DOMANDE E RISPOSTE NORMATIVA

L'entrata in vigore della nuova normativa DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 22 febbraio 2013 Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, si rilevano epocali per la loro portata ed influenza nel sistema paese per la semplificazione di imprese. Di seguito alcune delle principali domande e risposte in materia, con i relativi link alla normativa:

In pratica che differenza c'è tra le tre firme Qualificata, Avanzata, Digitale?

Nessuna, tutte e tre hanno la stessa valenza giuridica e pratica e lo stesso formato

> **Art. 61. Soluzioni di firma elettronica avanzata: 3.** I formati della firma di cui al comma 2 sono gli stessi previsti ai sensi dell'art. 4, comma 2.

Chi sono, in base alla nuova normativa, coloro che possono erogare Certificati di Firma Elettronica Avanzata FEA?

Tutti coloro che commercializzano Certificati di Firma Elettronica Avanzata in Europa (Art.1/6)

> 6. Ai prodotti sviluppati o commercializzati in uno degli Stati membri dell'Unione europea e dello spazio economico europeo in conformità alle norme nazionali di recepimento della direttiva 1999/93/CE del Parlamento europeo e del Consiglio, pubblicata nella Gazzetta Ufficiale dell'Unione europea, Serie L, n. 13 del 19 gennaio 2000, è consentito di circolare liberamente nel mercato interno.
>
> **Art. 55.**
>
> 1. La realizzazione di soluzioni di firma elettronica avanzata è libera e non è soggetta ad alcuna autorizzazione preventiva.

E' sufficiente compilare un modulo on-line per identificarmi con il certificatore o debbo recarmi nel suo ufficio?

Il modulo on-line è equiparato all'auto dichiarazione, da tempo operativa in Italia, le norme in vigore sono sotto elencate:

> Nel rapporto tra privati il riconoscimento della validità dell'autocertificazione resta a discrezione del privato che richiede il certificato o documento/auto-dichiarazione, ai sensi della Legge 24 novembre 2000, n. 340 nonché D.P.R. n. 445/2000 in particolare l'art. 2,76 "Le norme concernenti i documenti informatici e la firma digitale, contenute nel capo II, si applicano anche nei rapporti tra privati come previsto dall'articolo 15, comma 2 della legge 15 marzo 1997, n. 59.e successivi provvedimenti e modificazioni,

A quali rischi mi sottopongo se non dichiaro il vero nella compilazione del modulo on-line?

La dichiarazione on-line equivale all'autodichiarazione prestata davanti ad una autorità, inoltre, il codice penale Italiano prevede ben più rigide sanzioni all'art.495-bis e 640-quinquies . Ovviamente tutti gli atti firmati con FEA potrebbero essere privi di valore oltre ad altre sanzioni.

«Art. 495-bis. - (Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri). - Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione fino ad un anno».

Che valore ha la firma digitale avanzata su un documento?

Lo stesso valore di una firma autografa, la normativa è piuttosto vecchia, ma ancora in vigore e più volte ribadita derivante dall'art. 15/2 Legge 15 marzo 1997, n. 59

2. Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge.

Oltre alla firma autografa cosa garantisce la FEA?

Sempre più documenti, atti ed anche contratti, possono essere firmati digitalmente. La firma deve essere riconosciuta e gli atti derivanti dalla stessa sono altrettanto riconosciuti come firmati davanti ad un notaio o ad un pubblico ufficiale.

Quali sono i documenti che posso firmare con la Firma Elettronica Avanzata FEA?

Qualsiasi tipo di documento, le funzioni di firma digitale oltre al classico PDF, sono erogate anche da tutta la suite dei prodotti Office della Microsoft.

Come inviare un documento firmato digitalmente?

Il naturale modo di trasmissione di un documento firmato digitalmente è la posta elettronica, alla quale il documento stesso può essere allegato, anche la stessa posta elettronica può essere considerata un documento, che a sua volta può essere firmato con la FEA

In quali paesi del mondo è valida la Firma Elettronica Avanzata?

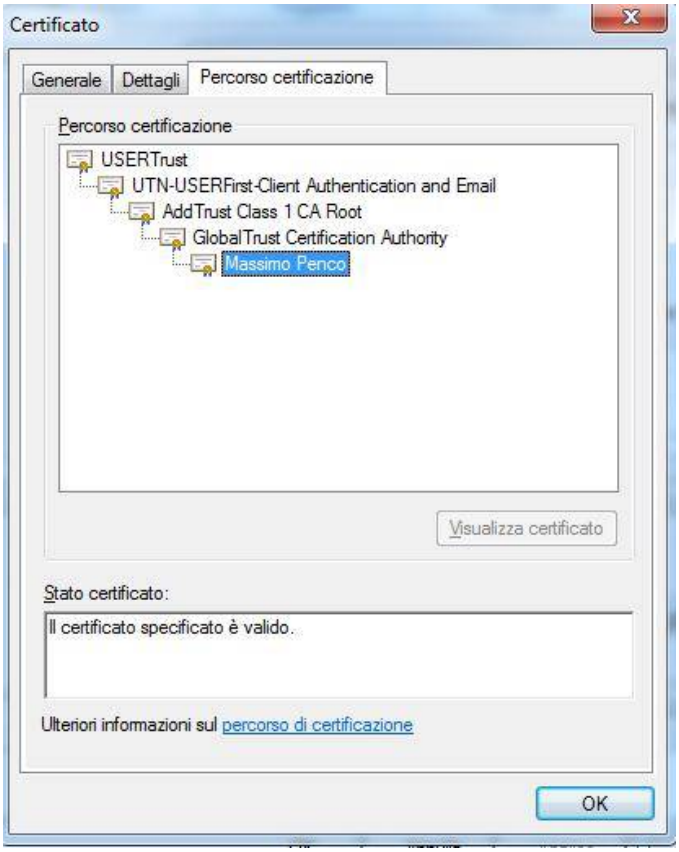
E' legata al certificatore che rilascia la FEA. Per la validità in tutto il mondo della FEA il certificatore deve essere chiaramente indicato nella lista delle CA riconosciute a livello mondiale. Tale lista è facilmente desumibile dai Browser che aggiornano periodicamente le liste in Internet Explorer: STRUMENTI/OPZIONI INTERNET/CERTIFICATI AUTORITA'DI CERTIFICAZIONE ATTENDIBILI. La lista è altresì rilevabile nel CABFORUM

Cosa devo fare per conservare il certificato?

Gli obblighi relativi al rilascio di un certificato in un "dispositivo sicuro" rimangono solo per i certificati qualificati. Come tutti sanno, la perdita di chiavette USB o di Smart card, come pure dimenticare un pin o una password, è una tragedia quotidiana, conseguentemente con la liberalizzazione della FEA ognuno potrà fare ciò che vuole conservando il certificato, con la propria cura e discernimento, , come per gli altri certificati, a proprio rischio e pericolo!

Come faccio a verificare dal certificato che chi lo ha rilasciato sia nella lista dei certificatori universalmente riconosciuti?

Basterà aprire il certificato stesso, comparirà una schermata simile a quella riportata in basso, cliccando su "Percorso Certificazione" basterà verificare che le prime tre, ma potrebbero essere anche due CA, siano nell'elenco sopra citato:



Come faccio a sapere se il certificato è adeguato all'uso che ne voglio fare?

Basterà cliccare su Generale (sempre all'interno del certificato) si leggerà il motivo per cui il certificato è stato generato normalmente quanto segue:

- Dimostra la propria identità ad un computer remoto
- Protegge i messaggi di posta elettronica

Se perdo il certificato cosa debbo fare?

Chiedere all'ente che lo ha rilasciato di revocare immediatamente lo stesso esigendo conferma dell'avvenuta revoca?

FIRMARE UN DOCUMENTO COME FARE

Oggi, con l'evoluzione della tecnologia e del software firmare un documento è una procedura molto facile.

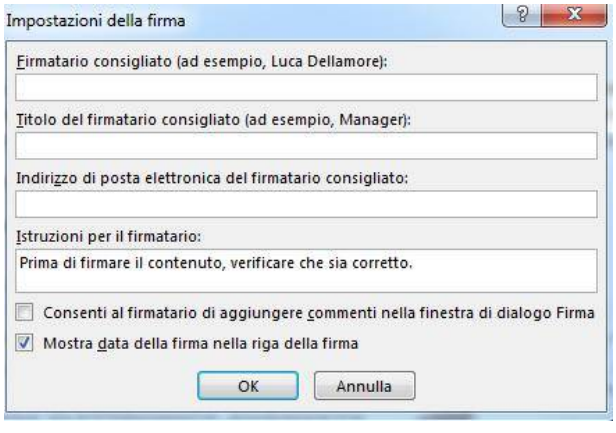
IN MICROSOFT OFFICE:

Per prima cosa bisogna sapere che Microsoft ha introdotto a partire da OFFICE 2010 la Firma Digitale Avanzata XADES nel proprio sistema. Microsoft inoltre ha, assieme a MOZILLA… aderito al CABFORUM. Detiene quindi, assieme agli altri, le liste delle CA Internazionalmente riconosciute al fine della firma Elettronica Avanzata sui propri documenti. Cosa fare in pratica.

IN WORD AD ESEMPIO:

Cliccando su inserisci e poi sull'icona di firma in alto a destra, si potrà inserire nel documento una riga di firma con l'immagine della stessa firma autografa. Microsoft inoltre, consiglia di dotarsi di un ID (certificato digitale) rilasciato da una Certification Authority riconosciuta, non solo dalla stessa Microsoft, ma da tutti nel mondo.

Cliccando quindi nella piccola linguetta a fianco si potrà inserire la firma. Nel documento apparirà la seguente schermata:



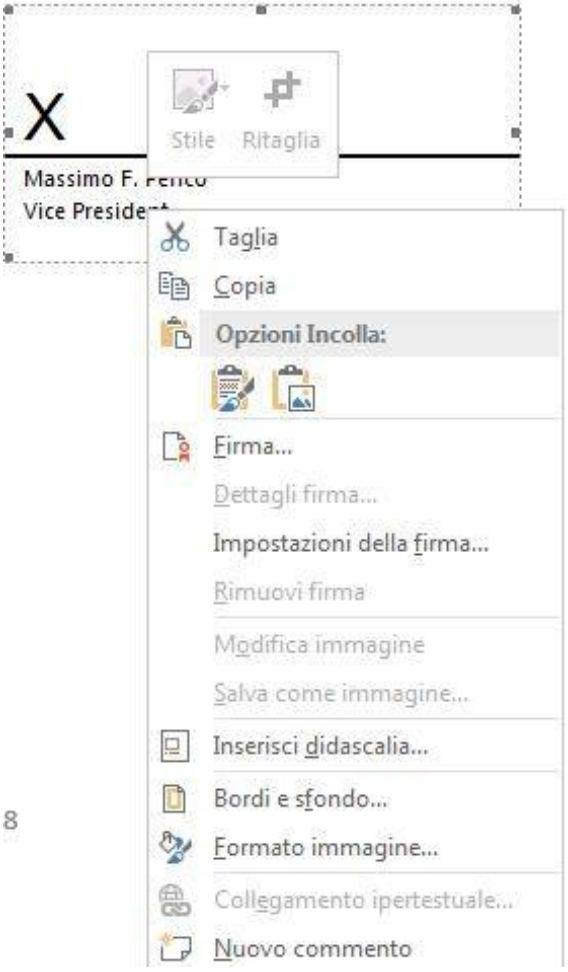
Compilare i campi presenti e apparirà il riquadro di firma:

X

Paolo Bianchi Rossi
CEO

Che si potrà spostare dove si vuole, normalmente alla fine del documento.

Cliccando con il pulsante destro del mouse si aprirà la finestra seguente che presenta varie opzioni:



Cliccando su "Impostazioni della Firma" si ripresenterà, per un eventuale controllo/modifiche, la schermata precedente come da noi compilata:

A questo punto, una volta controllato il documento, potremo firmarlo senza paura, in quanto l'operazione può essere reversibile. Apparirà la seguente schermata:

Si potrà selezionare l'immagine della firma autografa e compilare il resto della schermata in base alle proprie esigenze

Selezionando FILE della barra dei Menu, si aprirà questa finestra, posizionarsi su "Informazioni" – "Proteggi Documento" cliccare su aggiungi Firma Digitale:

Fig. 1

Compilare i campi in base alle proprie esigenze

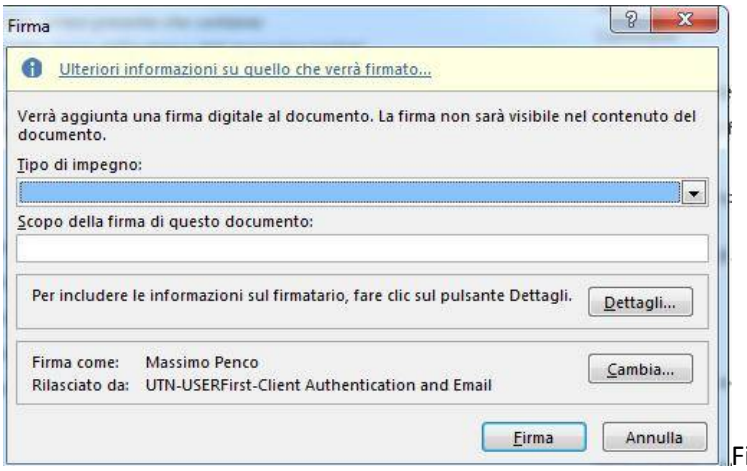


Fig. 2

Cliccando su "Dettagli" si potranno aggiungere ulteriori informazioni al documento (consigliamo di fare)

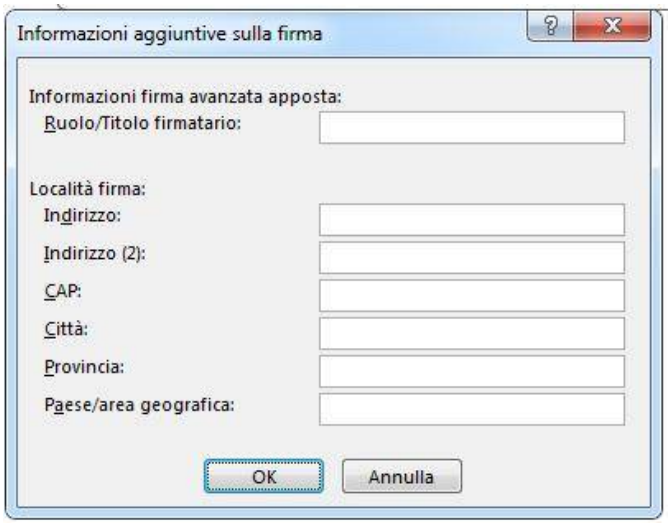


Fig. 3

Qualora si abbia più di un certificato, nella schermata precedente Fig. 2, si potrà scegliere cliccando su "Cambia" quale certificato utilizzare, apparirà la seguente schermata con l'elenco dei certificati installati nel proprio browser (IE). A questo punto scegliere il certificato FEA:

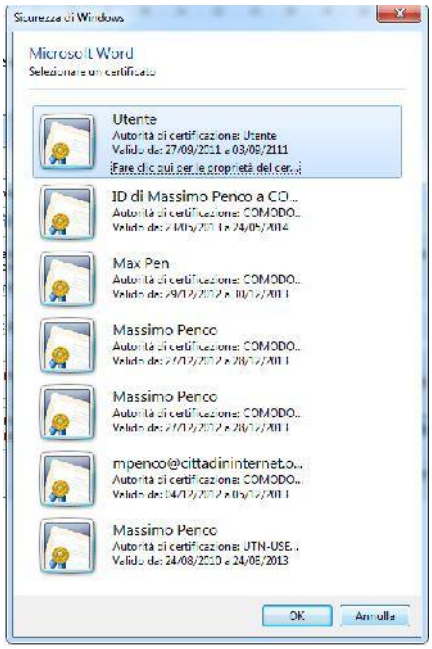


Fig. 4

A questo punto si potrà firmare il documento, che non dovrebbe essere più modificato. Apparirà il seguente avviso:

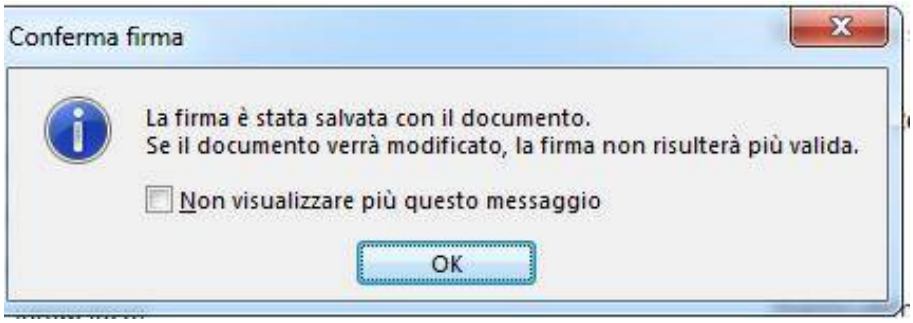
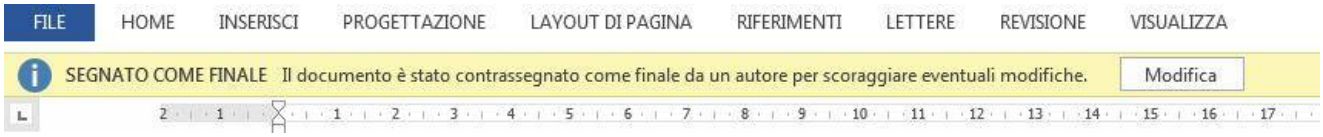


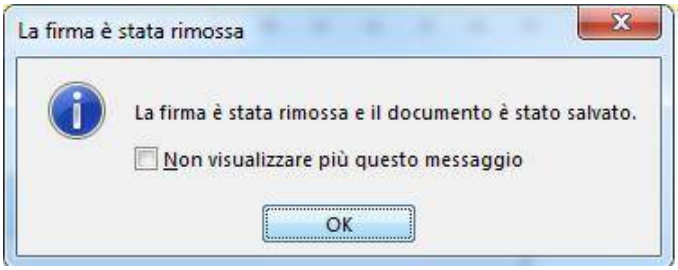
Fig. 5

Se si proverà a modificare il documento, una volta apposta la firma elettronica avanzata, appariranno una serie di avvisi che provocheranno la cancellazione da parte di Microsoft della firma stessa. Questa è la sequenza degli avvisi qualora si provi a modificare il documento:



Se si preme Modifica:

Se si preme Si:



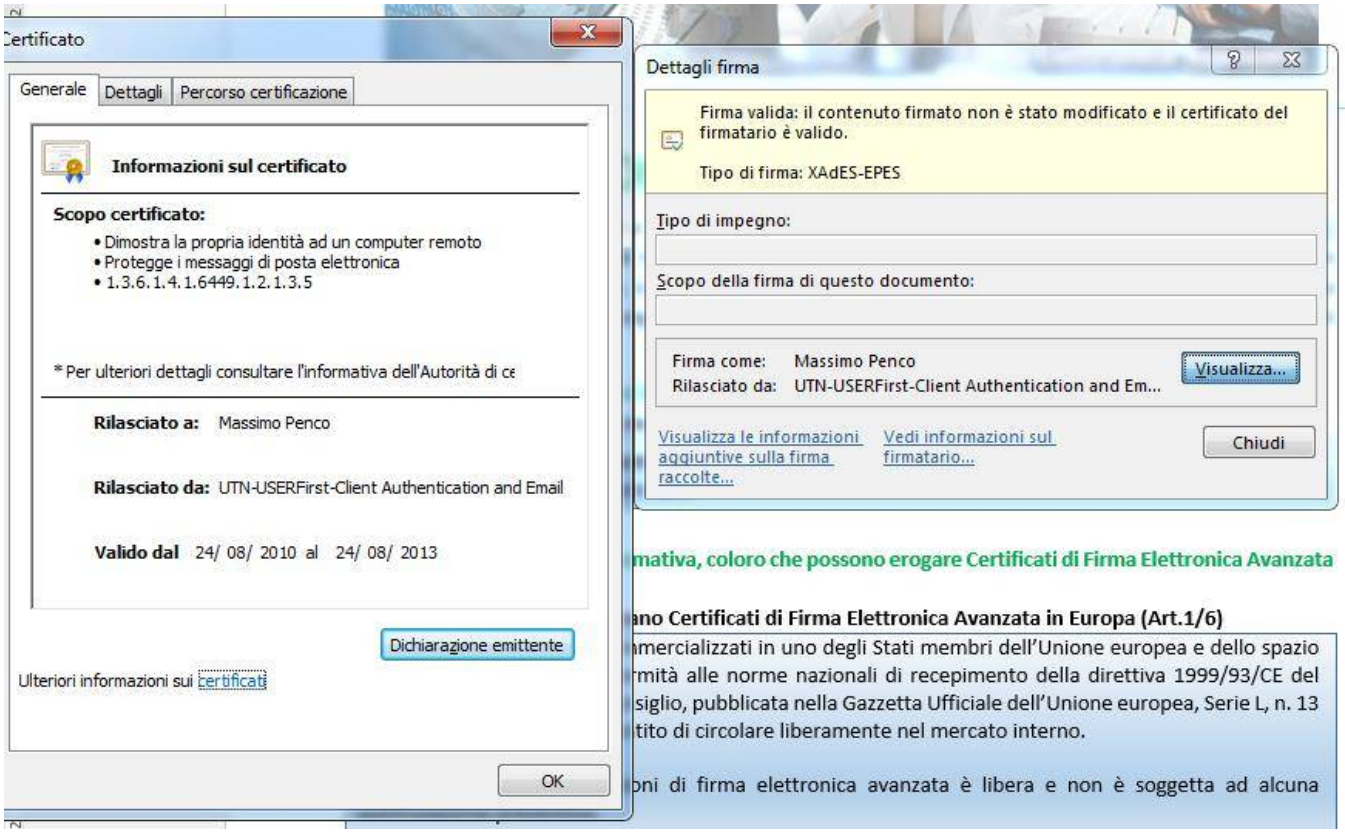
In sintesi: la procedura Microsoft rende pressoché impossibile modificare il documento dopo l'apposizione della firma

X X

Paolo Bianchi Rossi
CEO

Vediamo ora il controllo del documento:

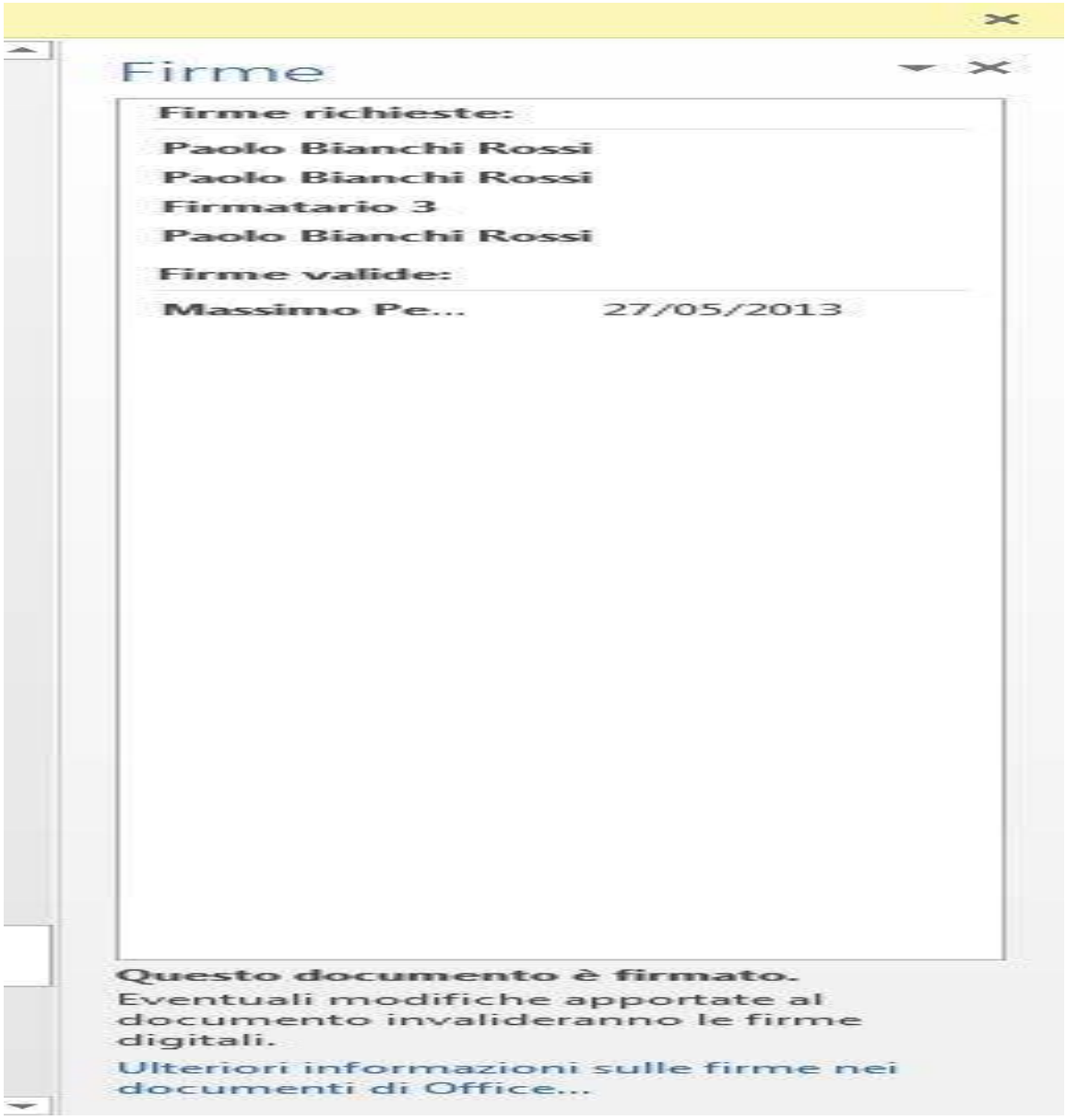
Quando il documento viene riaperto si mostrerà con la schermata di verifica firma come segue:



Cliccando su si apriranno le schermate su riportate che verificheranno la firma che potrà essere visualizzata completamente si avrà quindi la certezza che il documento non è stato modificato durante il suo percorso. La propria firma potrà essere rimossa in qualsiasi momento. Si ricorda che ogni volta che si firma un

documento questo viene archiviato automaticamente dal software come ultima versione, questo è visibile su proprietà documento:

Sulla parte destra dello schermo si vedrà un riepilogo delle azioni fatte e delle firme richieste per il documento stesso cliccando sulla firma si potrà accedere alle informazioni relative alla stessa già mostrate nella pagina precedente



Qui di seguito le ultime novità dei prodotti Office annunciate da Microsoft.

- Firma digitale Sono stati apportati miglioramenti alla firma digitale per i documenti creati utilizzando le applicazioni di Office 2013.
- Ora gli utenti possono firmare digitalmente i file in formato Open-Document (ODF v1.2) applicando una firma digitale invisibile.
- Office 2013 verificherà inoltre le firme dei file ODF creati utilizzando altre applicazioni.
- Le firme digitali XAdES nei documenti creati utilizzando le applicazioni di Office 2013 ora sono più semplici da creare. I documenti di Office 2013 firmati tramite XAdES consentono ai firmatari di aggiungere i relativi indirizzi, i titoli e di descrivere lo scopo delle firme. Office 2013 valuta inoltre le firme -XL utilizzando i certificati e gli eventuali dati di revoca contenuti nel file.

Microsoft suggerisce inoltre ancora in Office 2007 un paio di certificatori in office market place questa pagina sarà aggiornata a breve in quanto l'indicazione non è aggiornata e non più fruibile

ID digitali disponibili

ID digitali per Microsoft® Office System 2007

Gli ID digitali consentono di convalidare l'identità dell'utente e possono essere utilizzati per apporre la firma digitale a importanti documenti. I servizi che assegnano gli ID digitali oppure che li utilizzano e integrano Microsoft Office System 2007 sono riportati nel seguente elenco.

ID digitali disponibili

Avoco secure2trust: Prodotto software per la gestione dei diritti dell'organizzazione, utile per proteggere il contenuto dei documenti. secure2trust consente di controllare gli utenti che accedono ai contenuti e le operazioni da loro effettuate, nonché il processo di approvazione dei contenuti mediante le firme digitali. secure2trust si integra con i sistemi di autenticazione dell'organizzazione, come Active Directory e i certificati digitali, affinché l'accesso ai documenti contenenti informazioni riservate o alla proprietà intellettuale sia consentito solo agli utenti autorizzati. Per ulteriori informazioni su secure2trust e sulle modalità di acquisto, visitare il sito Web Avoco (in lingua inglese).*
IntelliSafe®: Servizio di invio, firma digitale e archiviazione protetta di documenti. IntelliSafe® offre applicazioni brevettate per la creazione di firme digitali che garantiscono l'autenticità e l'originalità di qualsiasi tipo di file. Il prodotto IntelliSafe Vault® è compatibile con Microsoft Office System 2007 e risponde alle necessità dei partner che riconoscono i vantaggi delle approvazioni e delle transazioni in formato elettronico. IntelliSafe consente di creare, firmare e archiviare in modo sicuro documenti importanti e con valore legale, in un ambiente totalmente privo di materiale cartaceo, direttamente da Microsoft Office. Per ulteriori informazioni visitare il sito IntelliSafe Technologies (in lingua inglese) (informazioni in lingua inglese).*
Per ulteriori informazioni su altri servizi e prodotti di terze parti da utilizzare con Microsoft Office, visitare il sito Office Marketplace.

Microsoft era da tempo che teneva nel cassetto la notizia senza per altro pubblicizzarla molto:

Microsoft supports EU Signature standard in Office 2010

2010-Apr-30 09:51 Filed in:All | Protocols
Microsoft has decided to support the EU digital signature format XAdES in Office 2010.

Read more about this at: http://blogs.technet.com/office2010/archive/2009/12/08/digital-signitures-in-office-2010.aspx

This format builds on the XML Digital signature standard from W3C which is the globally accepted standard for XML signatures.
XAdES adds a number of mandatory signed elements, which at least adds the signer's certificate as a signed element.
In addition to this, the XAdES standard also defines how to bundle the signature with extended verification data such as time-stamps and revocation information. This supports verification over a longer period of time when that verification data is hard to obtain from public resources.
The long term signature validation data bundling has always been the advantage with XAdES, but the added signer certificate as a signed property has been the reason why this standard has taken so long to accept and implement.
The problem was that for a long time, you could not add the long term validation data according to this standard unless the original signature was a XAdES signature with added signed elements. This made the standard useless for all implementations of XML signatures following the global W3C standard, which still is the vast majority of XML signatures.
Adding the signer's certificate as a mandatory signed element provides no real security advantage in the PKI trust model. All this does is that it prevents someone from suggesting the verifier to use another certificate for verification than the singer intended. However, in the PKI model it is the verifier's right to pick whatever certificate the verifier trust to identify the signer. In these typical uses of the PKI trust model, this added security feature have no value and the only real threat it address (attempting to prevent trust in a Malicious CA) is not anywhere closely mitigated by this feature.
This has divided implementations of digital signatures in a way that harms deployment and interoperability. However, once implemented, the added signed elements does not cause any harm for a verifier. It is therefore a good thing that Office now have decided to embrace this standard.