

POSTA ELETTRONICA

Panoramica Normativa e riferimenti legislativi

Premessa

La Posta elettronica certificata è ormai una realtà consolidata in tutto il mondo. I produttori di software sono sempre più attenti a questo fenomeno, che fra l'altro, si avvicina e si integra sempre più con la messaggistica dei cellulari.

Come ogni strumento, è soggetto a svariate problematiche e misure, ma in finale è anche il mezzo più rapido ed economico che sia 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 in modo più sicuro, rapido ed efficiente. Questa **Best Practice** è indirizzata alle aziende, ma può essere anche una buona norma nell'uso privato.

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" il rischio.

Evitare caratteri strani, scegliere un carattere che tutti hanno 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.

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. diminuirà 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 risponde o si inoltra un messaggio, in base alla regola fissata.

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

DISCLAIMER: 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.

Ad esempio:

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 opinions 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. È vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di 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 o 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. Non fatelo mai! Ricordate che il messaggio di posta elettronica è una cartolina postale che tutti possono leggere e nessuno manderebbe il suo *specimen* di *firma* in giro. Fatelo 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 dà la sicurezza matematica che il messaggio sia stato ricevuto e letto, ma almeno potrete insistere sulla sua ricezione e lettura. 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). 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.

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, che copre parzialmente il problema, difatti assieme al primo foglio potrebbero essere inseriti degli altri che non vengono in alcun modo garantiti.

L'ora di ricevimento: non viene garantita

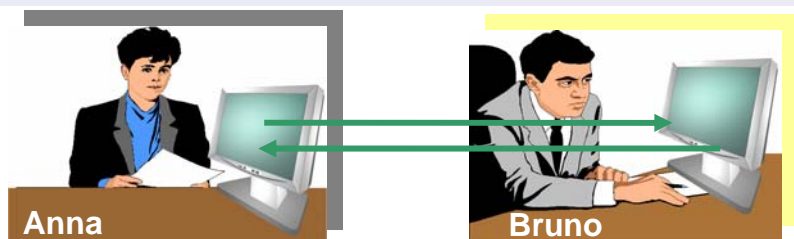
L'onere della prova spetta a: colui che riceve la raccomandata. Fortunatamente recenti sentenze della Corte di Cassazione hanno rivisto questa normativa.

[Alcune sentenze](#)

La PEC

Così come legiferata ed attuata:

- Ha bisogno che entrambi i soggetti (Anna e Bruno) abbiano una casella PEC con apparati specifici;
- Non è interoperabile con altri sistemi;
- Non può essere usata per corrispondere con altri paesi;
- Non può essere usata da più postazioni di lavoro;
- Non garantisce il non ripudio dei contenuti del messaggio;
- Non ha nessuna portabilità;
- Complessa nell'installazione e gestione;



- Non permette l'invio di allegati di grandi dimensioni.

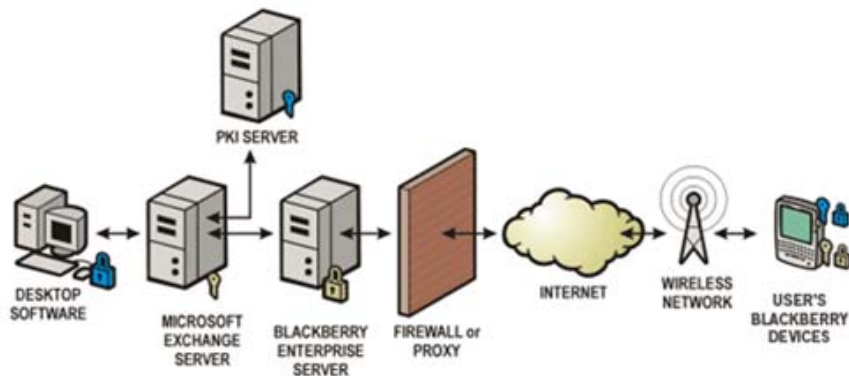
È, per ora, relegata all'uso solo con la pubblica amministrazione, dove, fra l'altro, non ha una grande diffusione. E' costosa da acquistare e da amministrare. In sostanza non si capisce perché ci sia voluta una legge apposita per la PEC quando era sufficiente e più semplice l'uso del [protocollo S-MIME](#).

Copre solo i seguenti campi:

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

Il certificato di 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, floppy, ecc.;
- E' interoperabile con qualsiasi sistema;
- E' valida in tutto il mondo;
- Esportando od installando 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;
- 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](#)



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 e 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 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 nel server dell'azienda di filtri antispamming 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.

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

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

<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>

TEST delle e-mail firmate ed anche criptate

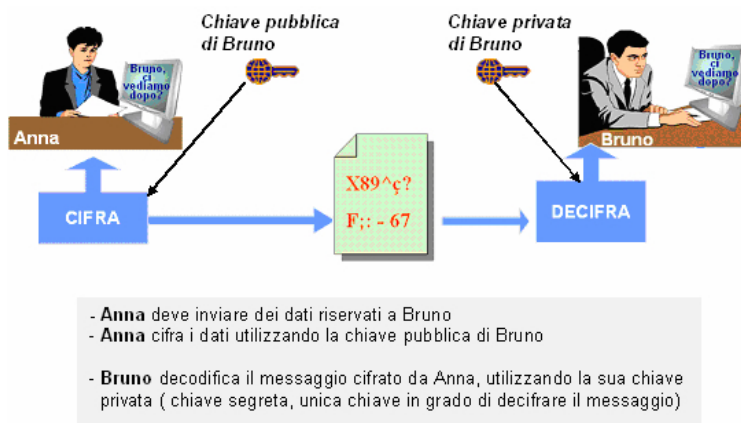
Al fine di verificare tutte le funzionalità del certificato S-MIME e buona norma effettuare subito dei test scambiando la chiave pubblica con chi si vuole corrispondere in modo sicuro, qualora vogliate effettuare una prova con il nostro servizio **KEYTEST che si attiverà con un e-mail non appena avrete scaricato ed installato il certificato S-mime** non dovrete far altro che seguire le istruzioni presenti nella e-mail: maggiori informazioni [nel nostro sito web](#).

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

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

Per allegati di grande dimensione si consiglia di usare il nostro sistema [Certified Mail](#) assieme volendo con il 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 =>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. 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.



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