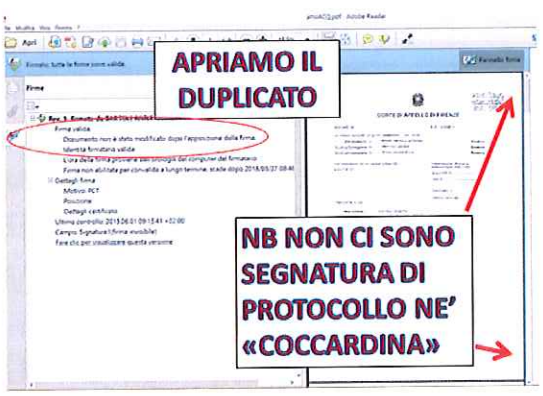
Ricordo ancora che il "DUPLICATO" non necessita di autenticazione, mentre la "copia informatica" si: vedi art. 16-bis comma 9 bis della L. 17 dicembre 2012, n. 221 :

- "Le **copie analogiche ed informatiche**, anche per immagine, estratte dal fascicolo informatico e **munite dell' attestazione di conformità** a norma del presente comma, equivalgono all'originale.

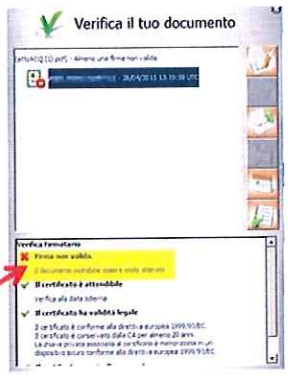
- "Il **duplicato informatico** di un documento informatico deve essere prodotto mediante processi e strumenti che assicurino che il **documento informatico ottenuto sullo stesso sistema di memorizzazione o su un sistema diverso contenga la stessa sequenza di bit del documento informatico di origine** (= abbia la stessa «impronta informatica», anche detta «hash»)"

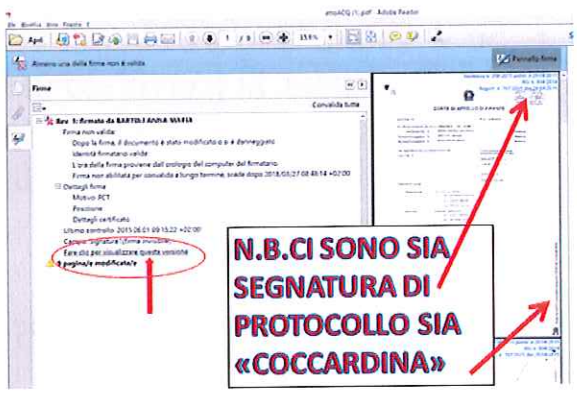
Scarichiamo e verifichiamo l'integrità del DUPLICATO della sentenza: «attoACQ» Il risultato è:



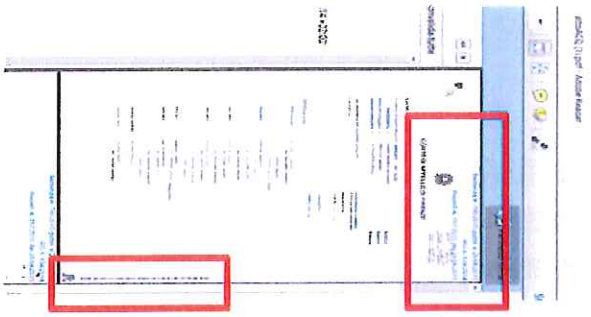


Scarichiamo e verifichiamo l'integrità della COPIA INFORMATICA della sentenza: «attoACQ(1)» Il risultato è:





Dal confronto tra le due versioni - prima e dopo la firma digitale del cancelliere – vediamo le «aggiunte» che hanno trasformato il «duplicato» in «copia informatica»:



COME SI SPIEGA?

- La firma della «copia informatica», a differenza di quella del «duplicato», risulta «non valida» alla verifica, ma il software «Adobe reader XI» **se correttamente configurato** indica il motivo della apparente «non validità»:
- DOPO LA FIRMA IL SOFTWARE DEL MINISTERO HA AGGIUNTO LA SEGNATURA DI PROTOCOLLO IN BLU E LA «COCCARDINA» A LATO CON I DATI DEL PUBBLICO UFFICIALE FIRMATARIO.
- Se si seleziona «*fare clic per visualizzare questa versione*» in Adobe reader XI (cerchiato in rosso nella slide precedente) si vedrà la versione «originale» prima della modifica (= che è e deve essere identica al «duplicato»)

Quindi in questo caso l'avvocato deve autenticare la "copia informatica" per il fatto che essa presenta quale motivo di "alterazione" la apposizione della (obbligatoria) "segnatura di protocollo" da parte dello stesso Ministero.

Tale adempimento è dovuto, ma a mio giudizio irragionevole perchè al suo interno è verificabile e consultabile l'"originale" dell'atto (equivalente al "duplicato") se il documento risponde – come deve – alle specifiche fissate dal D.P.C.M. del 22 febbraio 2013 (illustrate dall'AGID in questa guida alle firme multiple).

E' opportuno segnalare che talvolta gli atti scaricati sia come "duplicato", sia come "copia informatica", risultano identici.

Questo perché in questo caso il cancelliere ha inserito il provvedimento nel fascicolo telematico senza firmarlo digitalmente (e senza inserire la "segnatura di protocollo").

In questo caso vale comunque il principio: "*quod est in actis est originale*" al momento fissato dal comma 9-bis dell'art. 16-bis, per il quale:

"*Le copie informatiche, anche per immagine, di atti processuali di parte e degli ausiliari del giudice nonche' dei provvedimenti di quest'ultimo, presenti nei fascicoli informatici o trasmessi in allegato alle comunicazioni telematiche dei procedimenti indicati nel presente articolo,* ***equivalgono all'originale anche se prive della firma digitale del cancelliere di attestazione di conformità all'originale***"

Poiché l'attestazione dell'avvocato è diretta a documentare la correttezza della **sua** operazione nel fascicolo informatico, e non quella del cancelliere, secondo me se l'avvocato ha scaricato il file come "duplicato" dovrà trattarlo come tale e non dovrà autenticarlo, se lo ha scaricato come "copia informatica" dovrà trattarla come tale e la dovrà autenticare.

Se la "copia informatica" da autenticare proviene dalla scansione dell'atto detenuto dall'avvocato, come abbiamo visto in premessa, è sempre necessaria l'autenticazione.

Passiamo alla pratica.

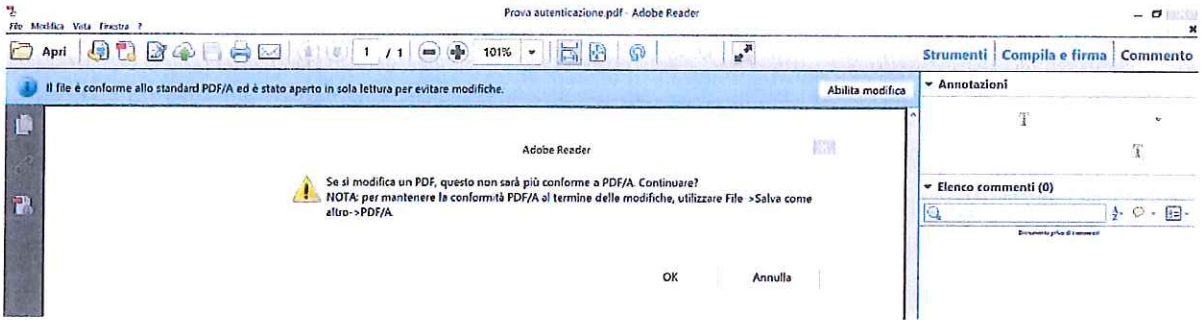
METODO A

Annotazione + firma CAdES

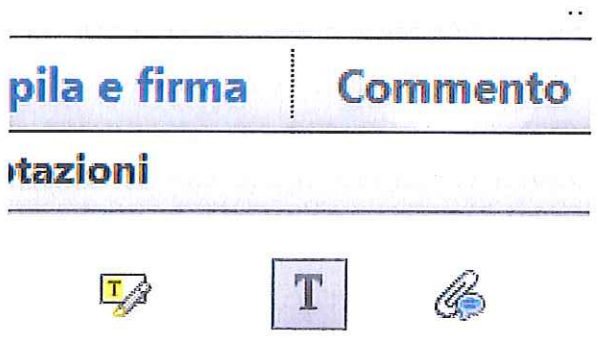
Modifica del documento informatico mediante l'annotazione grafica della formula di autentica in calce al documento, e sua successiva firma digitale in formato CADES, con produzione di un file *.pdf.p7m.

E' la soluzione di uso corrente ed è allo stato accettata dagli uffici giudiziari. Comporta tuttavia **l'oggettiva alterazione del file originale**, la possibilità che i software di verifica segnalino problemi, ed una minore facilità nella sua consultazione.

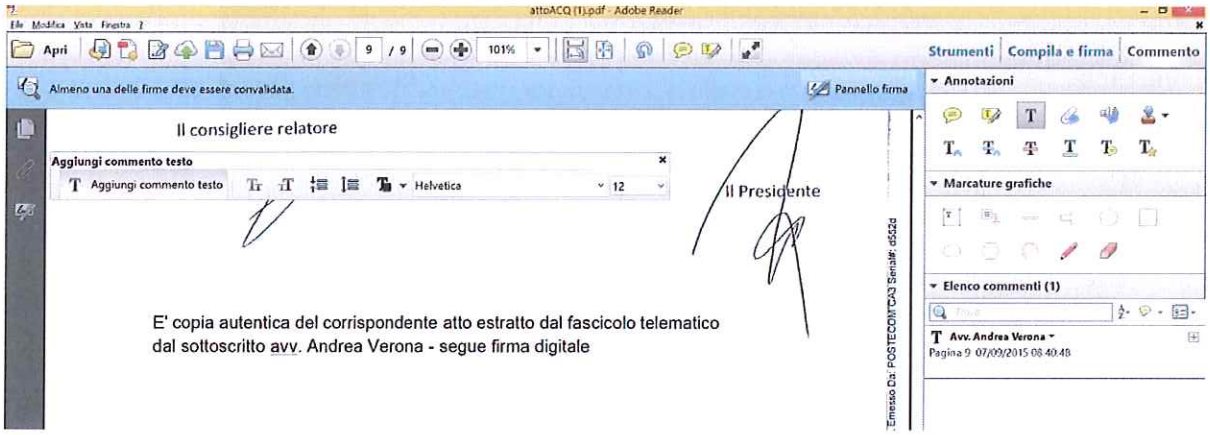
Cliccare sulla sezione "Commento - Annotazioni"; può comparire l'avviso delle conseguenze della modifica del formato PDF/A:



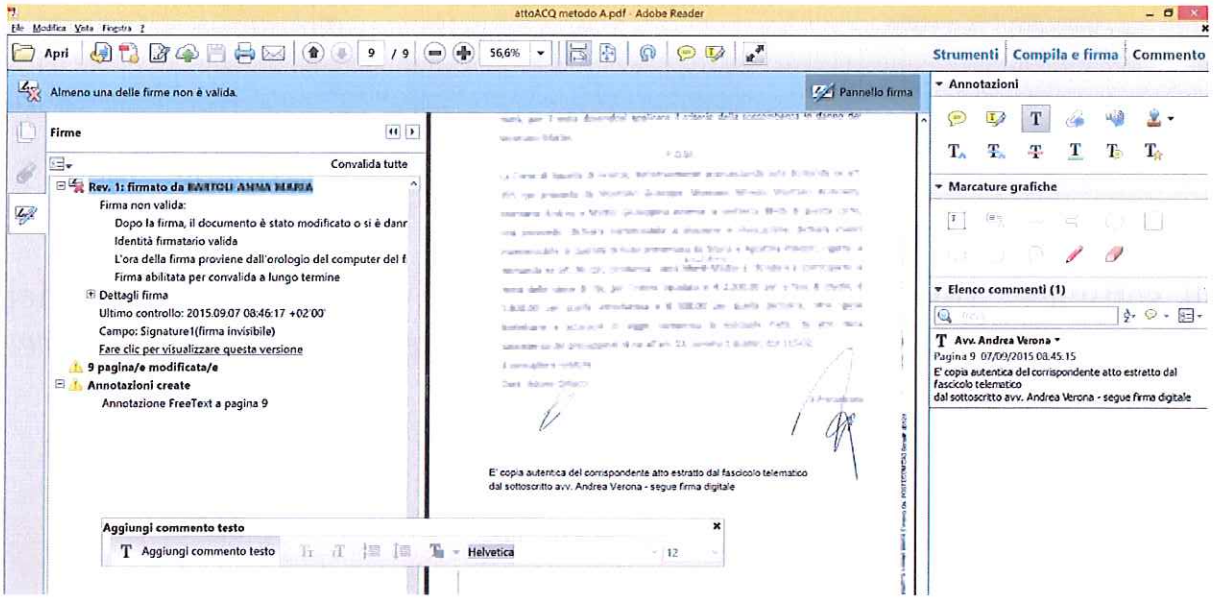
Cliccare OK, le icone diventano selezionabili, quindi cliccare su T:



Posizionare il cursore in calce al testo e digitare la formula voluta:

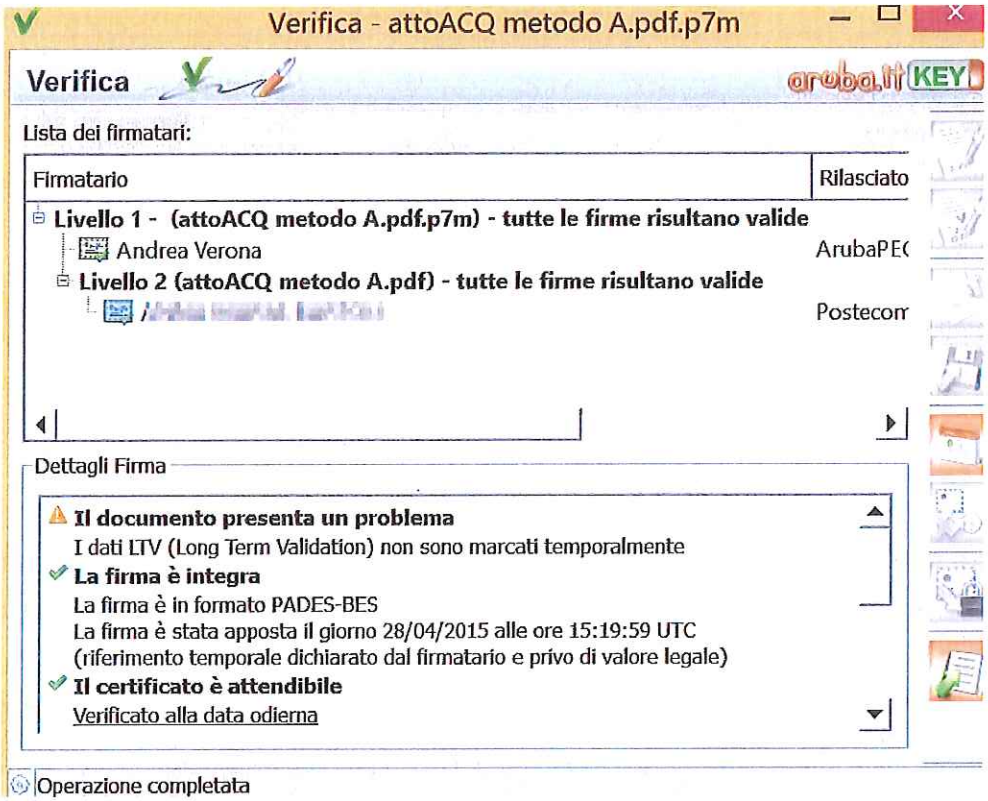


Questo sarà il risultato: nel "pannello firme" compare, oltre all'avviso delle firme non valide, l'avviso delle annotazioni create, leggibili anche nell' "Elenco Commenti"



Salvate col nome che volete il "pdf" così modificato e firmatelo digitalmente con il metodo abituale (CAdES).

La verifica di tale file avente estensione *.pdf.p7m con il software Arubasign dà il seguente risultato:



Il software "Dike pdf" sembra non "vedere" la firma "PAdES" del cancelliere, ma solo la (valida) firma CAdES apposta dall'autenticatore:



La consultazione grafica del risultato non è particolarmente semplice, perché la sottoscrizione digitale è contenuta nella "busta" che contiene il documento, mentre il "pdf" contiene la sola annotazione grafica.

METODO B

Firma PAdES

Inserimento di firma "digitale e grafica" in formato PADES all'interno del "pdf" contenente la formula di autentica (come "motivo" della firma stessa).

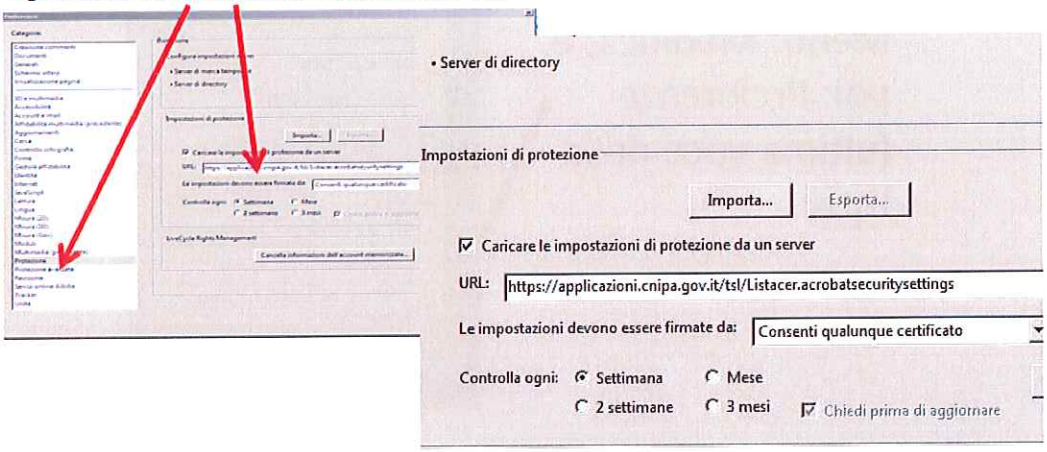
Con questo metodo il documento originale NON viene alterato, benchè la formula e la firma compaiano sia in forma grafica, in calce al documento, sia in formato digitale, verificabile sia nella lettura del "pdf" sul monitor, sia con software di verifica esterni.

Nella pratica quotidiana tale metodo risulta assai più semplice ed "automatico": lo svantaggio sta nel fatto che richiede una configurazione iniziale – una tantum - **alquanto complessa** del software Adobe Reader XI.

La premessa **indispensabile** è la configurazione suggerita da AGID in QUESTA PAGINA per la **verifica** delle firme digitali. Nel menu Modifica/Preferenze, scegli quindi la categoria "Protezione" ed inserisci:

Configurazione di Adobe Reader XI

Sempre in «preferenze» seleziona «protezione» e poi configura come nell'immagine (v. http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche/firma-pdf)



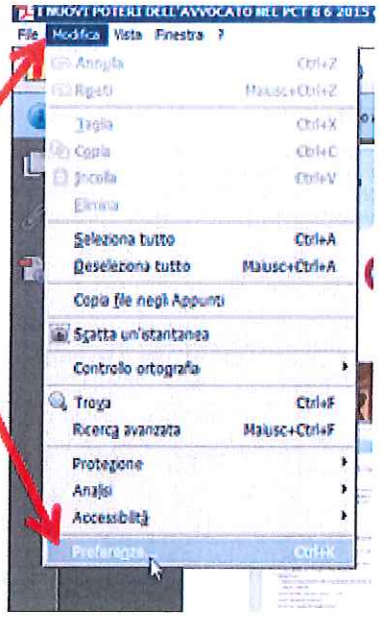
Perché Adobe Reader 11 utilizzi correttamente il certificato ed il modulo di firma digitale dell'avvocato che effettua la autenticazione occorre tuttavia procedere manualmente alla installazione e

configurazione anche del modulo PKCS#11, in modo che Adobe Reader venga forzato ad impiegare l' algoritmo di firma "SHA 256" anziché l'algoritmo "SHA 1", come già illustrato nell'articolo "Abilitazione della firma digitale in Acrobat Reader e Acrobat Pro" del collega Avv. Fabio Salomone del Foro di Matera che potete consultare e scaricare su QUESTA PAGINA DI AVVOCATI TELEMATICI.

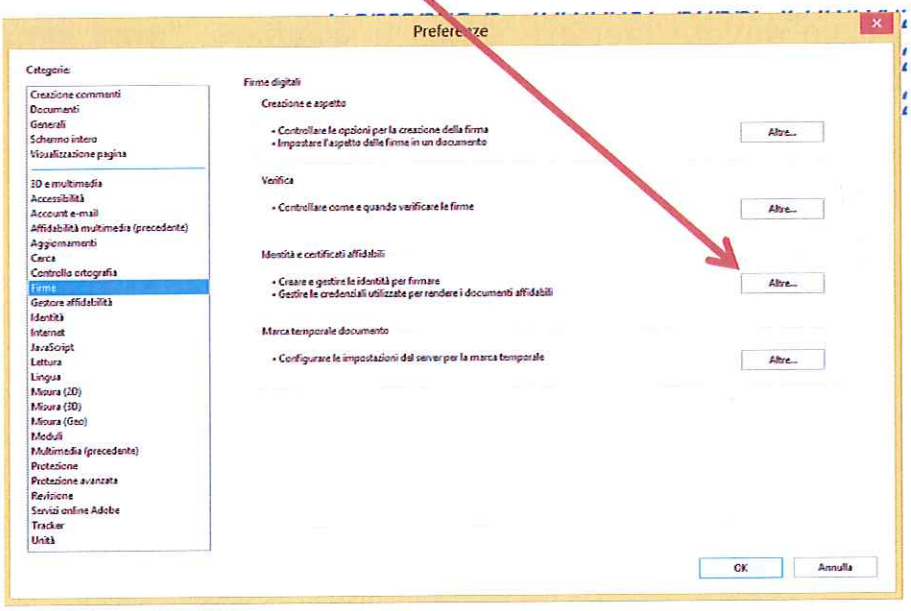
E' quindi necessario configurare la firma PAdES come "firma digitale" valida a tutti gli effetti anche se, limitatamente alla firma dell'attestazione di autenticità della copia informatica, le regole tecniche del CAD (art. 71) all' art 6 c.3 I parte del DPCM 13.11.14 prevedono che il documento nel quale è stata inserita l'attestazione di autenticità *"è sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato"* .

Configurazione di Adobe Reader XI

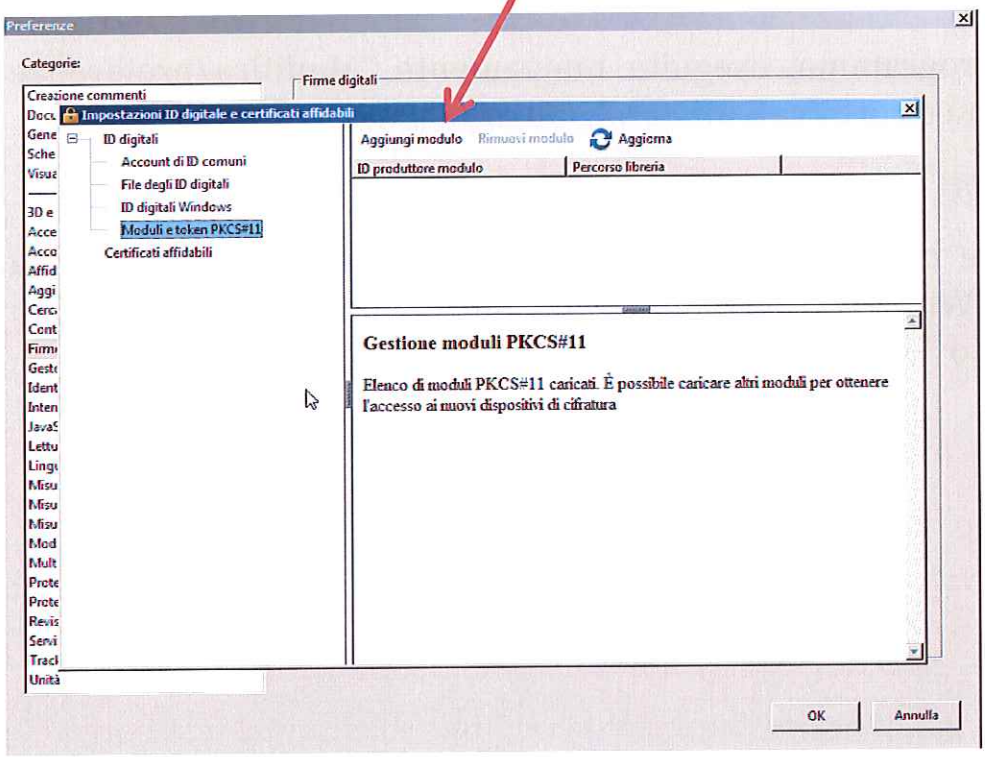
- Selezionare nel Menu: Modifica, e poi: Preferenze (ultima voce della lista)



Apriamo la categoria “Firme” e scegliamo la sezione “identità e certificati affidabili”, clicchiamo su “altre”…

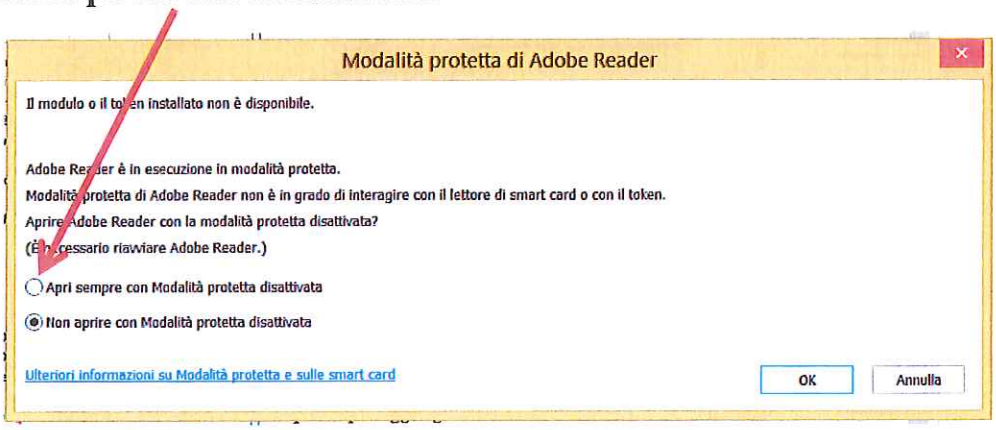


Si apre questa finestra: selezioniamo “Moduli e token PKCS#11”, poi clicchiamo su “Aggiungi modulo”



Normalmente il programma, se è in "modalità protetta", non vi consentirà l'apertura di tale comando.

In questo caso dovete mettere il flag e scegliere: "**apri sempre con modalità protetta disattivata**"

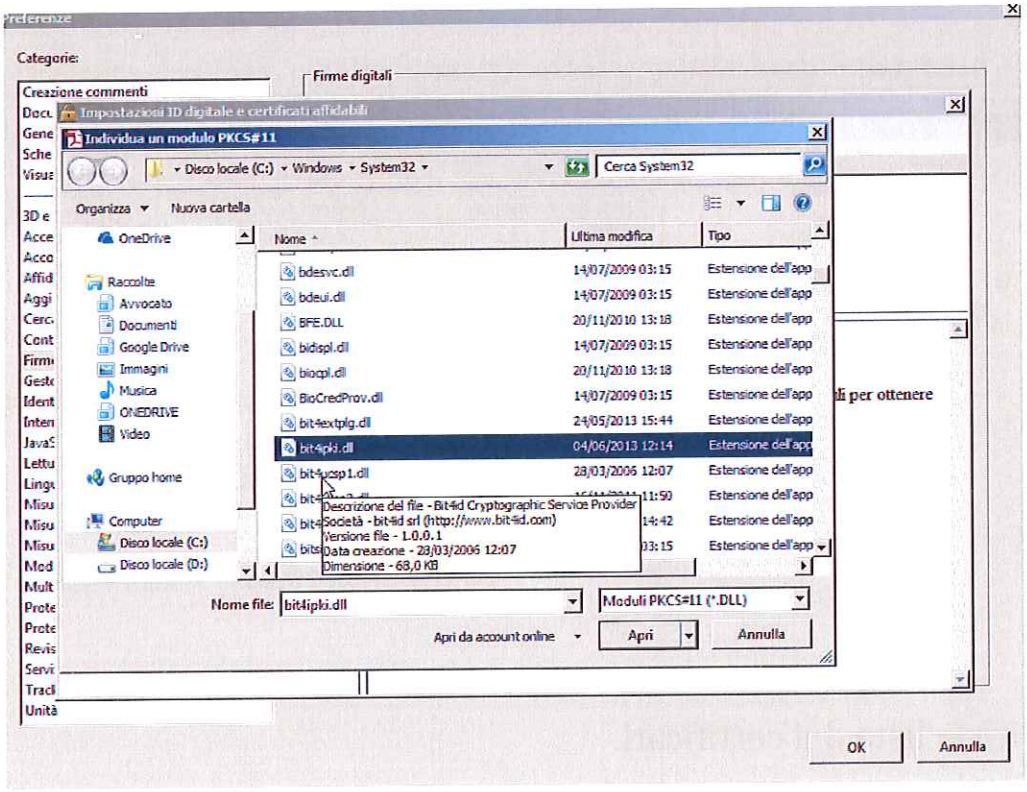


Cliccate su OK: a questo punto **dovete chiudere e riaprire il programma per consentire la disattivazione della modalità protetta.**

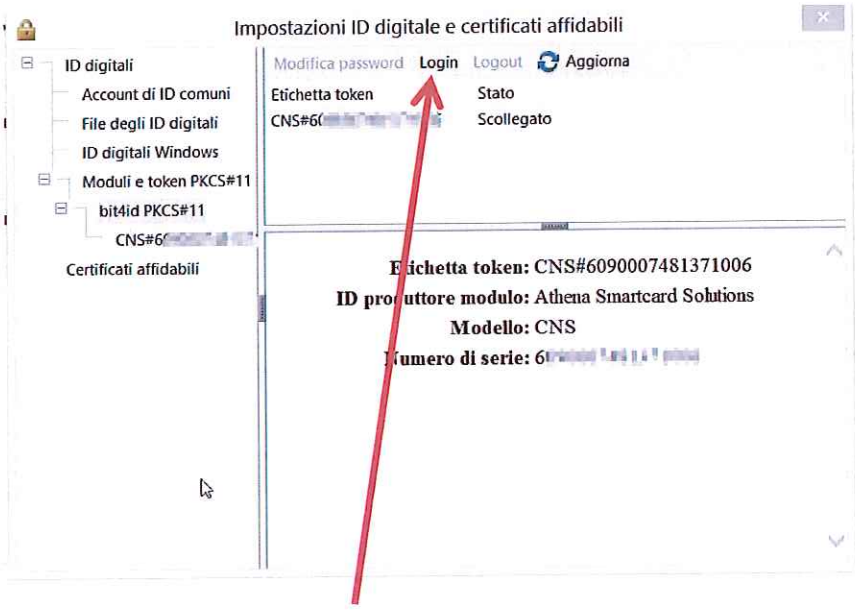
Riaperto il programma, eseguite nuovamente "Modifica/preferenze /firme/identità e certificati affidabili/altre /aggiungi modulo".

Cliccate su "apri": si aprirà la finestra di ricerca.

Adesso potete cercare il modulo che normalmente si troverà nella cartella "C:/Windows/System32" e normalmente si chiamerà: "bit4ipki.dll" (o "bit4opki.dll")

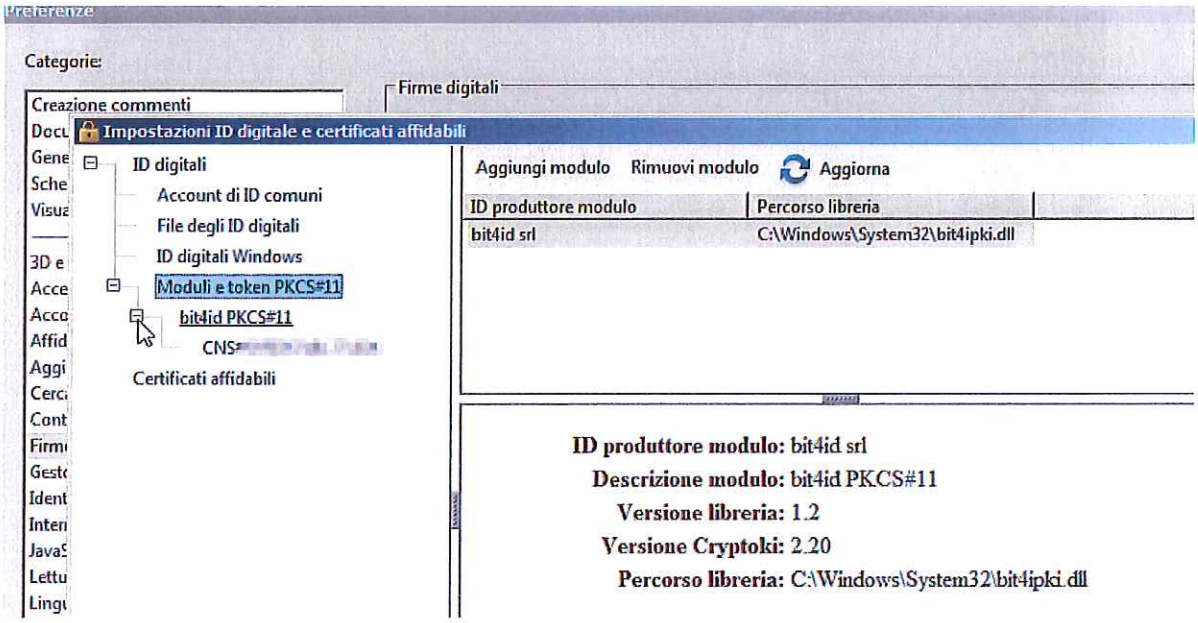


Se avete inserito il vostro dispositivo di firma, comparirà la seguente finestra:



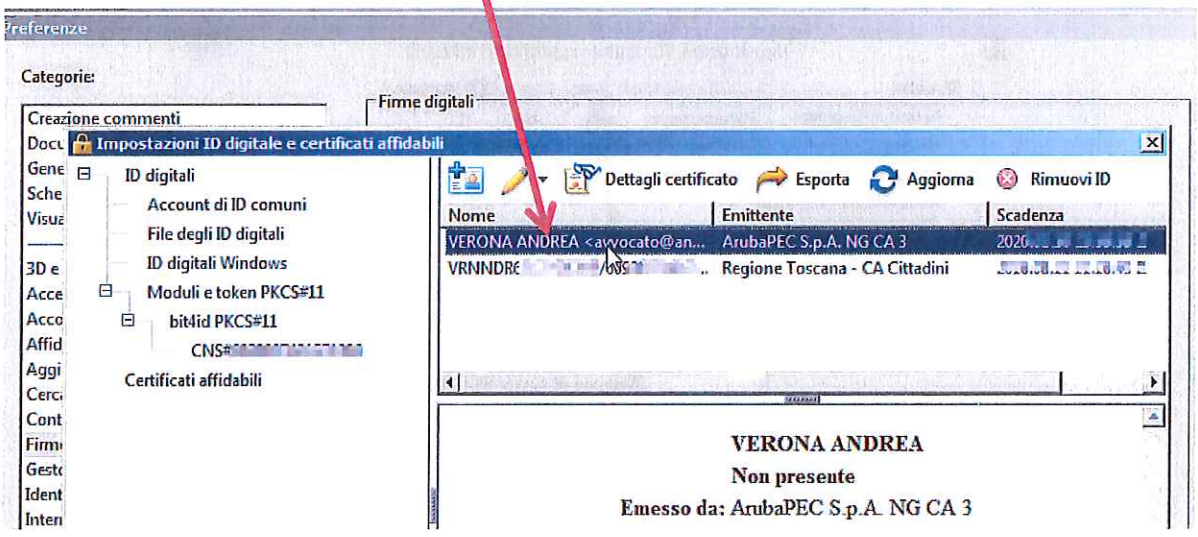
E' necessario effettuare il **login**, cliccando sulla relativa voce, ed inserire il PIN nella maschera che si apre.

Al termine la CNS sarà visibile: cliccando su di essa …

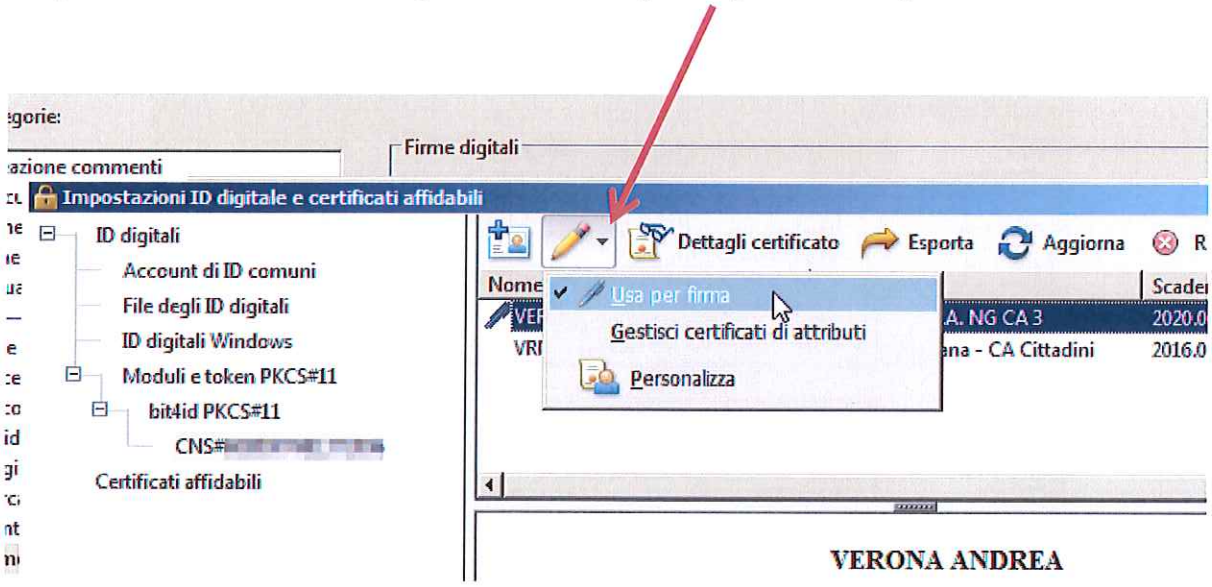


si aprirà la lista dei certificati.

Selezionate quello col COGNOME NOME (non quello col codice fiscale!):

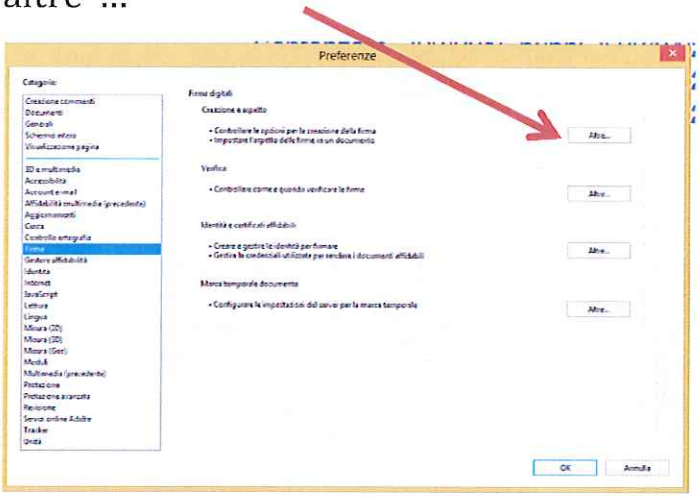


e quindi cliccate sull'icona a forma di matita, che consente di impostarla come firma "predefinita" ("usa per firma"):

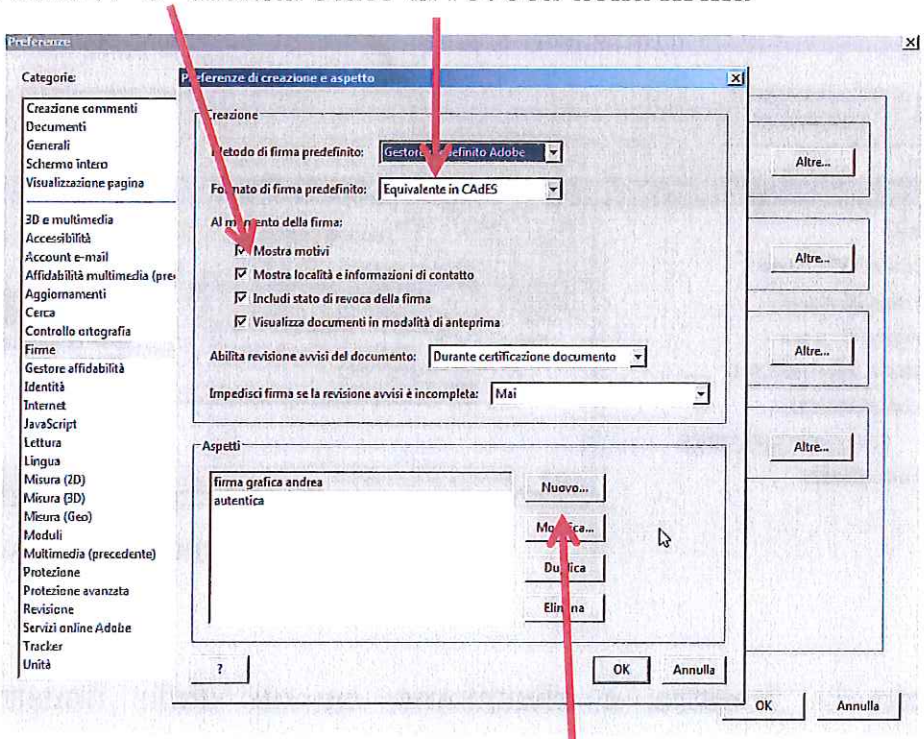


Chiudiamo la finestra e clicchiamo su ok della finestra delle preferenze.

Torniamo su "Firme", scegliamo la sezione "Creazione ed aspetto" e clicchiamo su "altre"...

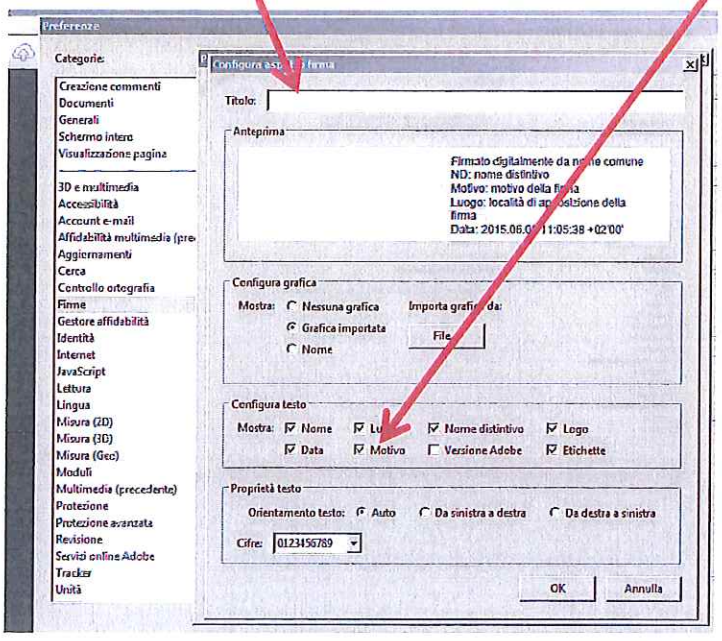


Nella finestra successiva selezionate come "formato di firma predefinito" la casella: "Equivalente in CAdES" (come suggerito anche da AGID) e mettete la spunta sulle opzioni sottostanti, in particolare su "Mostra motivi" e "Includi stato di revoca della firma"



Quindi cliccate su "Nuovo..."

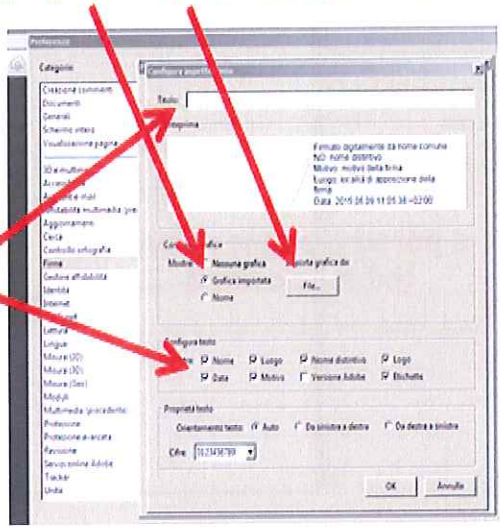
Si aprirà questa finestra, ove mettere senz'altro il flag su "motivo", ed il titolo della nuova firma



Configurazione di Adobe Reader XI

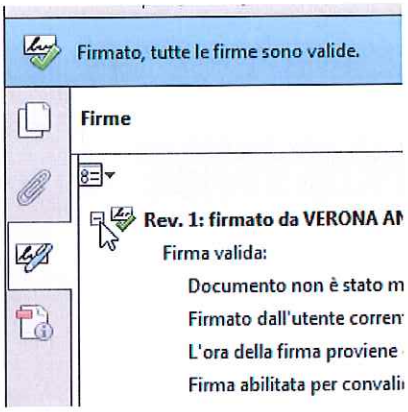
Se vuoi personalizzare la tua firma seleziona «Grafica importata» e scegli il file pdf che contiene la «firma grafica» da visualizzare

Scegli i dati che vuoi visualizzare in «configura testo». DEVE ESSERCI almeno IL «MOTIVO» il «NOME» e la «DATA» Ed infine salva la configurazione mettendo il suo «titolo»



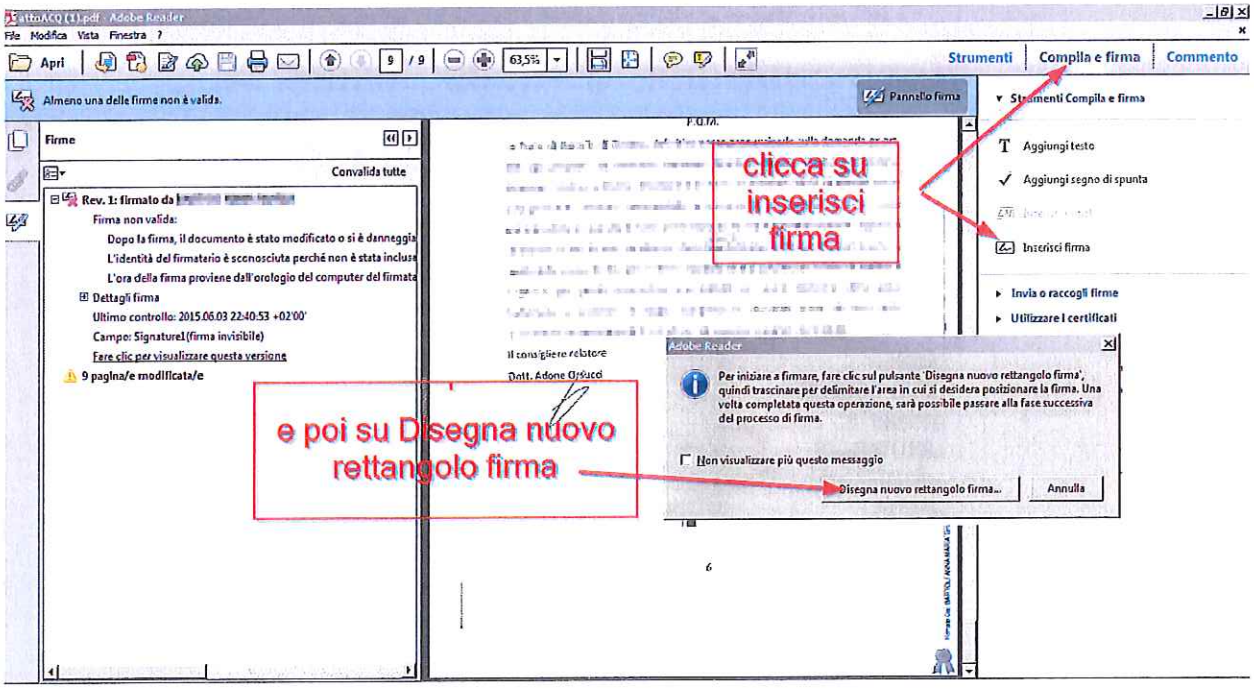
Siamo finalmente pronti ad **inserire la firma con la attestazione di autenticità in calce alla copia informatica:**

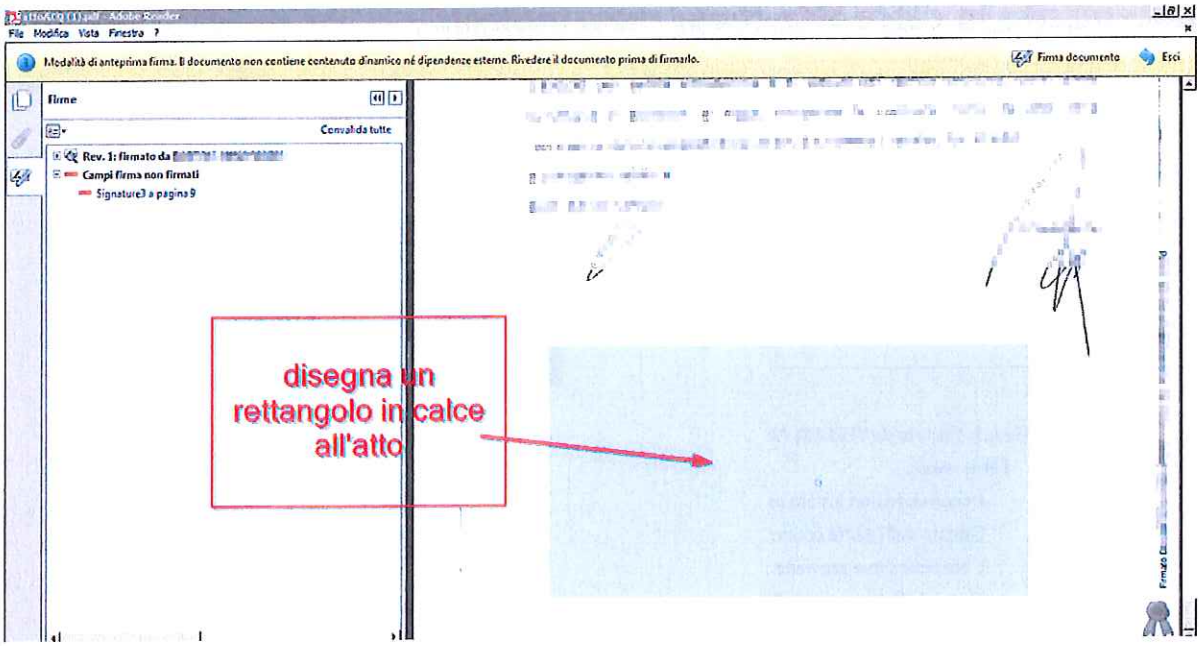
Ricordiamoci di attivare in alto a destra il pannello firma, che comparirà quindi alla nostra sinistra:



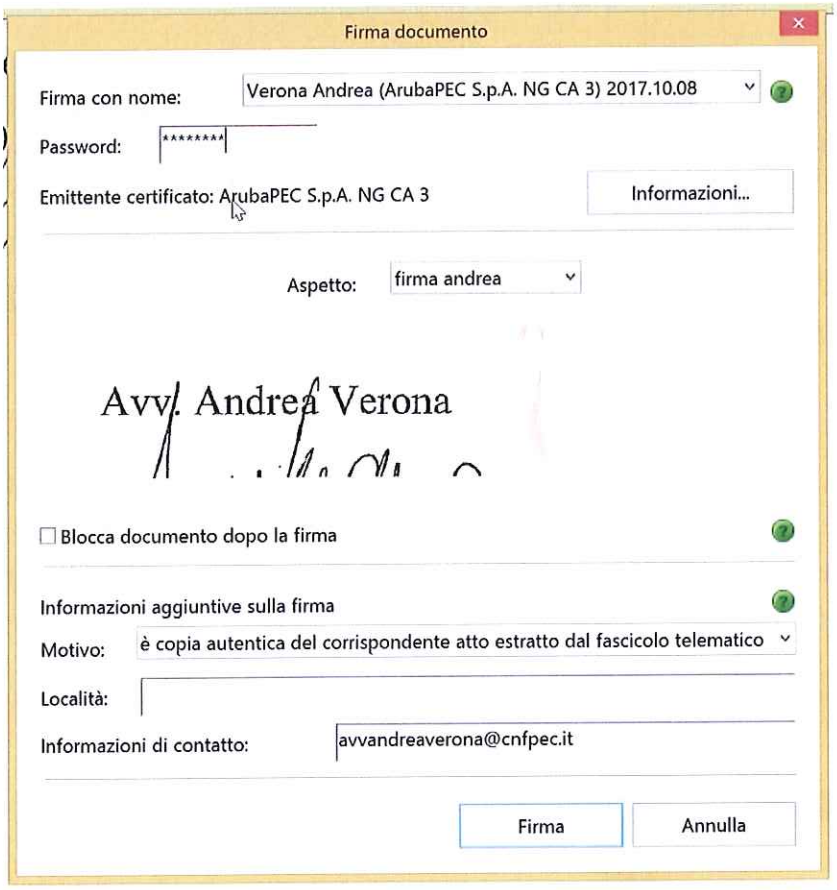


Quindi come nell'immagine, cliccare su Compila e Firma, Inserisci Firma e poi su Disegna nuovo rettangolo firma:

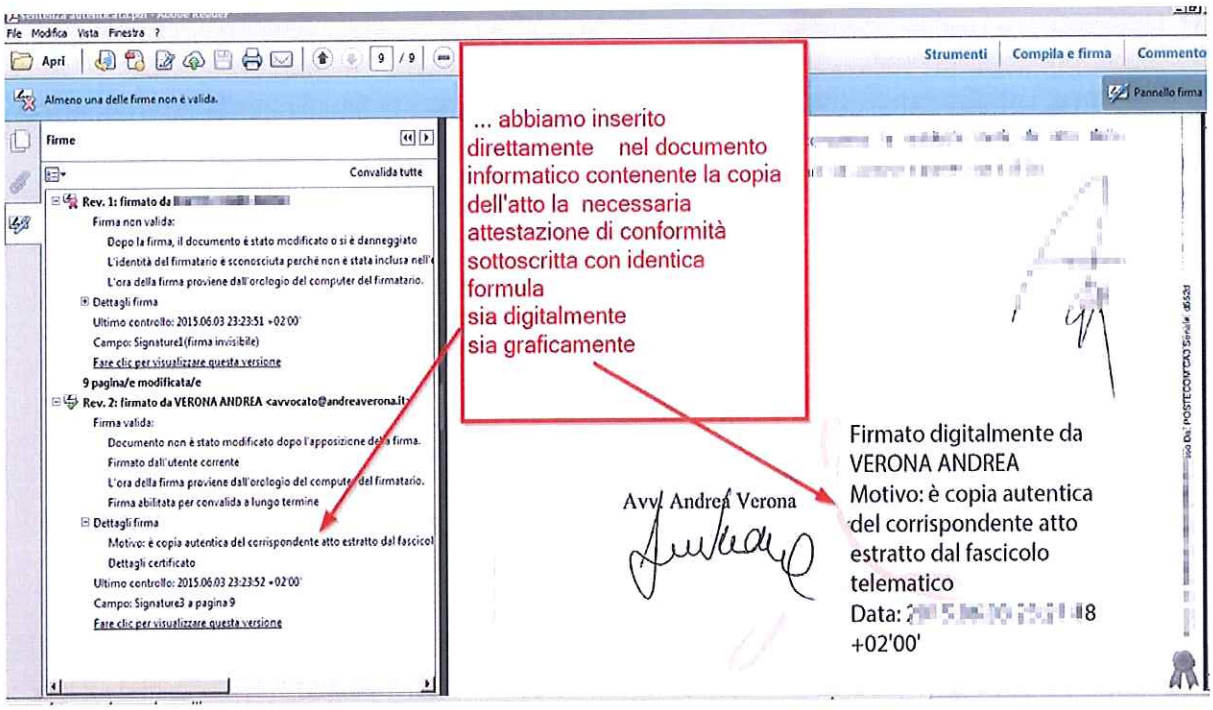




Si apre la finestra nella quale il programma proporrà il corretto certificato di firma prescelto in sede di configurazione: dobbiamo quindi inserire il PIN ed il motivo, nel cui campo scriviamo: "è copia autentica del corrispondente atto estratto dal fascicolo telematico"

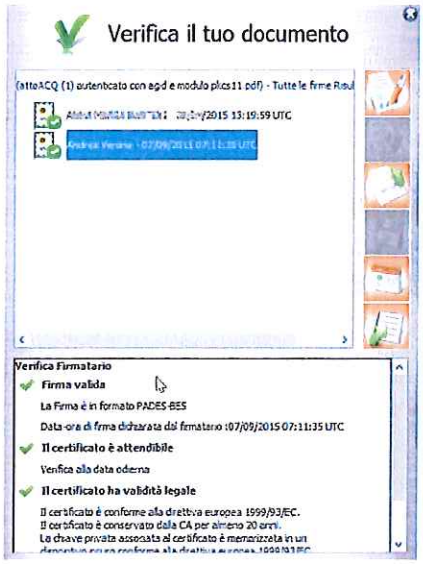


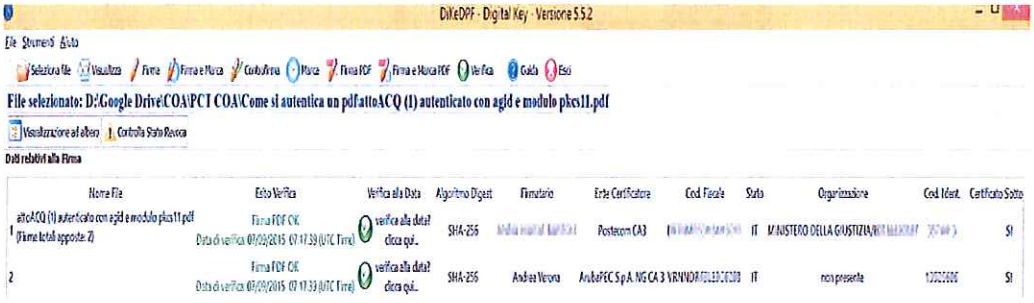
La dizione resterà memorizzata e disponibile ad essere selezionata con un clic in altre future operazione. Risultato:



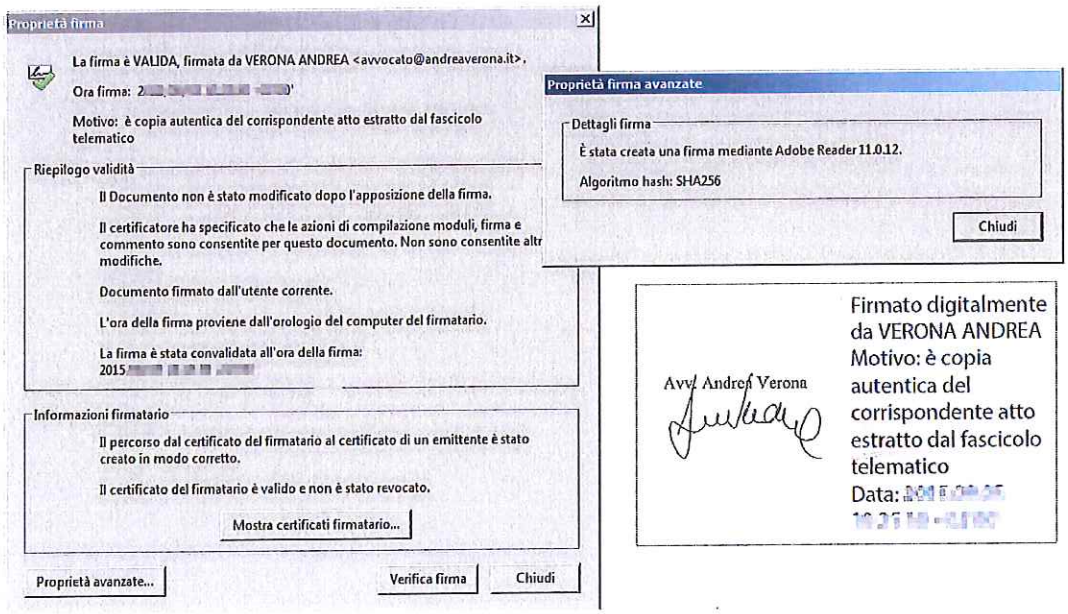
In questo modo nel documento digitale finale sono nidificati, senza reali alterazioni: l'atto originale, la firma in formato PAdES del cancelliere, i dati della "segnatura di protocollo", la firma e la formula di autentica dell'avvocato autenticante, simboleggiata graficamente dalla nostra firma, motivazione e, volendo, dal nostro logo: tutte le aggiunte sono registrate e direttamente verificabili a video.

La verifica, effettuata con i due diversi software utilizzati per la verifica del metodo A, non solo fornisce risultati univocamente positivi ma informa della valida presenza di tutte le firme PAdES presenti nel documento:





Anche la verifica attraverso il pannello "proprietà firma" di Adobe Reader conferma che la firma è stata creata con l'algoritmo "SHA-256":



Per l'autentica della "copia informatica" per immagine dell'atto o provvedimento che detenete in originale o copia autentica (p.e.s titolo esecutivo, precetto e verbale di pignoramento) inserite ovviamente una formula diversa, per es. "Attesto che il presente atto è conforme all'originale in mio possesso": anche questa formula resterà memorizzata e disponibile al successivo utilizzo di Adobe Reader.

Segnalo che il metodo B qui descritto è utile anche per la contestuale sottoscrizione "digitale e grafica" di altri documenti anche stragiudiziali quali lettere, contratti ecc. (naturalmente senza usare come "motivo" la formula di autentica), così sottoscrivibili anche "in sequenza" e da più soggetti (firme multiple) in modo che la restituzione grafica ed a video del documento riflette immediatamente e fedelmente il contenuto della sottoscrizione digitale, senza necessità di software di verifica.