FIRMA DIGITALE - POSTA ELETTRONICA – SICUREZZA DELL'IDENTITA' PERSONALE ARCHIVIAZIONE DATI

Panoramica Normativa Applicazioni e riferimenti legislativi

Premessa

La Posta elettronica certificata e la firma digitale sono ormai una realtà consolidata in tutto il mondo. I produttori di software/hardware sono sempre più attenti a questo fenomeno, che fra l'altro, si avvicina e si integra sempre più con la messaggistica dei cellulari, il recente annuncio di Microsoft si immagina quindi che in futuri tutti i cellulari avranno a bordo il proprio sistema operativo probabilmente Windows Mobile già abbastanza diffuso.
Come ogni strumento, è soggetto a svariate problematiche e misure, ma in finale è anche il mezzo più rapido ed economico che è stato mai inventato per trasmettere dati e come ogni strumento va usato con la dovuta attenzione.
Abbiamo pensato sia utile scrivere alcune chiare e semplici regole per utilizzare le e-mail e dell'utilizzo della firma digitale in modo più sicuro, rapido ed efficiente. Questa **Best Practice** è indirizzata alle aziende, istituzioni, ma può essere anche una buona norma nell'uso privato.

La situazione ed alcuni dati salienti

La gestione della posta elettronica costituisce una seria questione per tutte le aziende ed istituzioni:
• E' protagonista ormai dal 25% al 50% delle attività quotidiane (fonte AIIM)
• Custodisce fino al 75% delle conoscenze aziendali e dati sensibili (Fonte Gartner)
• Oltre 171 miliardi di messaggi ogni giorno (Fonte AIIM 2006)
• Fino al 70% di spamming (Fonte AIIM 2006)
• La e-mail è sempre più usata come prova durante procedure legali
  - La firma digitale è una componente inscindibile dell'e-mail come mezzo di trasmissione di documenti ed ora anche Fatture Elettroniche *E-Invoice*.

Eppure....
pochissime organizzazioni hanno intrapreso un progetto di gestione organica della corrispondenza elettronica e suo uso sicuro, malgrado tutto questo…

@eMail - I perché di un successo -
OGGI L'EMAIL ASSOLVE A TRE DIVERSE FONDAMENTALI FUNZIONI
1. Mezzo di comunicazione rapida ed economica
2. Strumento semplice ma immediato di archiviazione
3. Efficace ausilio alla collaborazione interna ad un'organizzazione
4. Sistema unico per l'invio di documenti anche fiscali (Fatture)

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

Come deve essere un'e-mail professionale e soprattutto sicura?

Scegliere il **FORMATO** in base al tipo dei messaggi aziendali che normalmente si inviano:

- **HTML:** è il formato con la veste grafica più bella, non accettato da tutti, ma sicuramente quello che colpisce di più.
- **TESTO:** solo testo privo di grafica ed immagini.
- **RTF:** un compromesso tra i due precedenti.
- **CARATTERE:** può sembrare banale, ma la scelta del carattere ha un impatto molto importante per chi riceve un'e-mail ed inoltre è un sistema per "mitigare" tutti rischi connessi.
  Evitare caratteri strani, scegliere un carattere che tutti hanno normalmente installato nel proprio pc, invitare tutti con una comunicazione di servizio ad usare lo stesso carattere, con lo stesso corpo. Infatti, se qualcuno riceverà un'e-mail con carattere diverso, avrà quantomeno il sospetto che l'e-mail non venga dalla stessa persona o azienda.

MITTENTE: è importante non solo ai fini della sicurezza, ma anche ai fini della "netiquette" che venga indicato in chiaro il nome e il cognome del mittente. Evitare anche di inserire appellativi generici come Avv., Studio, Dott., Soc. ,che non si riferiscono alla persona od ente e fanno letteralmente impazzire chi li deve gestire nella rubrica alfabetica.

INDIRIZZI DI POSTA ELETTRONICA: vanno oculatamente scelti e resi standard per tutti. Naturalmente, se l'azienda vuole attuare una politica di riservatezza dei propri dipendenti, gli indirizzi e-mail non dovranno essere semplici da trovare. Gli indirizzi e-mail come nome.cognome@sito.it sono facilmente rintracciabili e più inclini alla ricezione di messaggi indesiderati, cercate di usare il sistema di anagrammare secondo logiche semplici ad esempio inserire prima il cognome e poi alcune lettere del nome: pencoma@globaltrust.it, vedrete che lo spamming ecc. diminuiranno sensibilmente.

FIRMA: come la vecchia corrispondenza le e-mail vanno firmate da chi le spedisce. In questo modo viene rispettata la "netiquette" ed inoltre, non costa nulla. Basta impostarla nel proprio programma di posta elettronica e verrà inserita automaticamente ogni qualvolta si crea, si risponda o si inoltra un messaggio, in base alla regola fissata.

GRAFICA della Firma: in base alla scelta del **FORMATO** potrete decidere come crearla.

DISCLAMER: è essenziale inserire sempre un **disclaimer** per la posta elettronica che inviate, il miglior consiglio, dal vostro avvocato. Qualora usiate un certificato di firma (altamente raccomandato) è bene inserire il **disclaimer** nel corpo dell'e-mail possibilmente sotto la firma con un carattere piccolo.

Alcuni esempi di disclamer generici:

1. DISCLAIMER
   This message and any information contained within it, including but not limited to subject matter, addressees and their e-mail addresses and attachments hereto are intended only for the personal and confidential use of the designated recipients named herein. Internet communications may not be secure and may be intercepted, re-directed or spoofed and therefore XXXXXX does not accept legal responsibility for the contents of this message unless independently verified in writing or digitally certified. Any views or options presented are solely those of the author and do not necessarily represent those of XXXXXX unless otherwise specifically stated. You are hereby notified that if you have received this message in error any review, dissemination, distribution or copying of this message is unlawful and strictly prohibited, and you should, with normal business courtesy, immediately notify the sender of the incident and then destroy this message by deletion and removal from your Deleted Items folder. Any opinions, explicit or implied, are solely those of the author and do not necessarily represent those of XXXXXX group of companies.

2. DISCLAIMER
   Questo documento contiene informazioni di proprietà XXXXXX e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

XXXXXX. Qualora fosse stato ricevuto per errore si prega di informare tempestivamente il mittente e distruggere la copia in proprio possesso.

3. DISCLAIMER

Le informazioni trasmesse sono da intendersi inviate solo ed esclusivamente alla persona alla quale sono state indirizzate e possono contenere materiale strettamente confidenziale e/o riservato. Qualsiasi utilizzo, ritrasmissione o diffusione delle presenti informazioni, anche solo parzialmente, sono proibite a tutte le persone od entità diverse dal destinatario. Se hai ricevuto queste informazioni per errore, contatta urgentemente il mittente e cancella immediatamente il materiale dal computer.

The information transmitted is intended only for the person or entity to.
Which it is addressed and may contain confidential and or privileged material. Any review, retransmission, dissemination or other use of, or taking of any Action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.

FIRMA FISICA: è invalsa l'abitudine da parte di qualcuno di inserire uno *specimen* di *firma* (l'immagine della propria firma/fisica) nell'e-mail o negli allegati. Non va mai fatto! Bisogna sempre ricordare che il messaggio di posta elettronica è una cartolina postale che tutti possono leggere. Nessuno manderebbe il suo *specimen* di *firma* in giro, può essere fatto solo ed esclusivamente se il messaggio viene inviato **criptato** tramite un sistema S-MIME con relativo certificato digitale.

Gestione degli invii di posta elettronica

L'invio di un messaggio di posta è un aspetto che va considerato con molta attenzione. Inviare un messaggio non vuol dire avere la sicurezza matematica che venga ricevuto e soprattutto letto da chi lo state inviando.

Conferma di ricezione e lettura

Attivare sempre la conferma di ricezione e lettura del messaggio. Questo non vi da la sicurezza matematica che il messaggio sia stato ricevuto e letto, ma almeno si potrà insistere e magari provare in giudizio la ricezione e lettura special modo se ritorna indietro la conferma relativa. Solo utilizzando il certificato digitale e la richiesta di conferma con protocollo S/MIME avrete la certezza matematica della ricezione del messaggio.

LINK nelle E-MAIL

Da parte di tutti ormai c'è il timore dei link ricevuti tramite email, che possono condurre in situazioni poco piacevoli (phishing) ed altro. È bene quindi, diffondere l'utilizzo di **GlobaltrustCallingID LinkAdvisor** che permette di conoscere preventivamente dove si andrà a "navigare".

Allegati al messaggio

A volte si necessita di inviare messaggi con grandi files allegati. Bisogna ricordare di usare con parsimonia lo spazio altrui, potreste intasare e/o bloccare la casella di posta di colui con il quale state corrispondendo, con le ovvie conseguenze.
Usate un diverso sistema di posta come il nostro **GlobaltrustCertifiedMail** che consente, nella versione Corporate, di inviare anche 4 GB di allegati.

Protezione della posta elettronica e relativi allegati

Con l'avvento della PEC (Posta Elettronica Certificata), sicuramente si è iniziato un cammino che renderà più semplice la corrispondenza e tutte quelle incombenze che fino ad oggi erano affidate alla raccomandata con ricevuta di ritorno (avviso di ricevimento), ancora oggi largamente usata.

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

Qualche Cenno Sulla Ormai Obsoleta Raccomandata AR

È ormai diffusamente riconosciuto che l'invio della raccomandata AR non è la soluzione ai problemi di seguito elencati:

1) La **certezza** della ricezione;
2) Il **non** ripudio della ricezione;
3) I **contenuti** della stessa;
4) L'**ora e la data** di ricevimento.

Vi è infatti giurisprudenza consolidata che quello che veniva considerato un sistema sicuro in effetti non lo è.

La certezza della ricezione: la raccomandata si può perdere e non arrivare a destinazione, lo stesso per la ricevuta di ritorno.

Il non ripudio della ricezione: sulla base di quanto esposto, chiunque può dire di non aver ricevuto nulla, o manca uno dei due requisiti o una combinazione dei due. Ad esempio si può essere nella situazione che Bruno ha ricevuto la raccomandata,ma Anna non ha ricevuto la ricevuta di ritorno, ...e allora ?!!

I contenuti della raccomandata: non vengono in alcun modo garantiti. Conseguentemente, l'invio di una busta vuota provoca ad esempio che Anna riceve un avviso di ricevimento da Bruno di una busta che non contiene nulla. La panacea dell'invio è nel cosiddetto foglio busta con il timbro postale nel primo foglio inviato, risolve parzialmente il problema, difatti assieme al primo foglio potrebbero essere inseriti degli altri che non vengono valicati dal timbro postale la conferma di averli inviati e ricevuti vanificata.

L'ora di ricevimento: non è garantita

L'onere della prova spetta a: colui che riceve la raccomandata. Fortunatamente recenti sentenze della Corte di Cassazione hanno rivisto questa normativa anche se a volte di parere opposto.

Alcune sentenze

Qualche cenno sul costoso ed ormai obsoleto FAX

Il Fax ha ormai perso di valore ed alcune massime e sentenze ne escludono la validità legale. Vi è da osservare che la trasmissione di un Telefax è molto simile alla trasmissione di un messaggio di posta elettronica fatto si è, che oggi, si ricorre sempre più a sistemi fax che partono e sono ricevuti da un computer senza quindi dover passare il foglio scritto in una macchina, che, in effetti, non fa altro che "scannerizzare" il foglio contenente scritti od immagini e trasferirlo elettronicamente al destinatario. Quindi, anche in questo caso si creano una serie di situazioni:

1) **Il fax viene scannerizzato:** inviato dal fax del mittente, ma non viene ricevuto dal destinatario
   a) La macchina fax del destinatario ha finito la carta e non trattiene in memoria il fax.
   b) La macchina fax del destinatario trattiene i fax in memoria l'energia elettrica manca la memoria viene azzerata.
   c) Le conferme di ricevimento di un Fax non provano che il ricevente lo abbia ricevuto, integralmente il fax e soprattutto letto lo stesso!
   d) Parte delle pagine possono risultare parzialmente o totalmente illeggibili.
   e) Nel caso sia un documento da riprodurre o modificare si dovrà ri-digitare completamente.
   f) I fax viaggiando su rete non protetta, possono essere facilmente intercettati e sostituiti tutti od in parte.
2) **Il fax viene inviato da PC:** i rischi sono più o meno gli stessi dell'invio da apparato Fax dedicato

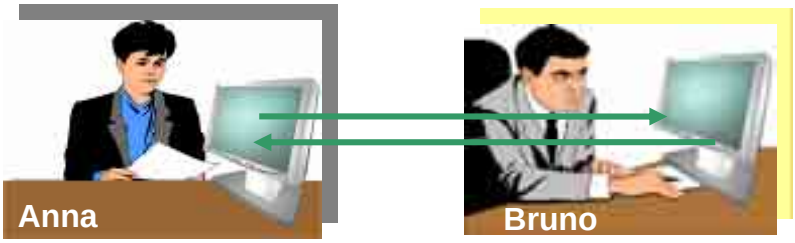
Questi sono alcuni degli eventi che dimostrano quanto sia labile e difficile avere la certezza tecnico/giuridica della validità di un Fax, tutto questo comporta fra l'altro il rischio evidente di ripudio da parte del ricevente.

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

Il fax in finale consiste nell'inviare una fotocopia di cattiva qualità di un documento originale. I costi dell'invio e della gestione di fax è molto elevato.

La PEC

Così come legiferata ed attuata:



- Ha bisogno che entrambi i soggetti (Anna e Bruno) abbiano una casella PEC con apparati specifici (es smartcard);
- Non è interoperabile con altri sistemi, con la produzione dello stesso effetto legale;
- Si perde l'identità della propria e-mail che non potrà più essere quella originale ma dovrà assumere la desinenza del provider PEC es. @poste.it
- Non può essere usata per corrispondere con altri paesi;
- Non può essere usata da più postazioni di lavoro, senza una nuova istallazione;
- Non garantisce il non ripudio dei contenuti del messaggio e neanche che ci sia nel contenuto nello stesso;
- Non ha nessuna portabilità;
- Complessa nell'istallazione e gestione;
- Non permette l'invio di allegati di grandi dimensioni.

È, per ora, relegata all'uso solo con la pubblica amministrazione, dove, fra l'altro, non ha una grande diffusione. E'costosa da acquistare e da amministrare. In sostanza non si capisce perché ci sia voluta una legge apposita per la PEC quando era sufficiente e più semplice l'uso del protocollo S-MIME , sembrerebbe quasi che il legislatore ed il relativo "controllore" abbia creato una forma di ***involuzione del francobollo*** che ormai da oltre un secolo consente di inviare e ricevere corrispondenza in tutto il mondo senza nessun particolare accorgimento ma in virtù della interoperabilità dei servizi postali, in sostanza all'incremento delle nuove tecnologie corrisponde un decremento della compatibilità. Del resto il solo paese che ha elaborato una legge apposita la PEC è l'Italia ??!!

Copre solo i seguenti campi:

Invio/Ricezione certificata di una busta elettronica senza certificazione del contenuto.

EVOLUZIONE LEGISLATIVA

La recente legge 28 gennaio 2009, n. 2 art. 6 cambia completamente lo scenario della Posta Elettronica certificata ponendo un alternativa alla PEC così come sopra descritta, difatti lo stesso recita "***"o analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità' del contenuto delle stesse, garantendo l'interoperabilità' con analoghi sistemi internazionali***."

In pratica:

In sostanza ognuno può scegliere il sistema di posta elettronica che vuole a condizione che:

1) L'uso di tecnologie che certificano la data ed ora dell'invio e della recezione delle comunicazioni

2) L'integrità del contenuto delle stesse

3) La garanzia di Interoperabilità con analoghi sistemi internazionali

Questi tre importanti liberi principi consentono di scegliere un ampia gamma di providers e soluzioni disponibili a tutti ma soprattutto garantisce la possibilità di comunicazione con tutto il mondo togliendo dal imbarazzo del sistema PEC che relegava l'Italia all'uso di un sistema inventato solo da questo paese come si è scritto ampiamente in merito dall'invenzione della stessa una per tutte (wikipedia ndr "E' bene però ricordare che si tratta di uno standard

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

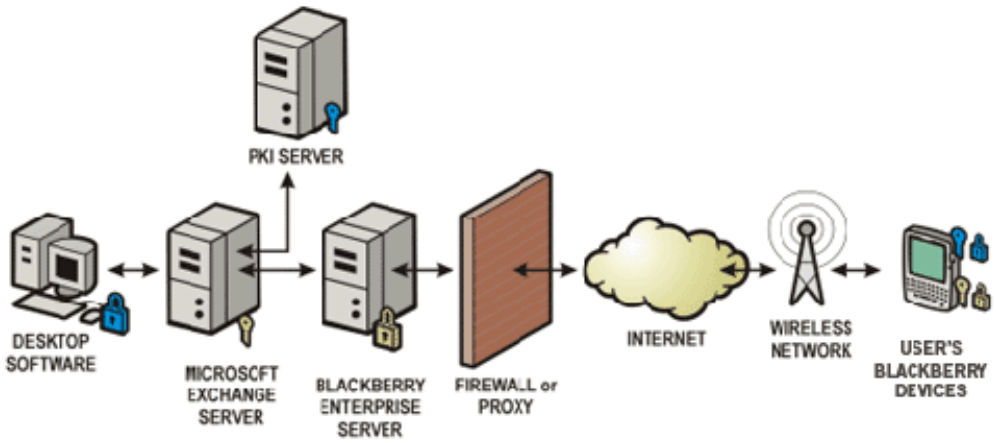
solamente italiano e per adesso nessun altro paese nel mondo ha sentito l'esigenza di creare un equivalente. Tecniche di firma digitale e di tracciamento della consegna equivalenti[2] e gratuite sono già disponibili per le email tradizionali da diversi anni.").

Si affronta finalmente al punto 2), l'integrità del contenuto delle e-mail ed ovviamente dei relativi allegati , questo in pochissime parole più che sufficienti però ! LA PEC non affrontava il problema si preoccupava solo del trasporto e dell'integrità della busta, senza pensare che la stessa come per le raccomandate AR può contenere un foglio vuoto.

Al punto 3 che si fa il passo più rilevante e noto infatti che il mondo è sempre più globale e mai come ora l'Italia ha bisogno di comunicare con certezze in campo Internazionale, esistono da oltre un decennio e previste fra l'altro dalla legge Bassanini, primi in Europa del lontano 1997, sistemi e protocolli sicuri usati in tutto il mondo ma che soprattutto in tutto il mondo spediscono miliardi di messaggi al minuto.

Il certificato di firma e posta elettronica e il protocollo S-MIME in combinazione con il sistema Certified Mail

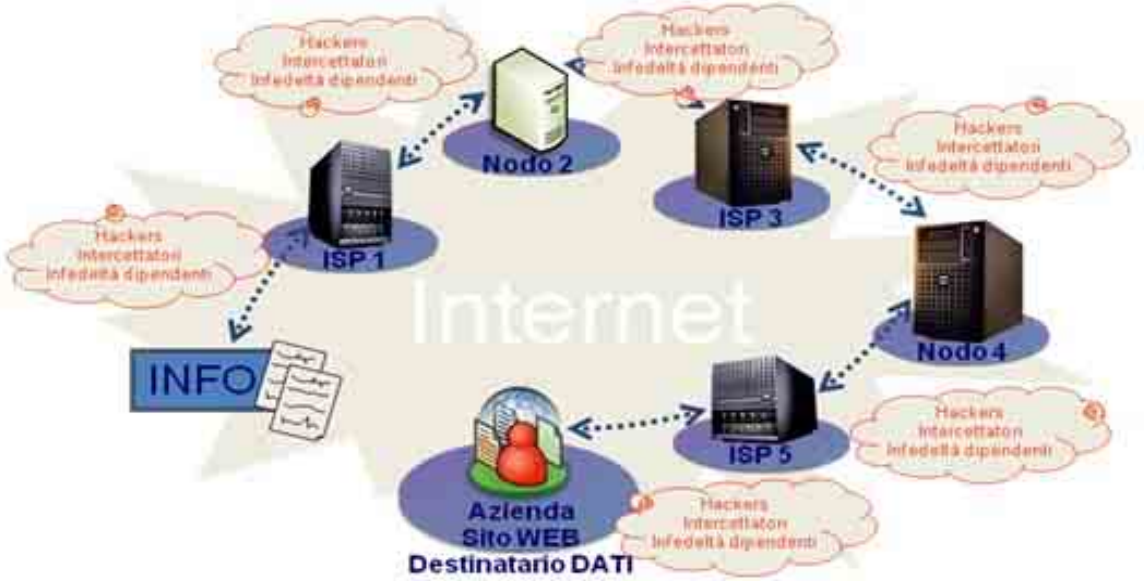
- Anna e Bruno non hanno bisogno di nessun apparato specifico a meno che lo vogliano. In tal caso possono scegliere qualsiasi cosa: token usb, floppy, ecc.;
- E' interoperabile con qualsiasi sistema;
- E' valida in tutto il mondo;
- Esportando od istallando più certificati può essere usata su più postazioni;
- La perdita di un certificato non comporta nessuna prassi burocratica (denuncia di smarrimento od altro) basta chiederne la revoca e non avrà più alcun valore e non potrà più essere usato.
- Garantisce il non ripudio del messaggio e dei contenuti dello stesso;
- Con funzioni di Time Stamping qualora implementate dal sistema garantisce e rende legali l'ora e ricezione del messaggio;
- Ha la massima portabilità e si può utilizzare, con la combinazione CertifiedMail, da qualsiasi postazione che abbia una connessione Internet;
- Semplice da gestire e da installare;
- Permette, con CertifiedMail, di inviare allegati fino a 4GB;
- È usufruibile da tutti ed ha valenza anche nei confronti della pubblica amministrazione;
- Molto economica da amministrare ed acquistare;
- Ampie applicazioni e flessibilità, l'esempio Blackberry



Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

L'inizio del Problema

La trasmissione dei dati, dopo aver premuto il tasto **INVIA** o **CONFERMA**, è **incontrollata** ed **incontrollabile**. I dati vanno in rete e transitano in un numero imprecisato di **Server/Computer**, linee telefoniche, connessioni, etc. facilmente intercettabili e/o sottraibili in tutto il loro percorso ed archiviazione.



Campagna Comunicare Sicuri - Roma, 8 Luglio 2008

LA MARCA TEMPORALE TIME STAMP L'ORIGINALITA' DEL DOCUMENTIO

La nuova disposizione di legge come su detto ripresenta il problema non banale dei contenuti del messaggio di posta che non è limitato al testo contenuto nei messaggi di posta elettronica ma anche agli allegati degli stessi, cosa piuttosto comune nella pratica di ogni giorno. Garantire quindi contenuti e non la "*busta di trasporto"* è una buona pratica che risolve non pochi problemi, indispensabile per questa forma di comunicazione certificata sono:

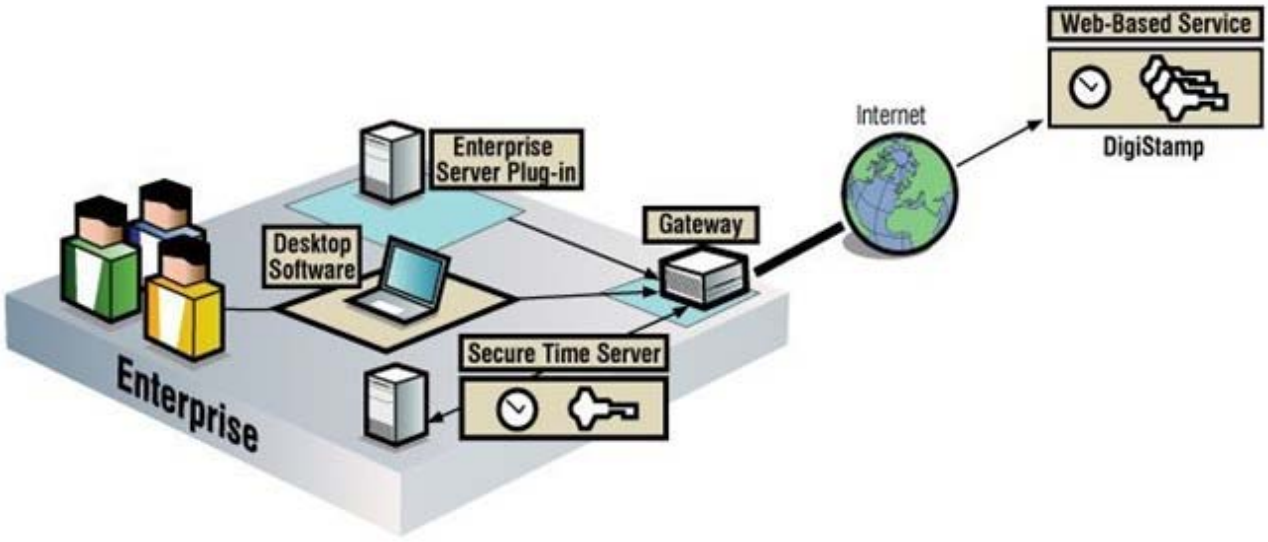
1. la certificazione con firma digitale
2. Il documento deve rimanere integro in tutto il percorso fino all'arrivo al destinatario
3. Deve essere garantita la privacy, conseguentemente la Best Practice è quella della criptazione dell'e-mail e dei suoi allegati, che non è proprio un eccesso di prudenza, ma la sicurezza che il messaggio non venga intercettato od aperto da chiunque, esistono sistemi ancora più sofisticati che prevedono in alcuni casi la distruzione dello stesso dopo che è stato letto.

CONTRARIAMENTE A QUANTO SI PENSA LA TRASMISSIONE DEI DATI NON AVVIENE DIRETTAMENTE TRA DUE SOLI SOGGETTI MA!

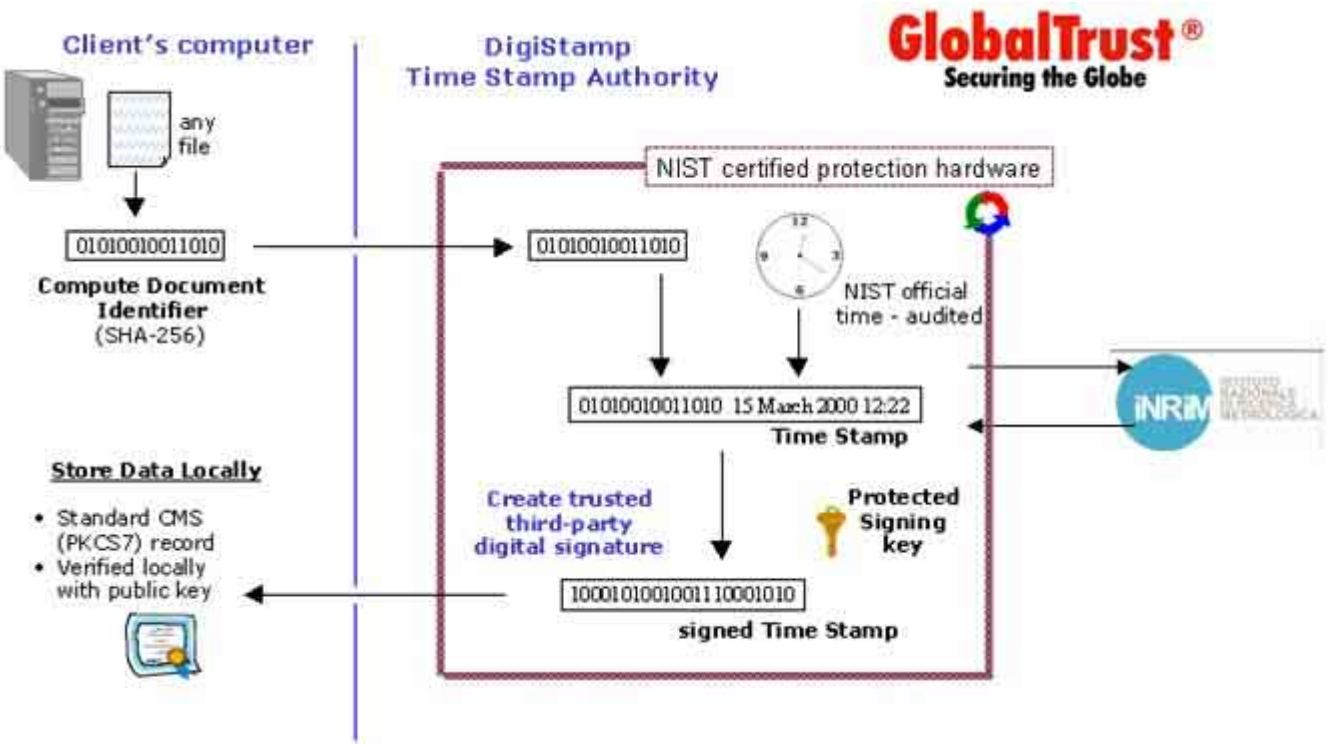
Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

4) Deve essere garantita qualora sia necessario la data ed in alcuni casi anche l'ora certa dell'elaborazione del documento, la PEC prevede solo la data ed ora certa di spedizione della "busta" che nulla ha a che vedere con il contenuto della stessa cioè il documento, quando questo si sia formato e sottoscritto digitalmente ed eventualmente scambiato tra le parti cioè firmato digitalmente dall'altra parte. Il riferimento nella nuova norma al fatto che: " ***certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità' del contenuto delle stesse, garantendo l'interoperabilità' con analoghi sistemi internazionali***." Spiega finalmente in modo semplice e conciso cosa si vuole, che poi è nel sistema già attuato in tutto il mondo.
5) È importante notare l'interesse del legislatore a ***garantire l'interoperabilità' con analoghi sistemi internazionali***" attraverso il sistema di marche temporali o TIME STAMP. Da tempo infatti tutto il sistema degli "orologi" che garantiscono l'ora e data di comunicazione sono interoperabili in tutto il mondo, del resto diversamente non potrebbe essere, in tutti i paesi esiste un organismo che regola l'ora interoperabile con tutti gli altri in Italia http://www.inrim.it/ questo a sua volta è collegato a tutti gli altri paesi per i sistemi informativi (computer) si usa il protocollo NTP Network Time Protocol. Il tempo coordinato universale (UTC) è la base temporale legale per tutto il mondo e segue il TAI, con uno scarto di un certo numero di secondi (attualmente 34). Tali secondi sono inseriti su consiglio dell'International Earth Rotation and Reference Systems Service (IERS), per fare in modo che, come media sugli anni, il Sole sia al meridiano di Greenwich entro 0,9 secondi dal 12:00:00 UTC.

Tutto questo per far capire quanto sia importante la standardizzazione di tutti i sistemi , dove una data ed ora devono essere riconosciute da tutti globalmente senza possibilità di dispute.



Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it



In Italia la data ed ora viene ulteriormente sincronizzata con L'**Istituto Nazionale di Ricerca Metrologica *(I.N.RI.M)***, onde avere una certificazione anche Italiana.

Avviso da inserire nei messaggi di posta con certificato S/MIME

È consigliabile inserire nei messaggi di posta elettronica un avviso come ad esempio:

"*E-MAIL FIRMATA DIGITALMENTE: questa e-mail, se firmata digitalmente, ha valore legale ai sensi della normativa vigente, maggiori info.*"

Questo servirà a far capire all'interlocutore che il messaggio che state inviando ha tutte le caratteristiche previste dalle leggi sulla firma digitale in vigore,non solo in Italia, ma anche in molti Paesi del mondo, per questo motivo è opportuno inserire un testo anche in lingua inglese come segue:

"*E-MAIL DIGITALLY SIGNED: this message is digitally signed and have legal value according to international law and treaties.*"

Entrambi gli avvisi potranno essere linkati verso le maggiori sorgenti di informazione nazionali e internazionali in modo da fornire all'interlocutore che lo voglia un'informazione corretta.

Alcuni tipi di problemi ed attacchi attraverso E-MAIL - il perché e la soluzione -

SPAMMING:

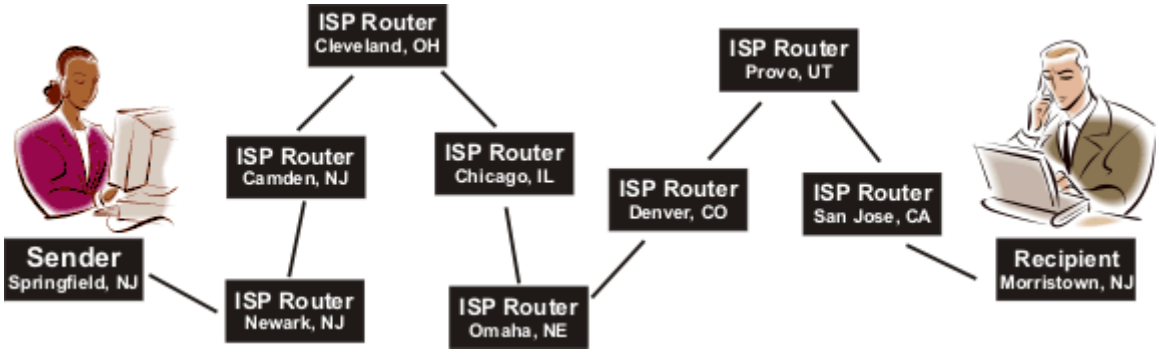
Ci si meraviglia di questo fenomeno! Purtroppo, a volte, siamo noi stessi a provocarlo navigando all'interno di siti che, ad esempio, ci fanno compilare moduli on-line non protetti da canali SSL, e noi, non verifichiamo se è presente il famoso lucchettino (con il nostro V-Engine è facilmente visibile). Così facendo lasciamo nella rete il nostro indirizzo e-mail. Nel mondo reale e non virtuale nessuno lascerebbe i propri dati alla portata di tutti!

L'uso estensivo da parte dei Provider o all'interno dei server delle aziende, di filtri antispamming

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

è ancora più dannoso messaggi importanti possono essere bloccati e non arrivare a destinazione, un buon filtro antispamming personale è molto più efficace in quanto controllato direttamente dall'utente.

Per avere un'idea più precisa di cosa succede quando s'invia un messaggio di posta elettronica lo schema seguente può essere d'aiuto:



Con i sistemi 'tradizionali' di trasmissione delle e-mail, molto simili a delle cartoline postali, il messaggio è vulnerabile e soggetto ad accessi ed utilizzi non autorizzati e quindi non sicuri con una trasmissione a dir poco 'rocambolesca'.

Un esempio, dimostra come, un messaggio invece di fare un semplice 'viaggio' di pochi chilometri, ne debba fare uno di circa 6000 chilometri passando attraverso numerosi ISP ed essere così esposto a numerosi rischi , non ultimo quello di *"sniffare"* o *"spoofing"* gli indirizzi e-mail dove esiste un vero e proprio mercato per la vendita degli stessi.

Approfondimenti in:

http://www.cert.org/tech_tips/email_spoofing.html

http://www.lse.ac.uk/itservices/help/spamming&spoofing.htm

FURTO DI IDENTITA':

E' una conseguenza indiretta di quanto precedentemente detto nessuno deve dare propri dati in un sito non protetto.

PHISHING:

E' ancora collegato a quanto sopra. In questo caso l'uso del nostro permette di conoscere a chi appartiene il link, normalmente inviato con una E-mail, prima di cliccarci!

LINK per chi vuole approfondire l'argomento sull'origine ed uso del protocollo/certificato S/MIME

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

http://guide.debianizzati.org/index.php/Chiavi_simmetriche_e_chiavi_pubbliche

http://www.tech-faq.com/lang/it/s-mime.shtml

http://ec.europa.eu/idabc/servlets/Doc?id=849

http://www2.cnipa.gov.it/site/_contentfiles/01379800/1379887_16%2003%2001%20caso%20aipa.pdf

http://www.microsoft.com/technet/prodtechnol/exchange/IT/Guides/E2k3ClientAccGuide/3316c76c-2527-4a78-8944-d17c075e9ab6.mspx?mfr=true

http://radarlab.disp.uniroma2.it/FilePDF/crittografia2.pdf

http://www.microsoft.com/technet/prodtechnol/exchange/IT/Guides/E2k3MsgSecGuide/02deb7c5-89d4-4e15-9300-5fc355ea83a4.mspx?mfr=true

Consigli per amministrare e gestire certificati S-mime

L'amministratore di sistema o il singolo utente hanno la possibilità di gestire e mettere in sicurezza il certificato:

- Impedendo l'esportazione dello stesso - in questo modo il certificato non potrà essere copiato da dove è installato.
- Proteggere l'accesso e l'uso del certificato tramite password.

La combinazione delle due daranno un'adeguata sicurezza al certificato e a chi lo usa, specialmente se viene installato su un dispositivo portatile, token, smart-card o altro.

Qualche cenno sull' Autenticazione del richiedente di un certificato S-mime.

Il dispositivo legislativo **Legge 24 novembre 2000, n. 340 e successive modificazioni** ed il successivo chiarimento nel D.Lgs. 7 marzo 2005 art. 2, si sono definitivamente pronunciati sulla legalità delle autocertificazioni, che sono così valide anche nei rapporti tra privati. GlobalTrust nell'ambito del programma RMS mette a disposizione Certificati Standard S-mime ad uso personale completamente gratuiti rilasciati in base alla disciplina legislativa richiamata. Con la ratifica della convenzione di Budapest che risale al lontano 23 novembre 2001 avvenuta con legge 18 marzo 2008, n. 48 si apportano notevoli cambiamenti al Codice Penale Italiano aggiungendo l'art. 491-bis e 640-quinquies, contenuti nella legge già richiamata introducendo il reato di falsità nelle dichiarazioni al certificatore, viene così da un lato ribadita la validità dell'autodichiarazione dall'altro la assoluta punibilità della stessa che precedentemente era solo stabilita dalle norme civilistiche relative.

TEST delle e-mail firmate ed anche criptate

Al fine di verificare tutte le funzionalità del certificato S-MIME è buona norma effettuare subito dei test scambiando la chiave pubblica con chi si vuole corrispondere in modo sicuro.

Qualora vogliate effettuare una prova con il nostro servizio KEYTEST (che si attiva con un'e-mail non appena avrete scaricato ed installato il certificato S-mime) non dovrete far altro che seguire le istruzioni presenti nell'e-mail che vi verrà inviata, maggiori informazioni nel nostro sito web.

Dopo aver inviato un'e-mail firmata digitalmente, semplicemente cliccando sulla coccarda posta in alto a destra del messaggio di posta elettronica  . Con Outlook 2003, una volta ricevuto ed aperto il messaggio, il certificato verrà installato automaticamente nel sistema del ricevente a prescindere che abbia o no un nostro certificato.

Ovviamente si possono con altrettanta semplicità criptare e firmare gli allegati di un messaggio.

Per allegati di grandi dimensioni si consiglia di usare il nostro sistema Certified Mail assieme al

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

certificato S-MIME.

La procedura è facilmente intuibile nel grafico qui sotto.

ATTENZIONE: In questo modo solo il destinatario, con la propria chiave privata, è in grado di leggere il contenuto del messaggio.

Certificati Internazionalmente riconosciuti e relative Certification Authority pubbliche

Tutti ne parlano ma nessuno è mai riuscito a trattare questo delicato argomento con semplicità cerchiamo di farlo noi.

I certificati digitali vengono regolati dai Browser dove sono elencati nella loro struttura ad "albero" in Explorer , ad esempio, cliccare in **Strumenti=>Opzioni Internet =>Contenuto =>Certificati.**

Qui e solo qui troverete tutti i certificati installati nel vostro computer e quelli personali da voi usati, qualsiasi aggiunta di altri certificati è fatta a proprio rischio e pericolo come viene riportato da tutti Browser.

Diffidate quindi da software come ad esempio XXXXX che istallano nel Browser altri certificati anche se non si mette in dubbio la attendibilità degli stessi essi hanno **validità solo ed esclusivamente** per colui che li accetta ed installa non nei confronti dei terzi con cui corrisponde ed interagisce che continueranno a ricevere messaggi di errore.

Quando si apre una finestra simile a quella che vediamo qui di seguito l'utente è arbitro di scegliere se considerare l'autorità di certificazione valida oppure no e conseguentemente installare il certificato nel proprio computer.

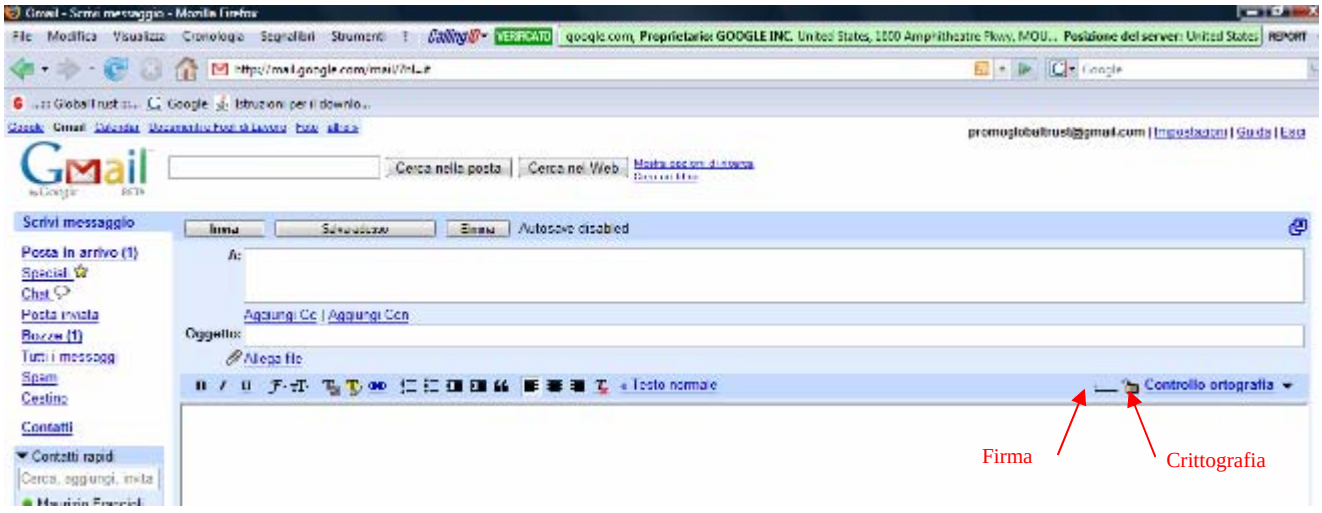
Una volta fatto considererete quel certificato ed il suo autore valido a **tutti gli effetti**, questo però non vuol dire che le comunicazioni che invierete tramite quel certificato saranno automaticamente valide per chi le riceve.

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

Questo meccanismo ed il protocollo S-mime sono gli **UNICI** sistemi di scambio sicuro di posta elettronica e messaggistica riconosciuti, tutti gli altri sistemi, a prescindere dalla qualità o serietà del prodotto sono all'origine considerati come **non attendibili** e rilasciano i messaggi come su riportati.

Client di posta Web: Gmail e Certificati SMIME

Grazie alla collaborazione tra Gmail , Firefox e con l'impiego dei Certificati Digitali SMIME, oggi è possibile inviare e-mail firmate digitalmente anche dal client di posta web Gmail ! Nel portale web Gmail ora è presente la funzione di invio di e-mail **Digitalmente Firmate e Crittografate**.



Il portale Gmail, è in grado di andare a impiegare i certificati digitali, visti da Firefox nel Pc, e ne sfrutta le proprietà per inviare e-mail firmate. Ma non solo, infatti il client Gmail grazie alla tradizionale procedura di scambio di chiavi pubbliche, consente anche l'invio di e-mail Crittografate, aumentandone sicurezza e riservatezza. Per usufruire delle nuove funzioni messe a disposizione da Gmail, basterà aggiornare Firefox con il nuovo componente aggiuntivo, scaricabile tramite il link https://addons.mozilla.org/it/firefox/addon/592 e disporre di un Certificato Digitale SMIME. Per saperne di più http://www.certifiedmail.it/pdf/Gmail_SMIME.pdf

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

Non solo posta elettronica: Firma e Cifratura di documenti

I certificati con protocollo S-MIME da noi emessi sono anche certificati di firma ai sensi della legislazione vigente sia in Italia che in tutto il mondo, gli stessi sono in grado di firmare legalmente documenti che a loro volta possono essere inseriti in messaggi di posta elettronica od archiviati in qualsiasi supporto informatico, possono essere altresì cifrati attraverso sistemi di criptazione standard. La creazione e lo scambio di documenti, è senz'altro una delle operazioni più comuni e diffuse. Grazie ai nostri Certificati Digitali di tipo *"Client"* in combinazione con applicativi della suite Adobe Acrobat o Microsoft Office, si può rendere tutto questo estremamente sicuro e conforme alle normative in vigore. L'unione tra Certificato Digitale e applicazioni come Microsoft Word, Excel o PowerPoint, permette in pochi click di garantire l'autenticità, l'integrità e l'origine di un documento.

Office 2007:

1 2 3

Office 2003:

1 2 3 4

ADOBE Acrobat

1 2 3

Il documento una volta firmato digitalmente garantisce che il firmatario corrisponda realmente alla persona che dichiara di essere, che il contenuto non sia stato modificato o manomesso dopo essere stato firmato digitalmente e rende impossibile il ripudio del documento, cioè l'atto di negazione da parte di un firmatario di qualsiasi associazione con il contenuto firmato e dell'invio dello stesso.

Il documento può avere altre protezioni come ad esempio password o limitare l'uso, vietarne la digitazione, stampa od altro.

Firma digitale in Microsoft Office

Firma digitale in Adobe Acrobat

Un documento Firmato e Certificato Digitalmente è facilmente riconoscibile, grazie all'apposito simbolo riportato nella barra delle applicazione, che con pochi click permette di venire a conoscenza di tutti i dati relativi all'identità del mittente che viene così ad essere Certificato Digitalmente apponendo la propria univoca Firma Digitale, attraverso un sistema di "Time Stamping", si certifica anche **ora e giorno** in cui è avvenuta la Firma del documento ed anche la suo invio e ricezione.

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

Schermate certificato

I documenti e le informazioni sia private, che aziendali costituiscono un valore da proteggere sia da furti, manomissioni che dall'accesso di utenti non autorizzati e ovviamente anche nella trasmissione on-line degli stessi. I Certificati Digitali oltre alla Firma Digitale permettono di Crittografare i nostri documenti, infatti grazie all'utilizzo dei Certificati Digitali ed applicativi come Globaltrust Enigma, i nostri documenti saranno Criptati con i più sofisticati sistemi esistenti (AES, 3-DES, etc.) garantendoci l'integrità e la riservatezza dei dati.

Uso specialistico della Firma digitale: Fatture Elettroniche (E-invoice)

L'invio di fatture attraverso posta elettronica è uno delle nuove applicazioni che molti già usano anche in questo caso senza conoscere sia la normativa che il sistema per attuare questa prassi in modo economico sicuro e in regola con le disposizioni di legge che non si limitano solo al territorio nazionale ma che sono operative in tutto il mondo e regolamentate da direttiva comunitaria nella Unione Europea. Ancora una volta l'interoperabilità e quanto richiesto dalla UE fanno si che la PEC così come legiferata in Italia sia non usabile per questo tipo d'uso specialistico mancando dei requisiti essenziali già precedentemente descritti (**La PEC pag. 4**).

Il nostro certificato di firma, assieme al protocollo S-Mime di cui è costituito, fanno si che lo stesso abbia piena validità legale a livello normativo sia nazionale che internazionale pertanto qualsiasi messaggio di posta Elettronica con il nostro certificato con allegato la fattura debitamente firmata sempre con lo stesso certificato ha piena validità legale ed in armonia con le circolari 45/E del 19/10/2005 36/E del 06/12/2006 e successive modificazioni del Agenzia delle Entrate ed oltre come vedremo in seguito anche altre importanti funzioni relativi all'archiviazione dei dati e la de-materializzazione dei documenti contabili/Fiscali.

Aspetti Normativi

Il quadro normativo è rappresentato dalla direttiva comunitaria del 20/12/2001 N.115/2001 recepita in Italia dal D.L. del 20/02/2004 N. 52 e successive modificazioni, tutte le normative concordano sul fatto che l'invio di fatture in formato elettronico tramite e-mail devono avere i seguenti principali requisiti:

- Essere firmate digitalmente attraverso i modi e termini e tramite un certificatore indicato dalla direttiva comunitaria 1999/93/CE ai fini di garantire l'assoluta interoperabilità della firma e del mezzo di trasmissione (e-mail) in tutti gli Stati dell'Unione Europea, confermata dalla direttiva n° 115/2001.
- La firma digitale va implementata attraverso funzioni di Time Stamping.
- Va richiesta la preventiva autorizzazione ad inviare fatture attraverso e-mail, seguire la procedura dello scambio chiave su indicata con un breve messaggio di richiesta autorizzazione è già di per se stesso una approvazione certificata dell' uso di questa procedura.

A prescindere dai requisiti di legge e/o fiscali ne esistono altri da tenere in considerazioni che sono:

- La riservatezza delle informazioni che s'inviano, intercettare una fattura vuol anche dire mettere in piazza i prezzi che si praticano oltre i dati cliente/Fornitore indispensabile inviare quindi un messaggio criptato.

Il non ripudio nel invio/ricevimento della stessa, è ormai prassi usuale nel ritardare o non eseguire pagamenti sostenere di non aver ricevuto le fatture.

L'Archiviazione elettronica delle fatture e dei documenti contabili .

La logica conseguenza dell'invio delle fatture in formato elettronico è l'archiviazione elettronica delle stesse e dei relativi documenti contabili, il quadro normativo è quello precedentemente indicato, esistono procedure molto complesse con applicazioni di tipo verticali molto costose in verità special-modo per le piccole e medie imprese la soluzione e molto più semplice e poco costosa.

LINK per chi vuole approfondire l'argomento sulla fattura elettronica/archiviazione digitale dei documenti contabili.

http://www.interlex.it/docdigit/fattelettr.htm

http://www.microsoft.com/italy/pmi/gestioneimpresa/speciali/fatturaelettrclausole/default.mspx

http://www.conservazione-sostitutiva.it/index.php

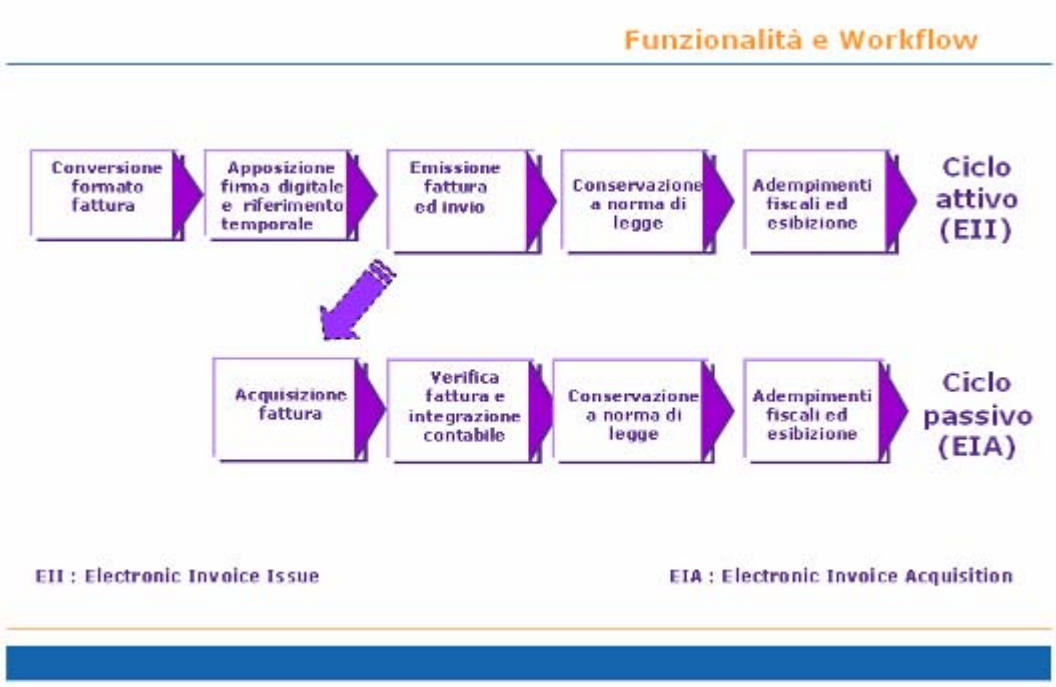
http://fo.src.cnr.it/reader/?MIval=cw_usr_view_articolo&articolo=8654&giornale=8763

http://www.cobrand.ilsole24ore.com/fc?cmd=art&codid=20.0.1759226677&chId=41

Ci sono parecchie informazioni On-Line basta digitare "fattura elettronica" nei motori di ricerca che si viene sommersi da un surplus di dati che e bene leggere con dovuta attenzione e andare nei siti ufficiali della Agenzia

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

delle Entrate e dell'Unione Europea già di per se ricchi di documentazione più che sufficiente per prendere le opportune decisioni in merito.



Alcuni degli usi più comuni delle e-mail certificate con protocollo S-MIME e Firma Digitale

- Firma digitale della E-mail e documenti di qualsiasi genere allegati alla stessa
- Invio di fatture ed altri documenti contabili loro archiviazione digitale
- Redazione ed invio di contratti
- Invio di documenti riservati (firmati digitalmente e criptati)

La portabilità sicurezza dell'identità personale

I Problemi della portabilità dell'identità personale e protezione dei dati:

- Come per i propri documenti personali ognuno di noi vuole avere con se quanto lo identifichi per necessità e per concetto ormai consolidato.
- La firma e certificazione digitale, così come concepiti non solo sono insufficienti, ma possono rappresentare un pericolo ancora più forte se non usati correttamente. Password OTP smart card e quanto altro non servono a nulla se non si usano con altre accortezze, debbono però avere la massima portabilità ed essere semplici da usare e gestire.

La Soluzione al Problema

- In un mondo così complesso e frenetico le soluzioni di sicurezza devono essere:

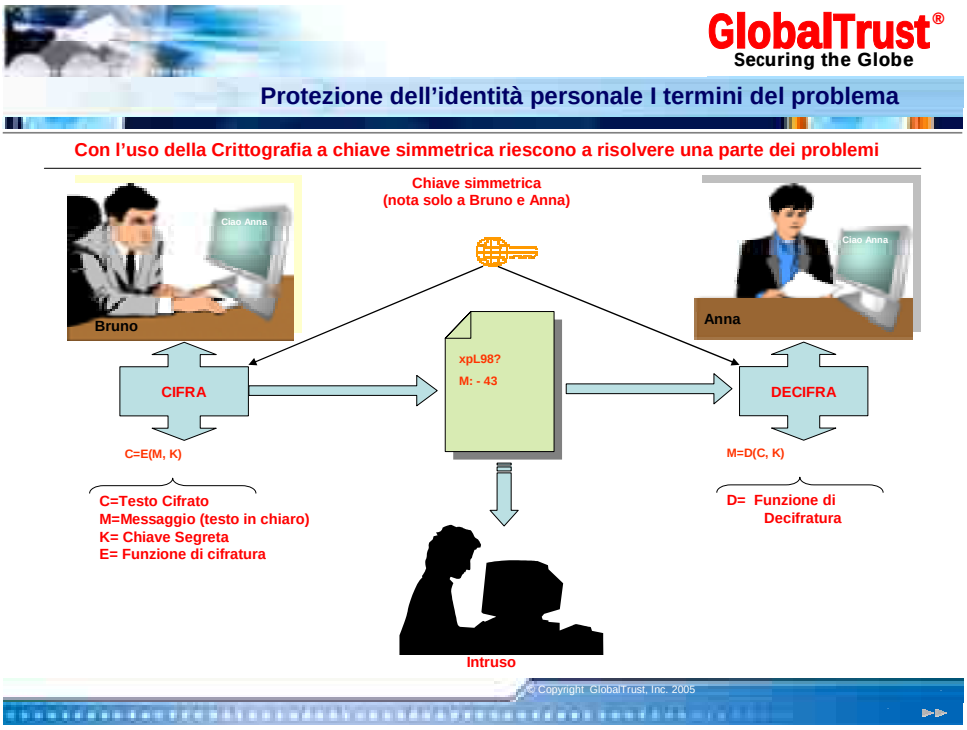
Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

- Semplici da usare e gestire
- Avere la massima portabilità
- Fruibilità e continuità del servizio sono altresì indispensabili.

APRITI SESAMO™ E' LA SOLUZIONE AL PROBLEMA

Apriti Sesamo™ è forse l'unica soluzione all-in-one che consente la scelta di qualsiasi apparato hardware con la possibilità di inserire la combinazione di software e certificati digitali ampliando la gamma dei fattori di autenticazione in un unico apparato hardware incluso il cellulare.

I grafici che seguono rappresentano quanto può avvenire con l'uso del solo certificato installato direttamente nel PC.

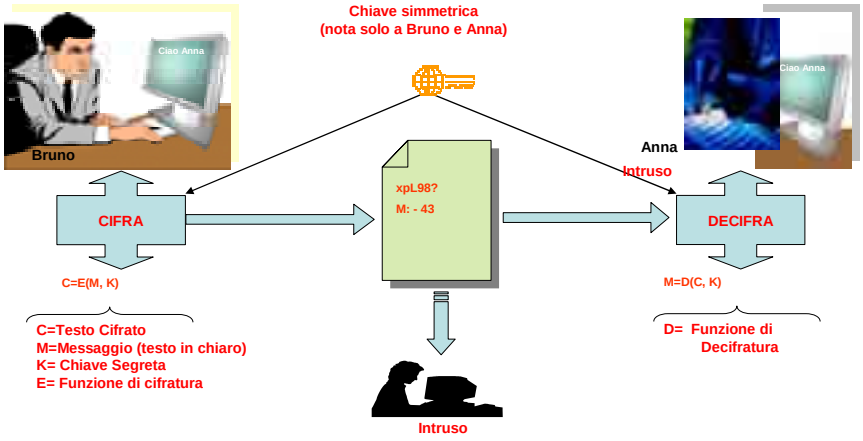


Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

GlobalTrust®
Securing the Globe

Protezione dell'identità personale I termini del problema

La problematica si ripresenta se Bruno invia un messaggio da Anna che lascia il PC Incustodito

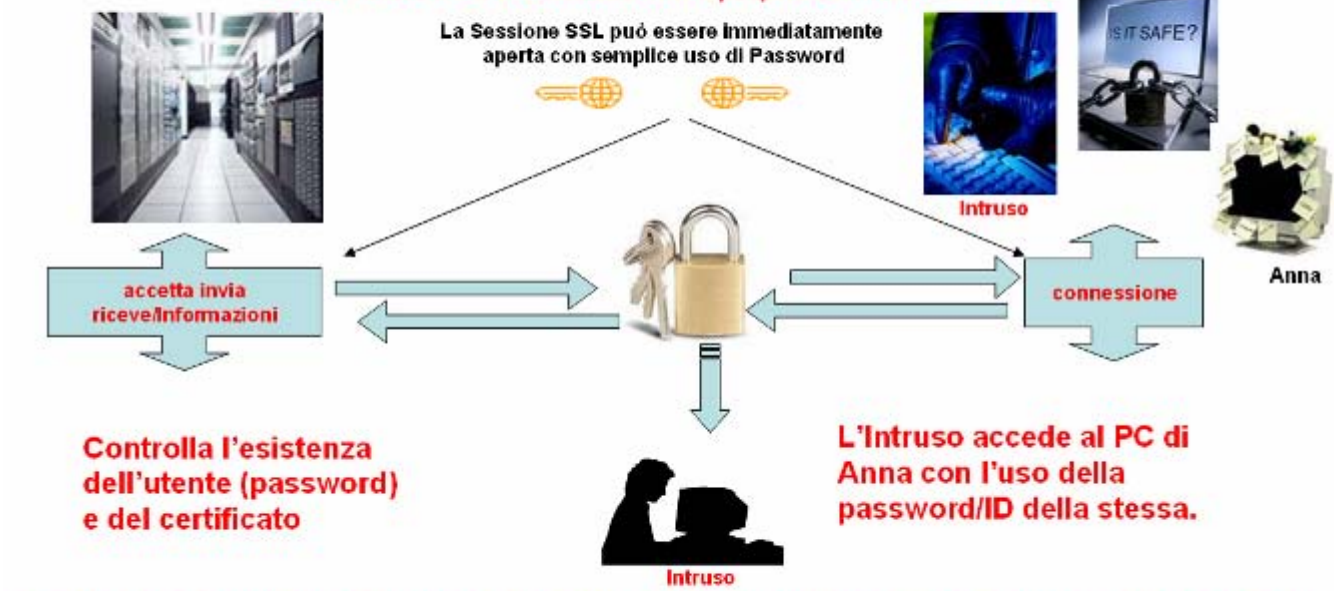


Al posto di Anna Potrebbe esserci chiunque malgrado la crittografia e la firma digitale il certificato residente nel computer diviene il pericolo ancora più grave.

GlobalTrust®
Securing the Globe

Protezione dell'identità personale I termini del problema

Analoga problematica si ripresenta se si usa una connessione sicura X509 (SSL) tipico nell'Home Banking
Anna lascia il PC Incustodito con il proprio certificato installato



Al posto di Anna Potrebbe esserci chiunque malgrado il certificato che residente nel computer diviene il pericolo ancora più grave.

27

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

La persona, che riesce ad entrare nel PC di Anna anche se protetto da password di accesso (troppo debole) dove è installato un certificato residente, potrà:

- **Accedere al PC.**
- **Copiare informazioni riservate.**
- **Danneggiare il PC (es. formattazione HD).**
- **Cambiare le informazioni contenute nello stesso.**
- **In qualche caso accedere all'intera rete.**
- **Leggere le E-mail anche se inviate criptate e con firma digitale.**
- **Rispondere alle stesse simulando di essere Anna.**
- **Rendere legale qualsiasi scambio di messaggi contratti o quanto altro.**
- **Rendere altresì legale qualsiasi transazione bancaria effettuata.**
- **Difficile da provare il ripudio delle operazioni effettuate da ambo le parti.**

IN SOSTANZA ANNA "VERA" SARA' COMPLETAMENTE SIMILE ALLA ANNA "INTRUSA" (*ANNA HACKER DIGITALE)*

La sicurezza portabilità ed archiviazione dei propri dati.

Avere con se il proprio cellulare, la chiavetta USB con giga-byte di dati è ormai prassi comune, la metodologia è quella di avere con se meno "cose" possibili. Aumentando il numero di quanto si porta con se, aumenta notevolmente il rischio di perderle, l'accortezza è quella di difendere in qualche modo i contenuti, concentrando l'attenzione sulle nuove tecnologie che consentono di avere in un unico apparato es. cellulare, tutto quello che possibile. Le nuove generazioni di cellulari, ad esempio, hanno una "scheda" di memoria leggibile anche dal PC di diversi Giga, usando questa semplice accortezza si concentra la nostra attenzione su un solo apparato. In questo modo diminuisce drasticamente la possibilità di perdita ad es. del cellulare, concentrando le proprie attenzioni allo stesso mettendolo in sicurezza.

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

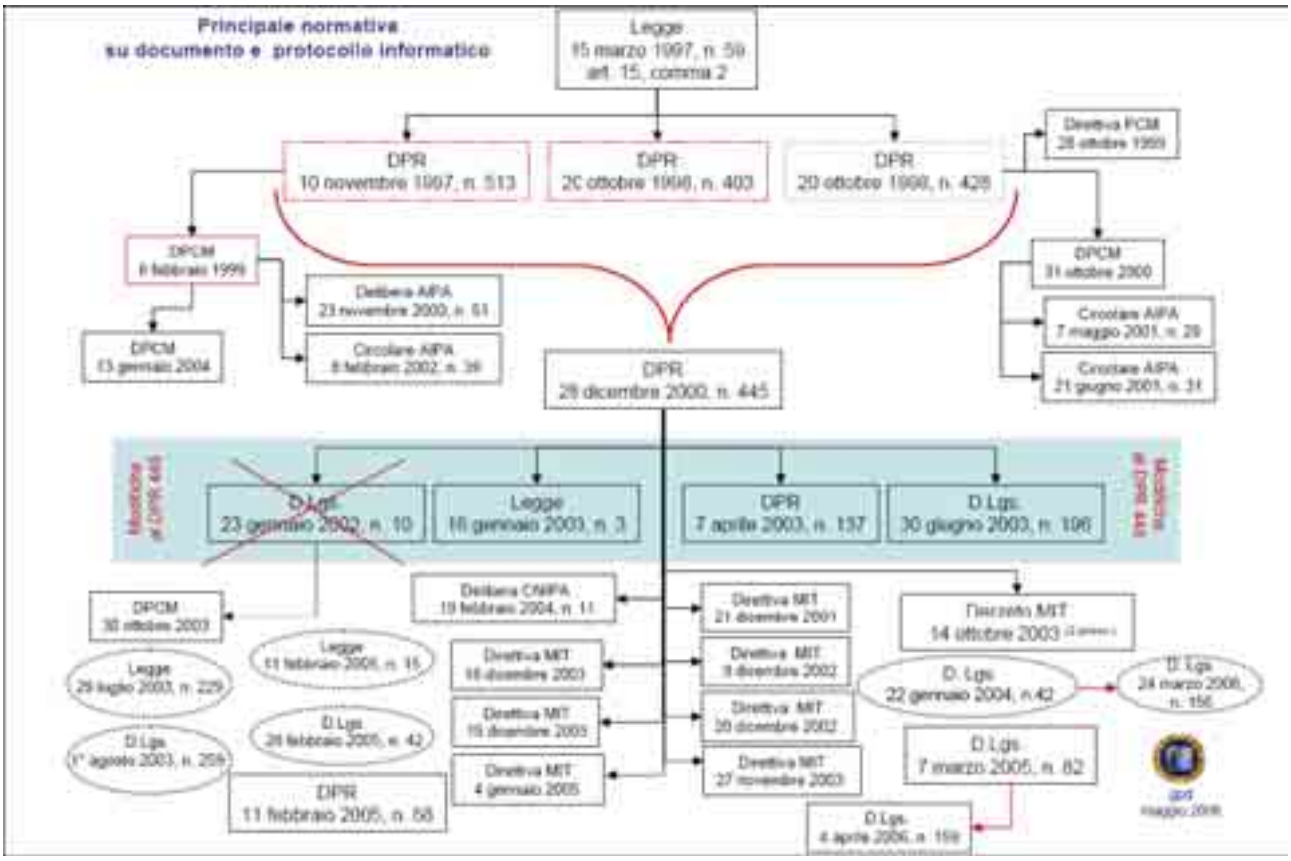
ASPETTI GIURIDICI E DI COMPLIANCE

L'annoso problema degli aspetti giuridici e di "compliance" con la PEC il CAD, la privacy e le direttive comunitarie relative vengono qui approfonditi dall'Avv. Nicola Fabiano www.studiolegalefabiano.it.

PREMESSE

L'invio attraverso sistemi di trasmissione dati qualsiasi essi siano include anche sistemi di Posta elettronica che nel loro ciclo vitale comprende anche la archiviazione dei documenti detta ora conservazione sostitutiva od anche dematerializzazione termine orribile; questo complesso sistema si sta cercando di regolare in qualche modo con molta difficoltà in Italia dal lontano 1997 dove da un semplice comma della legge detta Bassanini si è generato un "mostro" di leggi e regolamenti unico al mondo per incomprensibilità e complicazione il non esaustivo schema seguente ne dà una pallida visione, lo abbiamo reso interattivo per tutti coloro che vogliano approfondire l'argomento.

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it



A tutto questo si debbono aggiungere le normative sulla Privacy influenti su tutti questi processi, in sostanza si cerca di regolamentare i flussi documentali di qualsiasi genere trasmessi ed archiviati elettronicamente.

Contributo giuridico dell'Avv. Nicola Fabiano ex Presidente di Cittadini di Internet

http://www.studiolegalefabiano.it www.cittadininternet.org

Da questa ultima Versione della nostra Best Practice abbiamo ritenuto doveroso inserire un contributo giuridico per tutti coloro che vogliano approfondire l'argomento.

Nicola Fabiano

La posta elettronica certificata: qual è la reale portata giuridica?

(contributo pubblicato su www.altalex.it il 25/03/2008)

La posta elettronica certificata, meglio nota come P.E.C., ha la sua fonte normativa nel D.P.R. 11/2/2005, n. 68 intitolato "*Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3*".

L'analisi di tale testo normativo nell'attuale contesto tecnico e normativo consente alcune osservazioni.

Aspetti normativi – La disciplina della PEC è stata adottata con DPR, ai sensi dell'art. 17, comma 2, L. 400/88, così come si evince dal preambolo del provvedimento normativo. L'art. 17, comma 2, L. 400/88 recita: "*Con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei Ministri, sentito il Consiglio di Stato, sono emanati i regolamenti per la disciplina di materie, non coperte da riserva assoluta di legge prevista dalla Costituzione, per le quali le leggi*

della Repubblica, autorizzando l'esercizio della potestà regolamentare del Governo, determinano le norme generali regolatrici della materia e dispongono l'abrogazione delle norme vigenti, con effetto dall'entrata in vigore delle norme regolamentari".

Orbene, l'esame di tale disposizione non lascia dubbi: i regolamenti sono idonei a sostituire, mediante abrogazione dalla loro entrata in vigore, una esistente fonte legislativa primaria. Questo presupposto costituisce il carattere distintivo dei regolamenti governativi o presidenziali definiti, sul piano oggettivo, "autorizzati" o "di delegificazione" rispetto a quelli denominati "indipendenti" che sono, invece, disciplinati dall'art. 17, comma 1, lett. c) L. 400/88. Non è questa la sede opportuna per disquisire sugli aspetti giuridici della gerarchia delle fonti, ove una fonte secondaria sia o non idonea ad abrogare quella primaria, tuttavia è necessario che l'emanando regolamento – ai sensi del comma 2 del citato art. 17 – abbia come presupposto la sussistenza di una fonte legislativa primaria da sostituire. Si tratta di una figura di "delegificazione" che ha avuto corso proprio con la legge Bassanini (L. 59/97).

Ciò posto, nell'ipotesi della PEC, il DPR 68/2005 avrebbe, dunque, dovuto sostituire una fonte legislativa primaria che già disciplinava la materia della posta elettronica certificata. Purtroppo, però, la PEC è stata introdotta ed istituita proprio con il DPR 68/2005 in quanto non esisteva prima di tale provvedimento normativo alcuna disciplina della posta elettronica certificata.

Ma qual era lo scenario normativo esistente al momento in cui veniva emanato il DPR 68/2005 ?

La legge di riferimento era la n. 59/1997 che all'art. 15, comma 2, disponeva "*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*".

La direttiva comunitaria n. 93/99/CE veniva recepita con D.Lgs. n. 10/2002 e disciplinava, fra l'altro, la firma elettronica avanzata.

Altra norma menzionata nel preambolo del DPR 68/2005 è l'art. 27, comma 8 lett. e), della legge n. 3/2003 che recita: "*Entro un anno dalla data di entrata in vigore della presente legge sono emanati uno o più regolamenti, ai sensi dell'articolo 117, sesto comma, della Costituzione e dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, per introdurre nella disciplina vigente le norme necessarie ai fini del conseguimento dei seguenti obiettivi: ... e) estensione dell'uso della posta elettronica nell'ambito delle pubbliche amministrazioni e dei rapporti tra pubbliche amministrazioni e privati*". Altra norma era l'art. 14 DPR n. 445/2000 (ora abrogata dal CAD) "*1. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore. 2. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alle disposizioni del presente testo unico e alle regole tecniche di cui agli articoli 8, comma 2 e 9, comma 4, sono opponibili ai terzi. 3. La trasmissione del documento informatico per via telematica, con modalità che assicurino l'avvenuta*

consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge". Tale disposizione, però, non è menzionata nel DPR 68/2005.

La vicenda legislativa denota sicuramente non poca confusione sulla materia.

Il parere del Consiglio di Stato n. 7903 veniva adottato in data 14/6/2004, epoca in cui era ancora in vigore il citato art. 14 del DPR 445/2000 (abrogato in data 7/3/2005 con l'adozione del CAD, pubblicato sulla G.U. del 16/5/2005). Difatti, dal predetto parere, fra l'altro, si legge: "*La modifica delle disposizioni di cui all'art. 14 d.P.R. 28 dicembre 2000, n. 445 (già art. 12 d.P.R. 10 novembre 1997, n. 513), recata dagli artt. 3 e 6 dello schema di regolamento, si configura come specificazione di quanto implicitamente già contenuto nelle proposizioni a suo tempo adottate (v., infatti, il comma 2 dell'art. 12 d.P.R. 10 novembre 1997, n. 513) e, quindi, come svolgimento delle norme di rango primario, per le quali la conoscenza del destinatario si presume se ed in quanto il messaggio sia entrato nell'ambito della sua disponibilità. Analogamente le varie disposizioni sulle certificazioni rilasciate dai gestori in ordine ai vari passaggi della trasmissione trovano la propria giustificazione nel fatto di essere funzionali al principio della validità e rilevanza a tutti gli effetti di legge della trasmissione elettronica di atti e documenti, già sancito dal succitato art. 12 l. n. 513 del 1997.*".

Da quanto innanzi, scaturiscono almeno tre considerazioni: a) nessuna norma ha mai disciplinato l'istituzione della posta elettronica certificata; b) sembra che (così appare dalla lettura del parere del Consiglio di Stato) posta elettronica e PEC siano state considerate come se fossero la medesima cosa (ciò non può essere per gli effetti attribuiti normativamente alla PEC); d) sembra evidente l'errore di carattere normativo circa il tipo di provvedimento adottato per disciplinare l'uso (?) della posta elettronica certificata.

Sembrerebbe che si sia voluto creare un nuovo strumento comunicativo che, fondato sulla posta elettronica, fornisse maggiori garanzie legali circa la certezza della trasmissione e della ricezione dei messaggi. In sostanza, la PEC costituisce (per gli effetti legali che il legislatore ha voluto attribuire) un sistema di comunicazione diverso ed alternativo rispetto alla posta raccomandata (anche a.r.). Pertanto, la PEC non può essere identificato con la posta elettronica *sic et simpliciter* ed avrebbe dovuto essere istituito con legge.

Questo era il panorama legislativo ante CAD (D.Lgs. n. 82/2005). Il codice dell'amministrazione digitale, invece, prevede la PEC in due soli articoli: all'art. 6 e all'art. 47. La prima delle due norme dispone l'utilizzo della PEC per la PA, mentre il secondo si riferisce alla trasmissione dei documenti tra le pubbliche amministrazioni. Il risultato, comunque, non cambia poiché il CAD nulla aggiunge o modifica.

La materia oggetto della disciplina - Il titolo del citato DPR si riferisce alle "disposizioni per l'utilizzo della posta elettronica certificata". Le disposizioni contenute nel DPR in questione, quindi, riguardano soltanto le norme di utilizzo della posta elettronica certificata, ovvero una sorta di regole operative destinate a disciplinare il concreto utilizzo di tale strumento. Resta, pertanto,

legittimo nel giurista il dubbio circa la portata giuridica di tale provvedimento che, così come predisposto ed accompagnato da altro Decreto del Presidente del Consiglio dei Ministri emanato ai sensi dell'art. 17, sembra assumere l'identità di un breve manuale operativo. Del resto, questo era il rischio paventato dal Consiglio di Stato con il parere n. 7903 del 2004.

In definitiva, se con il DPR in questione si è voluto introdurre nel nostro ordinamento un sistema di posta elettronica più sicuro di quello comunemente utilizzato, probabilmente sarebbe stato necessario istituire preventivamente con legge (e non con DPR) il nuovo sistema di comunicazione e successivamente stabilire le regole tecnico-operative; il legislatore, invece, ha deciso di utilizzare direttamente il metodo regolamentare per disciplinare l'"utilizzo" di un sistema (la p.e.c.) al quale viene attribuita validità "agli effetti di legge" della trasmissione dei messaggi prima, però, che giuridicamente la stessa posta elettronica certificata sia stata effettivamente istituita quale ulteriore mezzo di comunicazione. Probabilmente sussiste qualche errore di normazione che va ad incidere sulla gerarchia delle fonti normative.

Raccordo con le norme comunitarie - Restando sul piano delle fonti normative, la confusione non è poca. Difatti, la direttiva comunitaria n. 93/99 individua soltanto due tipi di firma elettronica: *a)* la firma elettronica (art. 2, n. 1) e *b)* la firma elettronica avanzata (art. 2, n. 2). Detta direttiva è stata recepita nel nostro ordinamento con il D.Lgs. n. 10/2002 ma quest'ultimo provvedimento è stato abrogato con l'avvento del codice dell'amministrazione digitale. Tuttavia, lo stesso CAD menziona agli art. 6 e 47 la posta elettronica certificata creando così una grossa contraddizione. In questo processo di evoluzione normativa sono cambiate le firme elettroniche: il CAD (D.Lgs. n. 82/2005) ha aggiunto alla sola firma elettronica la firma elettronica qualificata e la firma digitale. Attualmente, quindi, secondo le disposizioni vigenti (solo il CAD) esistono tre firme tra cui non è contemplata quella elettronica avanzata.

Tuttavia, il DPR che disciplina la posta elettronica certificata (*rectius* l'utilizzo) all'art. 9, comma 1, dispone che "*le ricevute rilasciate dai gestori di posta elettronica certificata sono sottoscritte dai medesimi mediante una firma elettronica avanzata*" ed al comma 2 che "*la busta di trasporto e' sottoscritta con una firma elettronica di cui al comma 1*". In sostanza, per la validità della posta elettronica certificata – ai sensi dell'art. 4, ultimo comma, – è necessario che i gestori firmino le ricevute (di invio e di consegna) con la firma elettronica avanzata.

Da ciò si rileva che, secondo l'attuale assetto normativo, la validità "agli effetti di legge" della posta elettronica certificata non possa essere riconosciuta in quanto manca nel nostro ordinamento giuridico l'elemento della firma elettronica avanzata. Tale singolare situazione deriva dal risultato di un confuso e disorganico processo di produzione normativa – fatto di abrogazioni e rinvii – del quale è rimasto vittima lo stesso legislatore che, evidentemente, non si è preoccupato di rettificare anche il testo delle norme sulla posta elettronica certificata.

Una situazione del genere sembra che debba essere affrontata secondo i principi giuridici in materia di gerarchia delle fonti, poiché potrebbe soccorrere la direttiva comunitaria n. 93/99 che

contempla proprio la firma elettronica avanzata. Difatti, è noto che un atto amministrativo in contrasto con una norma comunitaria può essere disapplicato in sede giudiziaria. Una simile impostazione, però, introduce nel nostro ordinamento la figura della firma elettronica avanzata, facendo così entrare dalla finestra ciò che è uscito dalla porta. Da ciò ne consegue che il novero delle firme passa da tre a quattro con ogni immaginabile conseguenza.

Nessuna interoperabilità – La PEC non è sicuramente interoperabile, nonostante quanto espressamente disposto dall'art. 5 del DPR in questione. La non interoperabilità si rileva sia a livello interno (ossia in ambito nazionale) tra i diversi gestori, sia a livello internazionale. A livello interno sembra sussistano problemi operativi tra i diversi gestori non unificatisi al medesimo standard; in sostanza un soggetto che è titolare di una PEC con un certo gestore potrebbe avere difficoltà sia nella trasmissione sia nella corretta ricezione di un messaggio email inviato o ricevuto da soggetto dotato anch'esso di PEC ma con altro gestore. In ambito internazionale, poi, la situazione è penosa, poiché negli stati dell'Unione Europea e nei Paesi d'oltreoceano non risulta esistente questo sistema di comunicazione. In tale contesto è evidente l'impossibilità per chi è fuori dall'Italia di interloquire con soggetti italiani mediante la PEC.

Ambito applicativo – L'art. 16, comma 4, recita: "*Le disposizioni di cui al presente regolamento non si applicano all'uso degli strumenti informatici e telematici nel processo civile, nel processo penale, nel processo amministrativo, nel processo tributario e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti, per i quali restano ferme le specifiche disposizioni normative*".

La disposizione appena citata lascia supporre che, per il processo telematico secondo quanto disposto dal DPR 123/2001, le trasmissioni dei documenti avverranno mediante posta elettronica (non certificata) ma con firma elettronica avanzata (?). Da ciò ne consegue che la PEC non sarà sicuramente utile nell'ambito proprio del processo telematico.

Tuttavia, proprio di recente il Ministero della Giustizia con un documento del 14/1/2008, trasmesso dal Consiglio Nazionale Forense ai Presidenti dei Consigli degli Ordini degli Avvocati con nota del 25/2/2008, ha descritto il progetto di organizzazione del processo telematico. Con tale documento si afferma testualmente che "*Sarà previsto l'obbligo per gli avvocati di indicare un indirizzo di posta elettronica certificata e che le comunicazioni agli stessi ed agli ausiliari del giudice vengano effettuate tramite tale mezzo che diverrà lo strumento primario di comunicazione e notificazione*" ed inoltre "*Per il settore civile, ma non solo, è tuttavia indispensabile ottenere anche una convinta e decisa partecipazione degli avvocati, i cui studi dovranno essere al più presto provvisti di una casella postale certificata con relativa firma digitale che comporterà una spesa preventivata per poco più di cento euro per anno per ciascuno studio legale. Tale attrezzatura sarà indispensabile per consentirei il collegamento operativo ed il relativo funzionamento del sistema su cui poggia il PCT*".

Non sembra esserci dubbio che sulla PEC imperversi una grossa confusione.

Le vigenti norme sul PCT escludono l'utilizzo della PEC conservando (ma chissà fino a quando) il riferimento alla firma elettronica avanzata; il Ministero della Giustizia, invece, ritiene di dover imporre agli avvocati l'utilizzo della PEC (che prevede la firma elettronica avanzata) per il PCT.

Al termine di queste brevi osservazioni, una piccola provocazione sul tema importante della sicurezza: il DPR in esame riconosce che la trasmissione e la ricezione siano validi agli effetti di legge al pari di una raccomandata mediante l'utilizzo della firma elettronica avanzata (che non esiste nel nostro ordinamento); la PEC, pertanto, costituisce una busta "sicura" che veicola un messaggio di posta elettronica: quali i risvolti giuridici qualora il messaggio veicolato sia non scritto (come se si spedisse con raccomandata un foglio bianco)?

Qual è la rilevanza giuridica della firma elettronica?

1. Premessa. – Nel nostro sistema civilistico, in via di principio, con la sottoscrizione di un atto un soggetto approva il contenuto dello stesso e completa il confezionamento del documento che viene così formato. Non è questa la sede per disquisire sulla natura unilaterale o bilaterale dell'atto formato, poiché è interessante verificare la natura giuridica della sottoscrizione (firma) e la rilevanza giuridica della stessa in relazione anche al documento informatico.

Il codice civile, ovviamente, conosce soltanto la firma autografa ed attribuisce rilevanza alla sottoscrizione con diverse norme. Chi sottoscrive (o firma) un documento se ne assume la paternità sia con riguardo al contenuto dello stesso sia relativamente al requisito di forma che esso deve rivestire secondo l'ordinamento giuridico.

La sottoscrizione (quella autografa), quindi, assume la propria rilevanza giuridica, tant'è che la mancanza della firma in alcuni casi è causa di nullità (es. art. 606 c.c per il testamento olografo) se non addirittura di inesistenza del documento. Del resto l'art. 2702 c.c. attribuisce rilevanza probatoria piena, fino a querela d falso, alla scrittura privata della provenienza delle dichiarazioni di chi l'ha sottoscritta, salve le ipotesi di disconoscimento della sottoscrizione. Maggior rilevanza giuridica viene poi attribuita alla sottoscrizione autenticata *ex* art. 2703 c.c. In sostanza, a ciascun soggetto è attribuibile in maniera inequivocabile una determinata firma o sottoscrizione autografa. È possibile che ad un soggetto possano essere attribuite più di una firma o sottoscrizione autografa allorquando questi utilizzi sottoscrizioni grafologicamente diverse tra loro. In caso di contestazione della imputazione di una firma o sottoscrizione ad un certo soggetto sarà possibile accertare, anche giudizialmente, mediante prove grafologiche l'appartenenza o non allo stesso soggetto di una determinata firma.

Ciò premesso, è interessante valutare come l'evoluzione tecnologica attraverso l'informatica abbia contribuito ad innovare anche i settori più tradizionali del diritto tra cui proprio quello della sottoscrizione.

2. La normativa vigente. – Il vigente Codice dell'Amministrazione Digitale (per brevità in seguito indicato CAD), a seguito di una corposa ed articolata evoluzione normativa che si è

sviluppata nel corso degli ultimi dieci anni (per ragioni metodologiche non si propone l'*excursus* normativo che è poi sfociato nella vigente normativa), ha sostanzialmente innovato la disciplina sia del valore probatorio del documento informatico sia della firma elettronica (si utilizza questa espressione ma si chiarirà in seguito). Difatti, il Capo II del CAD è titolato "***documento informatico e firme elettroniche; pagamenti, libri e scritture***", ed è diviso in 3 sezioni, di cui la prima disciplina il "***documento informatico***", la seconda "***firme elettroniche e certificatori***", e la terza "***pagamenti, libri e scritture***". Il legislatore al Capo I del CAD, disciplinando i principi generali, fornisce le opportune definizioni, secondo cui si individuano almeno 3 tipologie diverse di firma informatica:

1. **firma elettronica**: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;
2. **firma elettronica qualificata**: la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;
3. **firma digitale**: un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Più specificamente, il CAD disciplina la firma elettronica con gli articoli 24 e 25, sebbene i riferimenti alla firma siano contenuti in diverse norme, tant'è che il termine "firma elettronica" viene utilizzato 20 volte, mentre l'espressione "firma elettronica qualificata" 12 volte e "firma digitale" 23 volte. Rilevante e connesso alla firma è l'argomento del documento elettronico, a cui il CAD riserva gli articoli dal 20 al 23.

Per mera completezza, va rilevato che il D.P.R. 445/2000 all'art. 10 (ora abrogato) prevedeva un altro tipo di firma oltre a quelle su indicate, disciplinando la "**firma elettronica avanzata**". Tuttavia, il legislatore non ha inteso riproporre nel CAD l'ulteriore tipologia di "firma elettronica avanzata", limitando a 3 il novero delle firme informatiche. Secondo alcuni[1] la firma elettronica avanzata dovrebbe intendersi quale sinonimo di firma elettronica qualificata.

Sempre sul piano normativo, non può essere esclusa la Direttiva n. 1999/93/CE che, sebbene recepita con il CAD, continua comunque a mantenere la sua rilevanza sia per i richiami contenuti nel codice, sia in quanto spiega i propri effetti in ambito comunitario, anche per gli aspetti

1 SIROTTI GAUDENZI, voce *Firma elettronica avanzata* in *Glossario di diritto delle nuove tecnologie e dell'e-government*, Milano, 2007, 270

2 SCIALDONE, *Guida al Codice dell'Amministrazione Digitale*, a cura di A. Lisi e L. Giacopuzzi, Halley Editrice, 2006,
3 SCHNEIDER-GERSTING, Informatica (ed. italiana a cura di Gentile-Pirrone), Milano, 2007, 3. Se l'informatica ha ad oggetto dati di rilevanza giuridica viene definita "informatica giuridica"; per le definizioni e la ricostruzione storica dell'informatica giuridica, si rimanda a IASELLI, *Compendio di informatica giuridica*, III Edizione, Simone, 2007, 7.
4 GIUSTOZZI, *Firme digitali e... analogie elettroniche*, in *Interlex*, http://www.interlex.it/docdigit/corrado9.htm
5 GIUSTOZZI, op. ult. cit.
6 Cons. Stato Sez. V, 31-05-2007, n. 2817
7 L'art. 3, comma 1, recita: "*I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni e con i gestori di pubblici servizi statali nei limiti di quanto previsto nel presente codice*"
8 Il comma 2, recita: "Le istanze e le dichiarazioni inviate o compilate su sito secondo le modalità previste dal comma 1 sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento; resta salva la facoltà della pubblica amministrazione di stabilire i casi in cui è necessaria la sottoscrizione mediante la firma digitale".
9 Con riguardo agli aspetti più tecnici, la dottrina rileva come il legislatore abbia optato per i metodi di autenticazione secondo la classificazione fornita dall'Uncitral. Seguendo detta classificazione si afferma che le firme elettroniche si possono "suddividere in tre categorie, a seconda che il meccanismo di autenticazione si basi sulla conoscenza dell'utente, sulle caratteristiche fisiche dell'utente, sul possesso di un oggetto da parte dell'utente" (Maggipinto – Niger, *Documento informatico e firme elettroniche*, in *L@ post@ elettronic@. Profili giuridici e tecnico-informatici*, Roma, 2007, 53).
10 sul punto, v. CAMMARATA - MACCARONE, *Troppe "firme" nell'attuazione della direttiva*, in *Interlex*, http://www.interlex.it/docdigit/nuovoreg.htm
11 SCORZA, *Commento all'art. 1*, in Cassano-Giurdanella, *Il codice della Pubblica Amministrazione digitale. Commentario al D.Lgs. 82/2005*, Milano, 2005, 10
12 Cons. Stato, Sez. consult., parere del 7/2/2005, in *Giur. It.*, 2005, 1163
13 SCORZA, op. cit., 8
14 SIROTTI GAUDENZI, voce *Firma elettronica* in *Glossario di diritto delle nuove tecnologie e dell'e-government*, Milano, 2007, 262
15 SIROTTI GAUDENZI, voce *Firma elettronica qualificata*, op. cit., 272
16 Autorevole dottrina fornisce la seguente definizione di firma digitale: "non è poi una vera «firma», ma più correttamente un sistema di accertamento della titolarità di un documento elettronico basato su presunzioni giuridiche fondate su un sistema tecnico tendenzialmente sicuro" (BORRUSO-CIACCI, *Diritto civile e informatica*, Napoli, 2004, 416)
17 In BORRUSO-CIACCI, op. cit., 453, si afferma che "Le nuove firme, infatti, da un punto di vista ontologico, non hanno nulla a che vedere con una firma in senso tradizionale, non riproducono il nome e il cognome di nessuno, non sono parole, né disegni, non hanno, quindi, nulla a che vedere con l'autografia e neppure con la grafia […] Se proprio si vuole trovare una analogia col passato, si può dire che la firma digitale o elettronica è più simile ad un sigillo (di metallo o di cera-lacca) che non ad una firma".
18 La finzione è definita come il "risultato di un processo mentale che, in quanto immaginato o inventato, non corrisponda puntualmente ad una specifica realtà" (S. PUGLIATTI, voce *Finzione*, in *Enc. dir.*, XVII, Milano 1968, p. 658
19 Nello stesso senso è parte della dottrina (CUNIBERTI, *Email, firma elettronica e forma scritta*, in Filodiritto, http://www.filodiritto.com/diritto/privato/informaticagiuridica/emailcuniberti.htm), secondo cui "Ora, poiché appare ovvio che la definizione "sottoscrizione" costituisca, per quel che riguarda un documento informatico - e quindi la rappresentazione grafica di dati - una fictio juris (in quanto in nessun caso si sottoscrive materialmente alcunché, neppure con la firma digitale, che corrisponde invece all'inserimento, da parte di qualcuno - quasi sempre diverso dall'effettivo titolare - di una smart card e della digitazione di un PIN, che non viene certo riportato nella mail), sembra logico che l'espressione "documento informatico sottoscritto con firma elettronica" possa anche esser interpretata con "firma elettronica apposta (o allegata) al documento informatico".
20 Nel vigore del D.P.R. 445/2000, ma con espresso riferimento al documento informatico, autorevole dottrina aveva sostenuto che "il sistema di firma digitale introdotto nel nostro paese può essere considerato una fattispecie a formazione progressiva" (BORRUSO-CIACCI, op. cit., 391.
21 Parte della dottrina ritiene che vi sia un errore terminologico derivante dall'espressione inglese mal tradotta in italiano, in quanto la firma svolge funzione di validazione dei dati. Si afferma appunto che "l'autenticazione informatica non esiste: "con la firma elettronica "debole"può esistere solo la validazione informatica dei dati" (MANNO, *La firma elettronica non serve per l'identificazione*, in *Interlex*, http://www.interlex.it/docdigit/r_manno16.htm); altra dottrina, evidenzia come firmare non equivale a sottoscrivere (NEIROTTI, *Firmare elettronicamente non sempre equivale a sottoscrivere*, in *Interlex*, http://www.interlex.it/forum10/relazioni/28neirotti.htm)
22 CAMMARATA, *Attenzione: sono tutte firme "digitali"*, in Interlex, http://www.interlex.it/docdigit/nuovoreg2.htm
23 Il Consiglio Nazionale del Notariato (CNN) con lo studio n. 2-2006/IG ha rilevato come la firma autografa e quella digitale spieghino gli stessi effetti proprio sul piano delle funzioni che, però, vengono limitate alle sole indicativa e dichiarativa. A parere di chi scrive, invece, è condivisa anche la funzione probatoria.
24 In dottrina si è parlato di "identità informatica" (SCORZA, op. cit., 11).
25 In dottrina, v. SIROTTI GAUDENZI, voce *Certificatore* in Glossario op. cit., 102
26 Art. 3 della Direttiva 1999/93/CE
27 Si riportano i commi 6-7-8 dell'art. 29 CAD: "6. A seguito dell'accoglimento della domanda, il CNIPA dispone l'iscrizione del richiedente in un apposito elenco pubblico, tenuto dal CNIPA stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione. 7. Il certificatore accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni. 8. Sono equiparati ai certificatori accreditati ai sensi del presente articolo i certificatori accreditati in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE".

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

connessi alle certificazioni ed ai Certificatori. La Direttiva citata, inoltre, acquisisce rilevanza anche come riferimento ermeneutico per la normativa nazionale.

La dottrina ha proposto una definizione di firma elettronica come "il concetto di firma elettronica è tuttavia molto ampio e include tutte le tecniche utilizzate per identificare una persona in ambiente elettronico e può essere espresso nei seguenti termini: la firma elettronica consiste in qualsiasi marcatura elettronica che indichi l'identità di un soggetto da considerarsi firmatario del documento. [...] La differenza fondamentale che intercorre tra le diverse tipologie di firma elettronica è rappresentata, oltre che dalla tecnologia utilizzata, anche dalla loro maggiore o minore capacità di assicurare la presenza di tutti gli elementi richiesti per garantire la manifestazione di volontà da parte del soggetto firmatario, nonché l'integrità e l' immodificabilità del documento così firmato. Allo stato attuale, la soluzione tecnica in grado di garantire maggiormente la presenza degli elementi da ultimo richiamati è rappresentata dalla firma digitale"[2].

Rilevano gli aspetti terminologici ? I titoli delle prime due sezioni del Capo II del CAD si esprimono in termini di documento "informatico" e di firma "elettronica". A parere di chi scrive sembrerebbe più corretto parlare di firma informatica, piuttosto che di firma elettronica. Tale orientamento, peraltro, sembra supportato dallo stesso dato testuale che identifica il documento come informatico e non, invece, come elettronico. Il legislatore avrebbe potuto definire il documento elettronico, piuttosto che qualificarlo come "informatico". In realtà l'aggettivo "informatico" non va inteso con il senso qualificativo del termine che lo precede ma deve essere letto per indicare il "modus" con cui si forma il citato documento. In sostanza, sembra che la migliore lettura dell'espressione in questione sia di "documento [formato con mezzo (o strumento)] informatico". Tuttavia, posto che il documento viene ad essere realizzato mediante l'utilizzo di un computer sembra, appunto, più idoneo che sia definito – come effettivamente ha fatto il legislatore con il CAD – "informatico" e non elettronico. Difatti, poiché l'informatica è definita come :"lo studio degli algoritmi"[3], nel contesto normativo non avrebbe molto senso qualificare il documento come "quello che ha attributi algoritmici". Queste brevi argomentazioni traslate sul piano della firma lasciano supporre che fosse stato meglio definire la firma come informatica e non, invece, elettronica. L'elettronica, infatti, "è proprio un'altra cosa: è, semplicemente, la tecnica che

28 MANCA (Responsabile Ufficio Standard architetture e metodologie, CNIPA), *Nuove tecnologie per l'interoperabilità del documento informatico*, http://www.cnipa.gov.it/site/itIT/La_Documentazione/Taccuino_tecnico/Documenti/Nuove_tecnologie_interoperab_doc_info.html) ha affermato che "Attenendosi alle definizioni e a quanto stabilito dal Codice è indispensabile stabilire regole tecniche che garantiscano l'interoperabilità nello scambio dei documenti informatici e in particolare garantiscano regole per il riconoscimento e la verifica delle firme digitali utilizzate per la sottoscrizione dei documenti informatici".

29 Nello stesso senso, LISI, *I processi di certificazione nella sottoscrizione del documento informatico, nella trasmissione dei messaggi di posta elettronica e nei processi di negoziazione telematica*, http://www.scintlex.it/documenti/certificazione%20elettronica, il quale afferma che "l'interoperabilità e la "usability" di tali strumenti a volte lascia un po' a desiderare e, soprattutto per quanto riguarda la PEC, essa – così come configurata dalla normativa italiana – è inutilizzabile a livello internazionale.

30 in questi termini, BENDANDI, *La posta elettronica: parte tecnico-informatica*, in L@ post@ alettronic@., cit., 273.

31 SCORZA, *Commento all'art. 20*, op. cit., 181.

32 Parte della dottrina ritiene che anche la rescissione rientri nella invalidità (BIANCA, *Il contratto*, 3, Milano, 1987, 574)

33 IRTI, op. cit., 61.

consiste nel manipolare fasci di *elettroni* in movimento lungo percorsi conduttori per ottenere una determinata funzionalità. L'elettronica, con la sua parente povera l'elettrotecnica, esistono come discipline rigorose dai primi anni del secolo scorso, ma come curiosità ed oggetto di studi scientifici sin dal 1700"[4]. Senza alcuna velleità tecnica (il cui campo lo si lascia aperto agli addetti ai lavori) e né tanto meno di purista della lingua, il comune senso logico farebbe pensare che se si utilizzasse il termine elettronico con funzioni di aggettivo si qualificherebbe la firma come costituita "tecnicamente da un fascio di elettroni", mentre ad una firma creata con strumenti elettronici sarebbe meglio sostituire quella creata con strumenti informatici. Pertanto, a parere di chi scrive, sembrerebbe opportuno che, per poter individuare la tipologia della firma apposta con l'ausilio di strumenti informatici, si parli più propriamente di firma "informatica"; diversamente, con la connotazione terminologica di "firma elettronica" si finirebbe nell'errato circolo vizioso del rapporto tra *genus* e *species* per riferirsi esclusivamente a due dei 3 tipi disciplinati dal CAD. Per completare il quadro terminologico, soltanto per dovere di completezza (sia pure sommaria e non approfondita sul punto), con riguardo al termine "digitale" la dottrina ha chiarito che «nel mondo della tecnica il termine "digitale" significa semplicemente "numerico", e si applica ad ogni grandezza fisica che venga rappresentata con un suo esatto equivalente numerico e non con una rappresentazione "continua" quale l'ago di un quadrante o il livello di un galleggiante. In italiano potremmo tranquillamente definire *numerico* tutto ciò che oggi, prendendo a prestito un termine inglese, definiamo *digitale*: ma l'esterofilia e la pigrizia ce lo impediscono [...] non ha senso sostituire il termine "digitale" con quello "elettronico", o viceversa, pensando di dire quasi la stessa cosa. Oltretutto è sbagliata anche la direzione di pensiero del legislatore: mentre infatti "digitale" è un termine di amplissima generalità, non essendo legato ad alcuna particolare tecnologia esistente o da sviluppare, e descrive dunque la *modalità* con cui i dati verranno codificati (e c'è da presumere che anche in futuro la codifica d'elezione sarà quella digitale, in quanto ricchissima di proprietà utili), viceversa il termine "elettronico" è estremamente specifico e specializzato, in quanto si riferisce ad una ben precisa tecnologia (quella degli elettroni) che molto probabilmente sarà soppiantata in futuro con qualcosa di più efficiente (diciamo i fotoni, tanto per rimanere nell'ambito della fisica atomica, ma l'elenco potrebbe essere più ampio)»[5].

Al di là di questo preliminare rilievo terminologico, è opportuno capire che cosa debba intendersi per firma elettronica e le definizioni sono contenute nello stesso CAD..

3. Esiste una natura giuridica della firma elettronica ? Una fattispecie a formazione progressiva. – Ciò che interessa ai fini di queste brevi note è la firma elettronica e la sua connessione con il documento informatico e con la rilevanza giuridica di quest'ultimo. È opportuno preliminarmente chiarire gli aspetti precipui della firma autografa e dei suoi effetti con riguardo al documento o atto cartaceo. Al di là dell'avvento dell'era digitale, l'ordinamento giuridico continua ad attribuire piena rilevanza giuridica alla firma autografa, quanto meno per le sue funzioni essenziali (indicativa, dichiarativa e probatoria) poiché essa costituisce il criterio univoco per presumere – fino al suo disconoscimento – che un atto o un documento sia imputabile, quanto alla paternità ed agli effetti, al soggetto che ne ha apposto la sottoscrizione. È interessante, sulla

qualificazione della firma, parte della motivazione di una recente pronuncia del Consiglio di Stato, secondo cui: "*Nessuna norma generale definisce in modo più preciso i caratteri della "firma" o della sottoscrizione rilevante nella redazione di atti pubblici o di documenti privati. 28. La sottoscrizione, in senso tradizionale, è considerata l'insieme dei segni grafici ed autografi idonei a riferire un determinato documento ad un distinto soggetto, il quale, mediante l'apposizione di tali segni grafici, se ne assume la paternità. 29. In analoga prospettiva dottrinaria, la firma deve evidenziare un proprio significato obiettivo, qualificandosi come segno autografo mediante il quale il soggetto fa proprio il contenuto di un testo. 30. Secondo la dottrina, quindi, la sottoscrizione svolge tre funzioni essenziali: indicativa (mira a individuare l'autore del documento), dichiarativa (comporta l'assunzione di paternità dell'atto) e probatoria (definisce l'autenticità del documento). 31. Per assolvere a queste tre funzioni, alla sottoscrizione sono spesso associate tre caratteristiche essenziali: l'autografia, la nominatività e la leggibilità. 32. Secondo la prevalente dottrina, poi, il carattere dell'autografia importa che debbano essere usati mezzi i quali rivelino il movimento grafico della mano (anche a caratteri stampatelli), con la sola esclusione di mezzi meccanici di qualsiasi tipo*"[6].

Premesse queste brevi considerazioni in ordine alla firma autografa, il progresso tecnologico ha fatto sì che il computer e l'informatica siano parte della attuale società dell'informazione. Il legislatore, ben consapevole di tale evoluzione ha disciplinato la materia della firma elettronica e del documento informatico in modo da rendere più aderente alla realtà attuale l'uso delle tecnologie. L'accesso alle firme elettroniche e l'utilizzo delle stesse non è riservata soltanto ai rapporti tra gli Uffici della P.A. e tra essa e i cittadini, ma la firma elettronica stessa può essere legalmente liberamente utilizzata anche dai soggetti privati. Difatti, l'art. 2, comma 3, CAD recita: "*le disposizioni di cui al capo II concernenti i documenti informatici, le firme elettroniche, i pagamenti informatici, i libri e le scritture, le disposizioni di cui al capo III, relative alla formazione, gestione, alla conservazione, nonché le disposizioni di cui al capo IV relative alla trasmissione dei documenti informatici si applicano anche ai privati ai sensi dell'articolo 3 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445*". Non a caso, poi, l'art. 3, comma 1, CAD[7] riconosce proprio un diritto all'uso delle tecnologie per coloro che intendono avere rapporti con la P.A.

Il legislatore non ha trascurato la rilevanza della firma autografa, poiché l'art. 65, comma 2, CAD[8] sancisce l'equivalenza giuridica della firma digitale alla firma autografa, nell'ipotesi di istanze e dichiarazioni presentate alla P.A. per via telematica. L'equiparazione normativa della firma autografa alla firma digitale (quella "sicura", cioè creata con sistemi tecnico-informatici tali da garantire un elevato livello di sicurezza)[9] consente di imputare l'istanza e/o la dichiarazione univocamente al soggetto che esegue l'operazione telematica. Occorre, quindi, chiedersi se il legislatore, nel CAD, abbia relegato o non la firma digitale (equiparata alla firma autografa) a *species* del più ampio *genus* della firma elettronica qualificata.

Una triplice configurazione di firme elettroniche (sino a qualche tempo le firme erano ben quattro)

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

non c'è dubbio che disorienti, con il rischio di fuorviare l'interprete. Del resto, questi argomenti sono ben noti alla dottrina che da tempo ha denunciato l'eccessivo ed inutile numero di tipologie di firma elettronica[10]. Altra dottrina, esprimendosi in maniera ancora più esplicita, ha evidenziato come nel "sovraffollamento di firme nel nuovo contesto normativo" il legislatore "abbia finito con il fare confusione tra firme elettroniche e firme digitali"[11].

Una lettura superficiale delle definizioni di firma fornite dal CAD potrebbe condurre alla illazione secondo cui il legislatore ha voluto creare due diversi *genus* di firma elettronica, e precisamente la "firma elettronica" e la "firma elettronica qualificata"; la firma digitale (definita come "un particolare tipo di firma elettronica qualificata"), poi, aumenta il sospetto (infondato) che si sia voluto creare una *species* per appartenenza al più ampio *genus* della firma elettronica qualificata. I sospetti, in realtà, sono connessi con il parere del Consiglio di Stato in sede consultiva con il parere 11995/04 del 7/2/2005 ove si legge "*la firma digitale, come risulta dalla definizione e come può dedursi dagli effetti, anche probatori, previsti dagli articoli 17 e 18, è peraltro una specie della firma elettronica qualificata (definita "elettronica avanzata" dalla direttiva comunitaria). Sembra quindi inopportuna la distinzione apparente in tre diverse specie di firma e, se deve essere apprezzata la riduzione a tre delle ipotesi di firma (sono quattro nell'attuale d.P.R. n. 445 del 2000), sarebbe opportuno un ulteriore chiarimento, nel senso che i tipi di firma sono solo due, la firma elettronica pura e semplice e quella qualificata, di cui la firma digitale è un tipo*"[12]. Il Consiglio di Stato, quindi, suggeriva al legislatore di semplificare la qualificazione delle firme elettroniche (genericamente intese), ma tale input non ha avuto alcun esito.

In realtà, si tratta di una impostazione assolutamente fuorviante. Non è giuridicamente corretto classificare in termini di *genus* e *species* le firme elettroniche (in particolare quella elettronica qualificata e quella digitale). Le diverse definizioni prospettate dal CAD che configura un rapporto di subordinazione della firma digitale rispetto a quella elettronica qualificata hanno una valenza puramente tecnica e non giuridica.

La dottrina che si è occupata *ex professo* della materia in questione ha fatto rilevare che "sotto un profilo squisitamente informatico - giuridico l'unica dicotomia esistente è tra firma elettronica debole e firma elettronica forte", posto che "le firme elettroniche qualificate e le firme digitali producono gli stessi effetti giuridici essendo le seconde [...] solo ed esclusivamente una sotto-categoria tecnico-informatica delle prime"[13]. Sostanzialmente negli stessi termini si pone chi[14], più di recente, manifesta il proprio contrario orientamento rispetto a quanto indicato dal Consiglio di Stato nel parere su citato, poiché – si afferma – l'espressione "firma elettronica" non va confusa con la "firma debole" essendo necessaria una lettura sistematica della materia che tenga conto anche delle disposizioni di fonte comunitaria (ed il riferimento è ovviamente alla Direttiva 1999/93/CE). Pertanto, tale dottrina ritiene che alla firma elettronica debba essere attribuito lo stesso "valore" riconosciuto alle "firme sicure", manifestando perplessità in ordine alla "apparente presenza [...] all'interno del Codice, di due diverse firme sicure". Ad ogni modo, oggi si assiste alla difficoltà di rinvenire una "firma elettronica qualificata diversa dalla firma digitale"[15].

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

Le perplessità e le incertezze in ordine alla qualificazione giuridica delle firme elettroniche derivano sostanzialmente dalla non corretta definizione del procedimento tecnico-informatico mediante il quale si distinguono le firme c.d. "deboli" o "meno sicure" dalle firme c.d. "sicure o "forti" o "pesanti" (il riferimento è alla firma elettronica qualificata ed alla firma digitale[16]). A parere di chi scrive bisogna distinguere tra la firma elettronica in sé e i suoi effetti. Ciò che rileva giuridicamente sono gli effetti, non potendo forzatamente riconoscere gli attributi giuridici a ciò che non lo è. La firma elettronica in sé considerata rileva sotto il profilo squisitamente tecnico che, coniugato con gli effetti che la legge ad essa attribuisce, confluisce nell'ordinamento giuridico assumendone rilevanza. Non esiste una ontologica giuridicità della firma digitale[17] e né si può obbligatoriamente riconoscerla; si tratta di una *fictio iuris*[18], poiché la legge riconosce che le istanze e le dichiarazioni prodotte con firma digitale sono equivalenti a quelle a cui è stata apposta la firma autografa[19]. La firma elettronica costituisce una fase di una fattispecie a formazione progressiva[20] che si completerà e spiegherà gli effetti giuridici previsti dalla legge soltanto a seguito dell'ulteriore procedimento di identificazione dell'utente da parte del certificatore, della creazione e del rilascio dei certificati digitali. Non a caso, a documento informatico è riconosciuta rilevanza giuridica nel nostro ordinamento anche in assenza della firma (elettronica, qualificata o digitale). La firma elettronica in sé e per sé ha solo ed esclusivamente rilevanza sul piano tecnico per le sue precipue caratteristiche[21].

Del resto, non a caso la dottrina ha affermato che "sul piano tecnico e allo stato dell'arte, le firme elettroniche previste dalla direttiva sono firme digitali in tutto e per tutto: la differenza è negli effetti sul piano giuridico e deriva dai diversi livelli di "certezza" assicurati dalla qualità dei certificatori e delle procedure"[22]. Non è ipotizzabile, neppure in termini di *fictio iuris*, attribuire alla firma elettronica (debole o forte) i caratteri propri della firma autografa (che è l'insieme dei segni grafici ed autografi idonei a riferire un determinato documento ad un distinto soggetto) poiché quest'ultima si esaurisce in un unico procedimento grafico senza necessità di alcun ulteriore accorgimento. Tuttavia, tra firma elettronica e firma autografa coincidono le funzioni essenziali (indicativa, dichiarativa e probatoria)[23] e proprio su questi caratteri il legislatore ha equiparato la firma digitale alla firma autografa (art. 65, comma 2). Gli effetti del documento informatico supportano quanto sostenuto.

3.1. I certificati ed i certificatori. – Il CAD definisce i certificati ed i certificatori come segue:

- **certificati elettronici**: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche;
- **certificato qualificato**: il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciato da certificatori che risponde ai requisiti di cui all'allegato II della medesima direttiva;
- **certificatore**: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

Anche per quanto concerne i certificati (elettronico e qualificato) vale quanto già detto in ordine alle firme. Sinteticamente, si tratta di una classificazione puramente tecnica priva di significati ontologicamente giuridici. È evidente, quindi, che il certificato costituisce – come già affermato – l'ulteriore elemento tecnico attraverso il quale si perfeziona il procedimento di firma; il certificato funge da collettore tra i dati e l'identità del titolare del certificato stesso[24].

Il certificatore in Italia viene qualificato diversamente rispetto ad altri paesi (ad es. gli Stai Uniti) dove è identificato come "*Certification Authority*"[25]. In Italia, tuttavia, i certificatori non rivestono il ruolo di Autorità di certificazione; l'art. 26, comma 3, individua due tipologie di certificatori che sono "i certificatori qualificati" e "i certificatori accreditati", ove questi ultimi rientrano – ai sensi dell'art. 29, comma 1, CAD – tra coloro che "*intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza*" e possono "*qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni*" (art. 29, comma 7, CAD). Ai certificatori qualificati – che rilasciano certificati qualificati secondo le disposizioni degli allegati alla direttiva 1999/93/CE – è riservata la disciplina contenuta nell'art. 27 CAD che descrive quali siano i requisiti da possedere.

Pertanto – così come già rilevato – è evidente che la normativa nazionale debba essere armonizzata con quella comunitaria e, in *subiecta materia*, specificamente con la direttiva 1999/93/CE. Per quanto concerne, in particolare i certificatori accreditati, l'art. 29, comma 8, CAD dispone: "*sono equiparati ai certificatori accreditati ai sensi del presente articolo i certificatori accreditati in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE*". In sostanza, al di là dell'elenco nazionale dei certificatori accreditati alla cui tenuta e pubblicazione provvede il CNIPA, va tenuto conto anche di quei certificatori già accreditati in altri Stati membri ai quali, per tale ruolo, viene attribuita la medesima rilevanza giuridica in ambito nazionale. L'attuale assetto normativo sul punto si manifesta, indubbiamente, poco chiaro con il rischio di pregiudicare i certificatori accreditati in altri paesi. In particolare, in ossequio a quanto disposto dalla citata e ben nota direttiva[26] che demanda ad singolo stato membro l'istituzione di un sistema appropriato di supervisione, il CAD prevede l'iscrizione del certificatore che faccia richiesta di accreditamento in un elenco pubblico la cui gestione è riservata al CNIPA[27]. Pertanto, nell'ipotesi (frequente) in cui venga indetta una gara pubblica c'è il rischio (fondato) che il certificatore accreditato in altro Stato membro dell'UE possa essere illegittimamente escluso in quanto non risulta presente nel citato elenco. L'esclusione, si è detto, è illegittima poiché è sufficiente documentare l'iscrizione nell'elenco presso altro paese dell'UE. Tuttavia, ciò potrà comportare un aumento dei tempi di gestione della gara con evidenti pregiudizi sia per chi ha indetto la gara sia per il certificatore illegittimamente escluso (e quasi sicuramente riammesso). Lo stesso, ovviamente, può accadere in occasione di una gara indetta in altro Stato. Sarebbe, quindi, auspicabile l'istituzione di un elenco pubblico dei certificatori accreditati su base internazionale o quanto meno comunitaria.

Altro aspetto importante è quello della interoperabilità. La ben nota Direttiva al punto 5) dei

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

considerando recita: "*occorrerebbe promuovere l'interoperabilità dei prodotti di firma elettronica; a norma dell'articolo 14 del trattato, il mercato interno comporta uno spazio senza frontiere interne, nel quale è assicurata la libera circolazione delle merci; per garantire la libera circolazione nell'ambito del mercato interno e infondere fiducia nelle firme elettroniche, è necessaria la conformità ai requisiti essenziali specifici relativi ai prodotti di firma elettronica, fatti salvi il regolamento (CE) n. 3381/94 del Consiglio, del 19 dicembre 1994, che istituisce un regime comunitario di controllo delle esportazioni di beni a duplice uso, e la decisione 94/942/PESC del Consiglio del 19 dicembre 1994, relativa all'azione comune adottata dal Consiglio riguardante il controllo delle esportazioni di beni a duplice uso*". Inoltre, al punto 23) del considerando recita: "*lo sviluppo del commercio elettronico internazionale rende necessarie soluzioni transfrontaliere che coinvolgano i paesi terzi; al fine di assicurare l'interoperabilità a livello globale, potrebbero essere utili accordi su regole multilaterali con paesi terzi concernenti il riconoscimento reciproco dei servizi di certificazione*".

L'obiettivo della interoperabilità è quello di garantire che cittadini ed amministrazioni di diversi Stati siano in grado di interloquire per canali telematici - elettronici utilizzando per le proprie comunicazioni posta elettronica e firme elettroniche con medesimo protocollo tecnico, di modo che sia garantita l'individuazione dei soggetti mittente/destinatario, l'eventuale codifica dei dati inviati e ricevuti ed alla decodifica degli stessi (qualora si trattasse di firme sicure). In realtà, sebbene sia noto l'impegno del CNIPA[28], ad oggi sembra che l'interoperabilità non sia ancora completamente realizzata, anche poiché i singoli certificatori spesso utilizzano protocolli non del tutto compatibili tra loro[29].

L'auspicio è che con il tempo si pervenga all'utilizzo di protocolli tecnici (attualmente esistenti) che consentano di garantire effettivamente il principio della interoperabilità. È appena il caso di aggiungere che per la sicurezza dei messaggi inviati per mezzo della posta elettronica è sicuramente prevalente e più diffuso l'utilizzo dei protocolli SSL/TSL, ma va precisato che con altro protocollo, definito S/MIME, è possibile ottenere un livello di sicurezza maggiore mediante il quale, oltre alla firme, si può anche criptare il contenuto del messaggio inviato di modo che il destinatario (utilizzando lo stesso protocollo S/MIME) sia in grado di decriptarlo[30].

4. Quale rapporto tra firma e documento informatico ? – Il quadro sin qui esposto viene chiarito con l'analisi delle norme sul documento informatico. Ai fini della presente indagine interessa capire quale rilevanza giuridica assuma la firma (elettronica, qualificata o digitale) in relazione al documento informatico. Il CAD dapprima fornisce la definizione di "documento informatico come "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*". Come si può notare, la definizione di documento informatico non contempla alcun riferimento alla firma. Del resto, anche l'art. 21, comma 1, CAD non contiene alcun riferimento, neppure implicito, alla firma, la quale – invece – viene espressamente menzionata nel successivo comma 2 in ordine al requisito della forma. Tuttavia, sembra utile soffermarsi sulla previsione normativa contenuta

Phone: +39.0761.402802 - Fax: +39.0761.403040 - E-mail: info@globaltrust.it - http://www.globaltrust.it

nell'art. 21, comma 1, del CAD al fine di chiarire in chiave ermeneutica quale sia la rilevanza del documento informativo in sé e se lo stesso abbia una relazione necessaria con la (o meglio con il processo di) firma. Tale norma dispone: "*Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice*". Parte della dottrina[31] ha già espresso ampie perplessità in ordine alla inadeguata formulazione della norma appena menzionata. Un dato è certo: il legislatore si è preoccupato di disciplinare i requisiti di forma e la rilevanza probatoria, per nulla chiarendo la scarna definizione indicata nella premessa del CAD. All''interprete attento, tuttavia, verrebbe da chiedersi quale senso abbia voluto attribuire il legislatore all'espressione "validi e rilevanti". In effetti, la dottrina prevalente[32] si riferisce all'invalidità nelle ipotesi di nullità e di annullabilità del contratto; per cui il concetto di validità va ricavato da quello di invalidità argomentando *a contrariis*. Il primo dato, quindi, è da registrare nel senso che il legislatore ha inteso escludere l'esistenza di ogni presupposto che possa determinare l'invalidità del documento informatico allorquando sussistano le condizioni indicate dal comma 1 dell'art. 20. Ma a ben vedere, le condizioni indicate nel comma 1 dell'art. 20 del CAD, hanno una portata di natura meramente formale; s'immagini un documento informatico formato da un interdetto, oppure per scopi illeciti: secondo la norma in esame, il documento formato (da chiunque), registrato e trasmesso è valido e rilevante.

Altro aspetto è quello che riguarda la rilevanza giuridica. La dottrina più autorevole che si è occupata *ex professo* della rilevanza giuridica, ha evidenziato come essa consista nel momento in cui un determinato fatto si collochi in uno schema normativo attraverso un procedimento di sussunzione del fatto stesso nella norma giuridica; l'efficacia, invece, diversa dalla validità, si colloca in un momento posteriore rispetto a quello della rilevanza, poiché "l'accadere del fatto provoca la sussunzione; e questa, a sua volta, è l'antecedente indeclinabile degli effetti"[33]. Su questi presupposti, è evidente un rilevante errore di normazione: il legislatore, prima che si verifichi l'accadimento del fatto, sussume la fattispecie concreta nella norma da sé creata esprimendo *ex lege* un giudizio di rilevanza. A parere di chi scrive, secondo gli orientamenti di teoria del diritto, la rilevanza si colloca in un contesto logico e cronologico successivo rispetto alla previsione normativa, posto che potrebbe anche ipoteticamente non verificarsi la fattispecie alla quale, però, il legislatore ha già attribuito a priori rilevanza giuridica. In sostanza, la norma contempla la fattispecie in astratto, il giudizio di rilevanza è soltanto quello che scaturisce successivamente alla sussunzione di una fattispecie concreta nella norma stessa. Non è pensabile attribuire rilevanza giuridica ad una fattispecie astratta. Gli effetti, poi, saranno quelli che si verificheranno a seguito del giudizio di rilevanza della fattispecie concreta. In sostanza, al di là di ogni fondato dubbio sulla errata attività di normazione, quanto su rilevato conferma l'idea di un legislatore più attento agli aspetti tecnici dei dati informatici e meno riguardo a quegli giuridici. Del resto, come si è già rilevato, ciò che è tecnico (come la firma e così anche il documento informatico) difficilmente può trovare adeguata qualificazione giuridica.

L'art. 20, comma 2, CAD menziona la firma soltanto ai fini della forma, mentre l'art. 21 disciplina gli effetti del documento informatico sul piano probatorio in ambito processuale.

Da quanto si è detto sin qui, la firma non è richiesta per la creazione del documento informatico e quindi non è un elemento costitutivo, ma assume rilevanza soltanto per gli effetti (di forma e di prova) del documento informatico stesso. In sostanza, gli aspetti più rilevanti che riguardano il documento informatico e la firma elettronica sono riconducibili alla forma (*ad probationem* o *ad substantiam*) e ai riflessi probatori in ambito processuale. Questa non è la sede per approfondire tali tematiche, ma sembra che la normativa vigente consenta la configurazione della firma come *fictio iuris* e come fattispecie a formazione progressiva che si esaurisce nel processo (identificazione, creazione, rilascio e controllo) che riguarda il corrispondente certificato.

Conclusioni. – In conclusione, *de iure condendo*, si auspica che intervenga una modifica legislativa tale da sgombrare il campo da ogni dubbio in ordine alla firma elettronica (o meglio "informatica"), chiarendo le classificazioni già esistenti. In ultimo, con riguardo al rapporto tra la firma elettronica e certificato, sarebbe anche auspicabile la creazione di un elenco unico dei certificatori di rilevanza internazionale o quanto meno comunitaria. Meglio ancora sarebbe una più completa armonizzazione delle disposizioni contenute nel CAD con quelle dettate dalla Direttiva 1999/93/CE sia in ordine ai certificati sia con riguardo ai certificatori, la cui proliferazione senza un preciso albo comunitario potrebbe ingenerare dubbi tanto a livello interno quanto in ambito internazionale.

Nicola Fabiano

Convegno 1997-2007 - DIECI ANNI DI DOCUMENTI INFORMATICI A CHE PUNTO SIAMO CON L'AMMINISTRAZIONE DIGITALE?

Nel convegno istituzionale alla Camera dei Deputati a Roma sono stati ribaditi i concetti della nostra Best Practice da esponenti di spicco della materia fra cui il Padre della Legge sulla Firma digitale **Prof. Franco Bassanini** il programma ed il video completo del convegno sono visibili in:

http://www.cybercrimeworkingroup.org/ sito dell'Università di Perugia.

BIBLIOGRAFIA ARTICOLI E CENNI ON-LINE RELATIVI ALLA POSTA ELETTRONICA

LINK

http://it.wikipedia.org/wiki/Posta_Elettronica_Certificata

http://www.ilsoftware.it/articoli.asp?id=4957