L'apposizione di firme e informazioni su documenti firmati

Il presente documento si pone l'obiettivo di chiarire alcuni aspetti generali dei formati di firma CAdES (file con estensione *p7m*) e PAdES (file con estensione *pdf*) e la loro attitudine ad ospitare più firme e informazioni disponibili solo dopo la generazione della firma digitale quali, ad esempio, la segnatura di protocollo prevista dall'articolo 55 del D.P.R. 28 dicembre 2000, n. 445.
Come noto, un documento sottoscritto con firma digitale ha nel nostro ordinamento piena efficacia giuridica, a condizione che non sia modificato dopo l'apposizione della firma.
Con la diffusione dell'uso dei documenti informatici, sono sempre più numerose le richieste di chiarimento sul corretto utilizzo della firma digitale, con particolare riferimento ai casi in cui sia necessario apporre più firme su un medesimo documento o in cui si intenda aggiungere dei dati dopo la sottoscrizione, ad esempio, allo scopo di riportare gli estremi della segnatura di protocollo di un documento spedito o ricevuto da una pubblica amministrazione.
A tal fine, appare utile richiamare alcune nozioni sulle firme digitali.
Senza entrare in dettagli tecnici, la firma digitale consiste nella creazione di un file, definito "busta crittografica", che racchiude al suo interno il documento originale, l'evidenza informatica della firma e la chiave per la verifica della stessa, che, a sua volta, è contenuta nel certificato emesso a nome del sottoscrittore, come mostrato in figura 1. L'autenticità del certificato è garantita da un'Autorità di certificazione, in Italia, dai certificatori accreditati ai sensi dell'articolo 29 del CAD (D.Lgs. n. 82/2005).

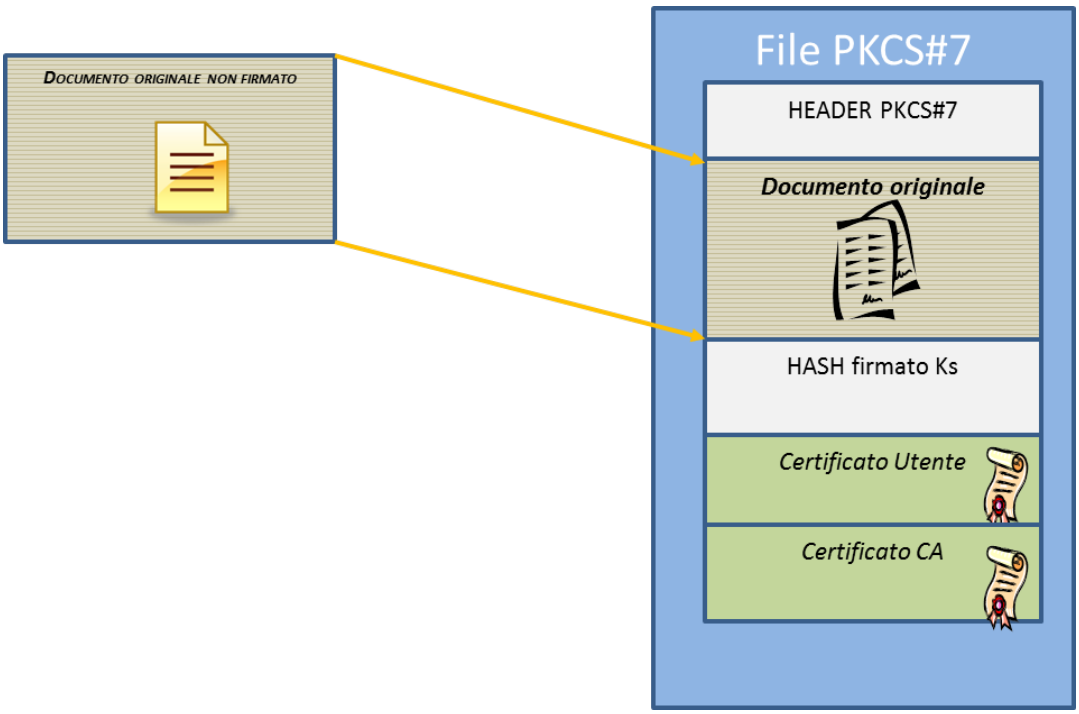

Figura 1 - Firma

Gli standard europei[1] prevedono tre tipi di sottoscrizione digitale, identificati dagli acronimi CAdES, PAdES e XAdES, modalità di sottoscrizione adottate anche in Italia. Ai fini del presente documento si tratteranno solo i primi due tipi.

La firma CAdES

La busta CAdES è un file con estensione *.p7m*, il cui contenuto è visualizzabile solo attraverso idonei software in grado di "sbustare" il documento sottoscritto. Tale formato permette di firmare qualsiasi tipo di file, ma presenta lo svantaggio di non consentire di visualizzare il documento oggetto della sottoscrizione in modo agevole. Infatti, è necessario utilizzare un'applicazione specifica.

Per il formato CAdES l'apposizione di due o più firme può essere effettuata in due modi:

- re-imbustando in una nuova busta CAdES la busta generata dalla sottoscrizione precedente (c.d. controfirma o "firma matrioska"), come mostrato in figura 2;
- oppure aggiungendo nella busta ulteriori firme, accompagnate dai relativi certificati (c.d. firme congiunte), come mostrato in figura 3.

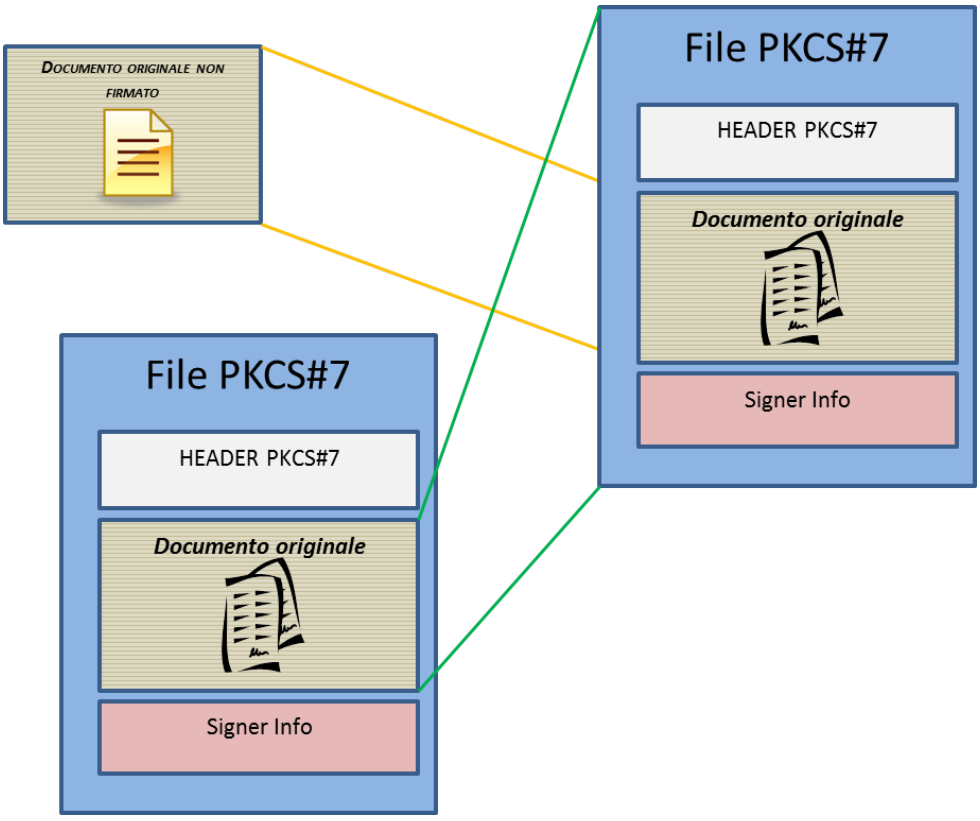

Figura 2 – Firma a matriosca – ogni firma afferisce al documento e alle firme precedenti formato CAdES

[1] Decisione della Commissione europea 2011/130/EU.

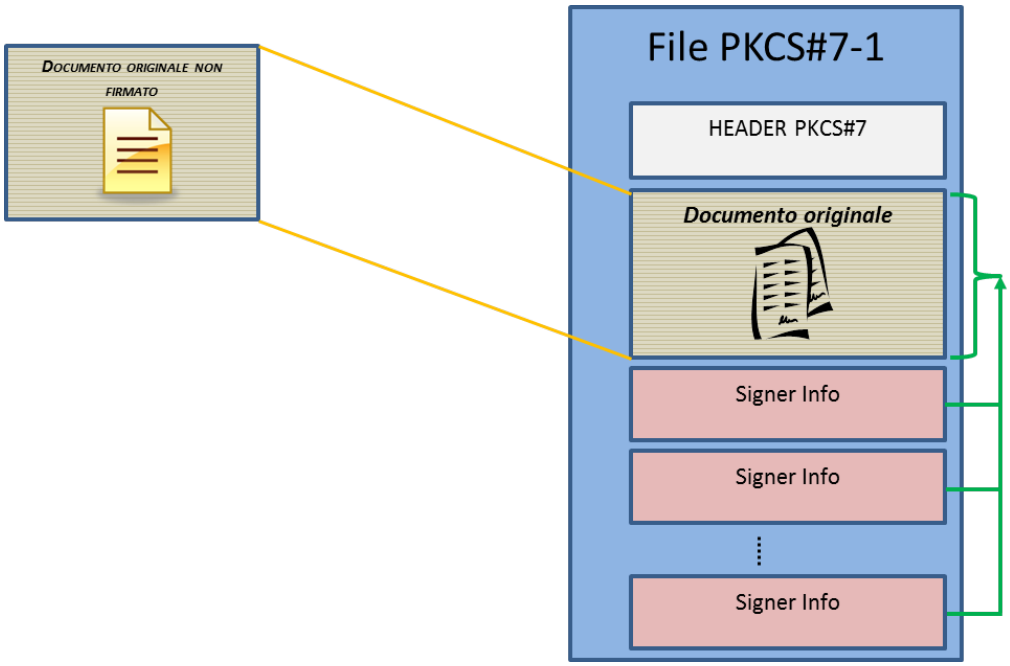

Figura 3 - Firme congiunte CAdES – ogni firma afferisce al documento

In entrambi i casi è presente un'unica versione del documento, che pertanto può solo essere oggetto di ulteriori firme digitali senza modificarne il contenuto.

Nel caso di documenti sottoscritti in formato CAdES, come si è detto, non è possibile gestire diverse versioni di uno stesso documento all'interno della busta crittografica, pertanto, nell'ipotesi in cui si voglia riportare sul documento delle annotazioni successive alla sottoscrizione (ad esempio i dati della segnatura di protocollo), sarà necessario esportare il documento nel formato originario, ossia non firmato, per apportarvi le annotazioni. Tali modifiche, infatti, sarebbero apportate nell'unica versione del documento presente all'interno della busta CAdES, operazione questa che renderebbe le firme invalide.

E' evidente il limite di questa tipologia di firma. Nell'esempio fatto, si avrebbero due documenti: uno con la firma digitale del sottoscrittore del documento, l'altro con la segnatura di protocollo ma privo della firma digitale del sottoscrittore.

La firma PAdES

La firma digitale in formato PAdES è un file con estensione *.pdf*, leggibile con i comuni *reader* disponibili per questo formato.

Questa tipologia di firma, nota come "firma PDF", prevede diverse modalità per l'apposizione della firma, a seconda che il documento sia stato predisposto o meno ad accogliere le firme previste ed eventuali ulteriori informazioni, rende il documento più facilmente accessibile, ma consente di firmare solo documenti di tipo PDF.
Il formato PDF consente inoltre di gestire diverse versioni dello stesso documento senza invalidare le firme digitale apposte.

Predisposizione del documento PDF

Il documento può essere predisposto, attraverso la funzione "moduli", alla firma digitale da parte di utenti che dispongono di un prodotto conforme allo standard PDF (ISO 32000), fra questi Acrobat Reader.
A tale scopo sarà necessario trasformare il documento in formato PDF (filmato 1) e, successivamente, predisporre i campi firma (filmato 2).


Filmato 1


Filmato 2

Il documento può anche essere predisposto per contenere dei campi testo ove è possibile inserire delle informazioni successivamente alla firma senza invalidare la stessa (filmato 3).


Filmato 3

Altra interessante caratteristica è che il documento in formato PDF consente di collocare fisicamente la firma digitale in un preciso punto del documento. Tale caratteristica è particolarmente utile nel caso di sottoscrizione di clausole vessatorie o, comunque, in ogni caso in cui la collocazione della firma abbia una qualche valenza.

Molteplici firme nel documento PDF

Qualora il documento non fosse stato predisposto per tutte le firme necessarie, è comunque possibile apporre ulteriori firme senza invalidare le precedenti.
A tale scopo, il formato PAdES implementa la funzione della gestione delle versioni (*versioning*): ogni versione successiva alla prima, contiene la versione integrale, non modificata, del documento precedente (comprese le firme digitali).
Ogni modifica al documento (ulteriore firma o aggiunta di testo o immagini) produce, infatti, una nuova versione che contiene la versione originale non modificata (figura 4).

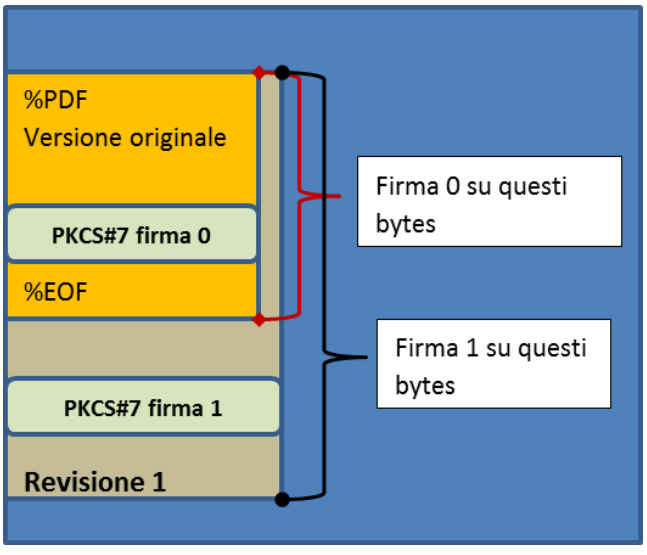

Figura 4 - busta formato PAdES – firme di versioni del documento firmato

Tale caratteristica della busta PAdES rende questo formato particolarmente idoneo anche nel caso in cui si renda necessario apportare delle modifiche al documento dopo averlo sottoscritto, ad esempio per riportarvi delle annotazioni, come i dati degli estremi di protocollo che sono disponibili solo successivamente alla sottoscrizione del documento stesso.
Ad una prima analisi, un documento sottoscritto sul quale sono riportate tali annotazioni potrebbe apparire corrotto in quanto modificato dopo la firma (figura 5), tuttavia nella busta PAdES è presente ed è accessibile anche la versione non modificata del documento (figura 6), che pertanto conserva piena efficacia giuridica. Non devono, infatti trarre in inganno i messaggi mostrati dal *reader* del documento "*Almeno una delle firme non è valida*" e "*Il documento dopo la firma è stato modificato o si è danneggiato*", in quanto è comunque possibile accedere alla versione del documento correttamente sottoscritta, coerentemente con quanto previsto dalle regole tecniche di cui al D.P.C.M. del 22 febbraio 2013[2].

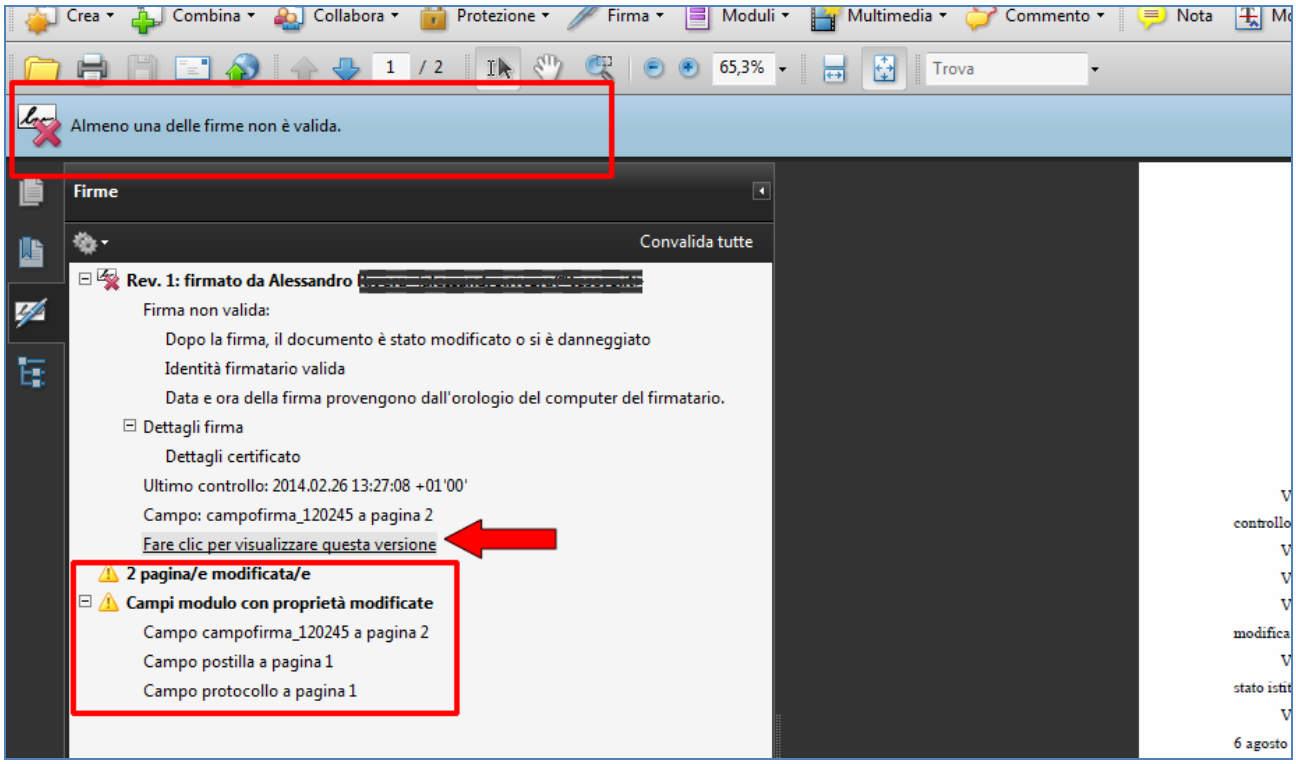

Figura 5 – accesso alla versione non modificata del documento firmato – formato PAdES

[2] Il D.P.C.M. del 22 febbraio 2013 "*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71.*", all'art. 14 comma, 2 lett. f) in materia di "*Verifica delle firme elettroniche qualificate e digitali*", dispone che Il sistema di verifica delle firme elettroniche qualificate e digitali deve quantomeno "*evidenziare l'eventuale modifica del documento informatico dopo la sottoscrizione dello stesso*", e al precedente articolo 4, comma 3 detta che: "*Il documento informatico, sottoscritto con firma elettronica qualificata o firma digitale, non soddisfa il requisito di immodificabilità del documento previsto dall'art. 21, comma 2, del Codice, se contiene macroistruzioni, codici eseguibili o altri elementi, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.*"

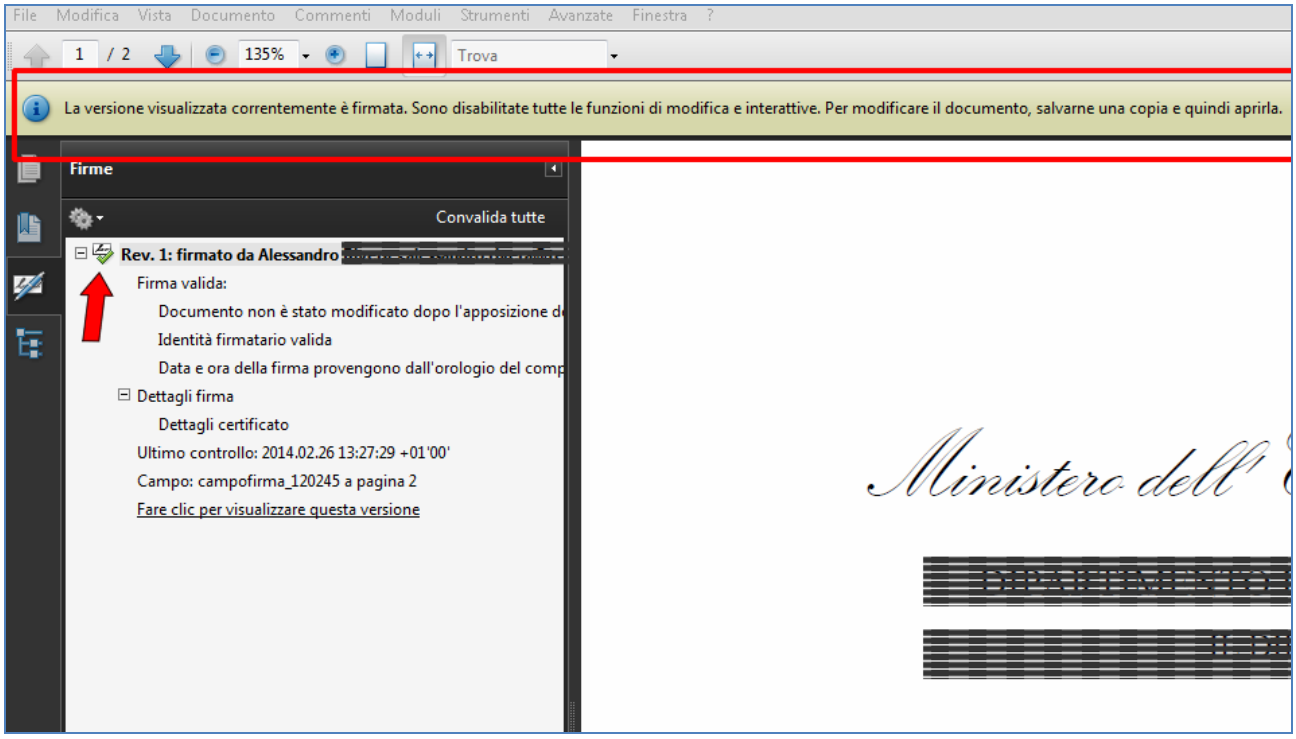

Figura 6 – busta formato PAdES- versione non modificata del documento sottoscritto digitalmente

Questa modalità di gestire le versioni del documento PDF, consente di risolvere il problema della segnatura di protocollo.
Altra possibile soluzione potrebbe essere la realizzazione di un documento pdf contenente gli estremi della segnatura di protocollo cui allegare il documento protocollato nella sua versione originale (figura 7).

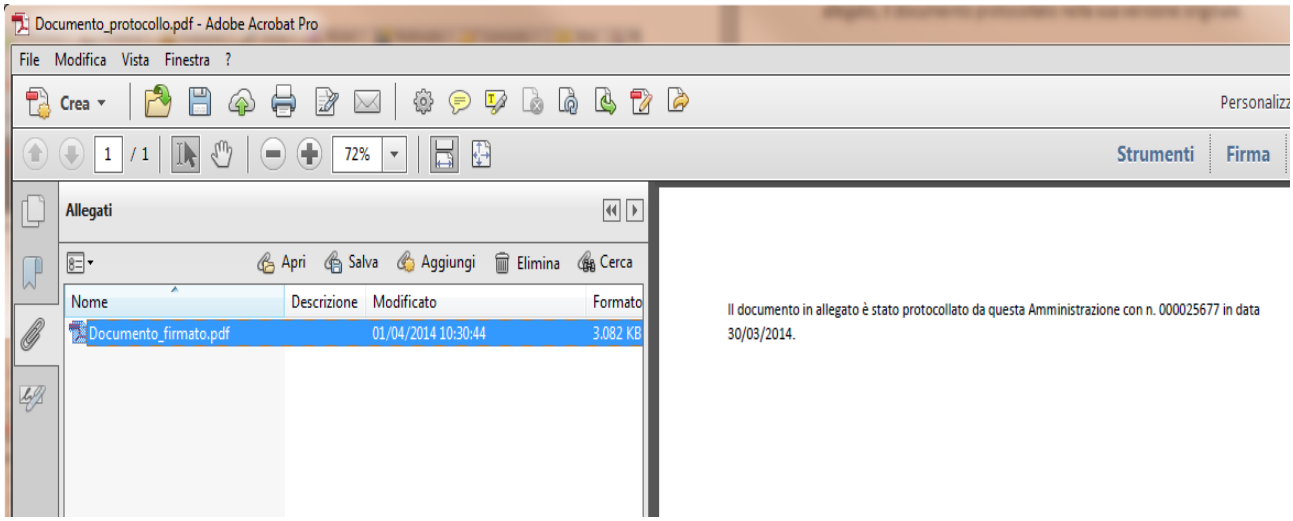

Figura 7 – Documento contenente la segnatura di protocollo associata all'allegato

Con un semplice "doppio click" sull'allegato si apre il documento trasmesso verificandone la firma (figura 8).

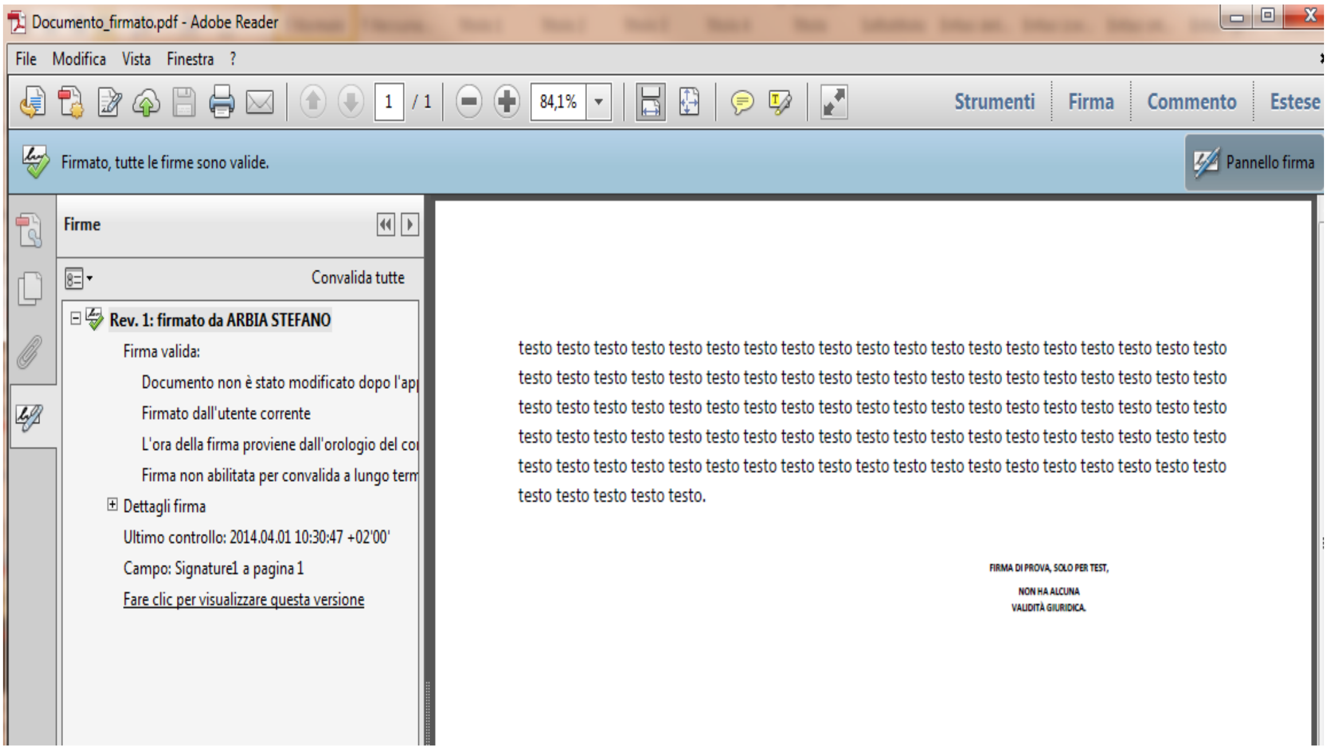

Figura 8 – Documento allegato nella versione originale

Note di chiusura

In conclusione, operazioni su un documento pdf già firmato quali allegare il documento pdf in altro documento pdf, l'apposizione di una ulteriore firma digitale al documento, l'aggiunta di un campo testo o immagine al documento, non invalidano la firma digitale in quanto la stessa è comunque verificabile con successo.