PROVINCIA DI BRINDISI
Affari Generali

RELAZIONE
FIRMA DIGITALE, POSTA ELETTRONICA CERTIFICATA, DEMATERIALIZZAZIONE E CONSERVAZIONE SOSTITUTIVA

Brindisi li 27/05/2014

Luigi Settembrini

Sommario

Il presente documento è stato redatto al fine di descrivere alcune nuove tecnologie divenute strumenti indispensabili nel nostro lavoro quotidiano, indicando, per ciascuna di esse, lo stato dell'arte nell'Ente.

1. Firma Digitale

La firma digitale o meglio la firma elettronica (essendo normativamente, ai sensi della lettera s comma 1 art. 1 d.lgs. 82/2005, la firma digitale solo un particolare tipo di firma elettronica qualificata), in informatica, rappresenta l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica. Può essere basata su varie tecnologie, tra cui la crittografia a chiave pubblica.

In diritto si usano i termini di Firma elettronica semplice, Firma elettronica avanzata e Firma elettronica qualificata.

1.1 Definizione

Le firme elettroniche di un documento informatico ed in particolare le firme elettroniche avanzate e qualificate, tra cui quella digitale, si propongono di soddisfare tre esigenze che non tutte le tipologie di firma elettronica però soddisfano:

1. che il destinatario possa verificare l'identità del mittente (autenticità);
2. che il mittente non possa disconoscere un documento da lui firmato (non ripudio);
3. che il destinatario non possa inventarsi o modificare un documento firmato da qualcun altro (integrità).

Un tipico schema di firma elettronica basata sulla tecnologia della chiave pubblica consiste di tre algoritmi:

1. un algoritmo per la generazione della chiave che produce una coppia di chiavi (PK, SK): PK (Public Key, chiave pubblica) è la chiave pubblica di verifica della firma mentre SK (Secret Key) è la chiave privata posseduta dal firmatario, utilizzata per firmare il documento.
2. un algoritmo di firma che, presi in input un messaggio m e una chiave privata SK produce una firma σ.
3. un algoritmo di verifica che, presi in input il messaggio m, la chiave pubblica PK e una firma σ, accetta o rifiuta la firma.

1.2 Sistemi per la creazione e la verifica di firme elettroniche con crittografia asimmetrica

Il sistema per la creazione e la verifica di firme elettroniche può sfruttare le caratteristiche della crittografia asimmetrica.

Un sistema crittografico garantisce la riservatezza del contenuto dei messaggi, rendendoli incomprensibili a chi non sia in possesso di una "chiave" (intesa secondo la definizione crittologica) per interpretarli. Nei sistemi crittografici a chiave pubblica, detti anche a chiave asimmetrica, ogni utente ha una coppia di chiavi: una chiave privata, da non svelare a nessuno, con cui può decifrare i messaggi che gli vengono inviati e firmare i messaggi che invia, e una chiave pubblica, che altri utenti utilizzano per cifrare i messaggi da inviargli e per decifrare la sua firma e stabilirne quindi l'autenticità.

Perché il sistema risulti sicuro, è necessario che solo l'utente stesso e nessun altro abbia accesso alla chiave privata. Il modo più semplice per ottenere questo è far sì che l'unica copia della chiave sia "in mano" all'utente (il quale deve impedirne l'accesso a terzi); tuttavia, esistono soluzioni alternative (come nel caso della firma digitale remota).

Per ogni utente, le due chiavi vengono generate da un apposito algoritmo con la garanzia che la chiave privata sia la sola in grado di poter decifrare correttamente i messaggi cifrati con la chiave pubblica associata e viceversa. Lo scenario in cui un mittente vuole spedire un messaggio a un

destinatario in modalità sicura è il seguente: il mittente utilizza la chiave pubblica del destinatario per la cifratura del messaggio da spedire, quindi spedisce il messaggio cifrato al destinatario; il destinatario riceve il messaggio cifrato e adopera la propria chiave privata per ottenere il messaggio "in chiaro".

Grazie alla proprietà delle due chiavi un sistema di crittografia asimmetrica di questo tipo è adatto anche per ottenere dei documenti firmati, ma in modalità inversa rispetto a quella appena descritta cioè con la chiave privata a cifrare e quella pubblica a decifrare. Infatti, la chiave pubblica di un utente è la sola in grado di poter decifrare correttamente i documenti cifrati con la chiave privata di quell'utente. Se un utente vuole creare una firma per un documento, procede nel modo seguente: con l'ausilio di una funzione *hash* (pubblica) ricava l'impronta digitale del documento, detta anche message digest, un file di dimensioni relativamente piccole (128, 160 o più bit) che contiene una sorta di codice di controllo relativo al documento stesso, dopodiché utilizza la propria chiave privata per cifrare l'impronta digitale: il risultato di questa codifica è la firma. La funzione hash è fatta in modo da rendere minima la probabilità che da testi diversi si possa ottenere il medesimo valore dell'impronta, inoltre, è *one-way*, a senso unico, questo significa che dall'impronta è impossibile ottenere nuovamente il testo originario ovvero essa è non invertibile. La firma prodotta dipende dall'impronta digitale del documento e, quindi, dal documento stesso, oltre che dalla chiave privata dell'utente. A questo punto la firma viene allegata al documento insieme alla chiave pubblica.

Chiunque può verificare l'autenticità di un documento: per farlo, decifra la firma del documento con la chiave pubblica del mittente, ottenendo l'impronta digitale del documento, e quindi confronta quest'ultima con quella che si ottiene applicando la funzione hash al documento ricevuto; se le due impronte sono uguali, l'autenticità e l'integrità del documento sono garantite.

Le firme elettroniche possono essere disconosciute, cioè non è garantito il non ripudio, ma l'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria (art. 21 d. lgs. 82/2005).

Le operazioni di firma e di verifica possono essere demandate ad appositi programmi rilasciati, in caso di firme elettroniche avanzate o qualificate, dall'ente certificatore oppure dal proprio provider di posta elettronica, che, con una semplice configurazione, le effettuerà automaticamente.

1.3 Schema di firme a doppia chiave

I due elementi fondamentali di uno schema di firme create con il sistema della crittografia a doppia chiave sono l'algoritmo di firma e l'algoritmo di verifica.

L'algoritmo di firma crea una firma elettronica che dipende dal contenuto del documento a cui deve essere allegata, oltre che dalla chiave dell'utente. Una coppia (documento, firma) rappresenta un documento firmato, ovvero un documento a cui è stata allegata una firma.

L'algoritmo di verifica può essere utilizzato da chiunque per stabilire l'autenticità della firma elettronica di un documento.

Si parte con l'impronta di un documento che è una sequenza di caratteri ottenuta applicando una funzione di calcolo, detta funzione di hash, al file. Uno stesso file a cui è applicata la stessa funzione di hash genera sempre la medesima impronta. La stringa di output è univoca per ogni file e ne è un identificatore.

L'utente calcola l'impronta digitale del documento con un algoritmo di Hash che restituisce una stringa funzione del documento. La stringa viene poi cifrata con l'algoritmo a chiave asimmetrica usando la chiave privata del mittente. Il risultato di tale codifica è la firma elettronica del

La vulnerabilità più nota è strettamente correlata al fatto che una smart card è un calcolatore elettronico limitato, poiché manca dei dispositivi di I/O. Dovendola quindi interfacciare a un PC risulterà non completamente sicuro il processo di generazione della firma in dipendenza della potenziale insicurezza del PC utilizzato per generare l'impronta del documento da firmare. Il rischio concreto è che alla fine il PC possa ottenere dalla smart card una firma su un documento arbitrariamente scelto, diverso da quello visualizzato sullo schermo e effettivamente scelto dall'utente. Chiaramente l'utente potrebbe non essere consapevole dell'esistenza di un siffatto documento, per cui tale problema può essere considerato molto grave.

1.5.2 Documenti contenenti macro-istruzioni o codice eseguibile

Un'altra ben nota vulnerabilità è derivante dalla possibilità per i documenti di incorporare macro-istruzioni o codice eseguibile (si pensi per esempio alle macro dei documenti Word, oppure al codice Javascript dei documenti PDF). Il problema è che un documento contenente istruzioni non è statico, nel senso che la visualizzazione (la presentazione) del suo contenuto potrebbe dipendere da tali istruzioni. Per esempio, si consideri il caso di un contratto che include un valore che dipende dalla data di sistema, in modo tale che, dopo una certa data, il valore visualizzato sia modificato. La firma digitale dovrebbe essere in grado di evitare la modifica di ciò che un documento mostra all'utente, allo scopo di garantire l'integrità dell'informazione, non solo in termini tecnici, ma anche dal punto di vista degli effetti (legali) prodotti dai bit che compongono i documenti digitali. Nell'esempio precedente, chiaramente i bit del contratto digitale non variano, ma il loro effetto, in termini di contenuto rappresentato, sì. Sfortunatamente, la firma elettronica non è in grado di rilevare il comportamento dinamico del documento, tantomeno i suoi (pericolosamente dinamici) effetti legali, in quanto è ottenuta a partire dai bit che compongono il documento mediante l'applicazione di una funzione di hash crittografico prima, e l'esecuzione di un algoritmo di crittografia asimmetrica (tipicamente RSA) poi. Questa vulnerabilità è ben nota e il modo per contrastarla è banalmente quello di forzare l'utente a verificare la presenza di macro nel documento prima della firma, quindi assumendo che egli sia in grado di svolgere tale compito.

La vigente normativa italiana, comunque, esclude espressamente la validità della firma digitale per le sopraddette tipologie di documenti: l'art. 3, comma 3 del DPCM 30 marzo 2009 (nuove regole tecniche in vigore dal 6 dicembre 2009) recita infatti "Il documento informatico, sottoscritto con firma digitale o altro tipo di firma elettronica qualificata, non produce gli effetti di cui all'art. 21, comma 2, del codice, se contiene macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati" .

1.6 Valore giuridico della firma digitale in Italia

Nell'ordinamento giuridico italiano il termine firma digitale sta a indicare un tipo di firma elettronica qualificata, basato sulla crittografia asimmetrica, alla quale si attribuisce una particolare efficacia probatoria, tale da potersi equiparare, sul piano sostanziale, alla firma autografa.

Oggi, la legge che disciplina la firma elettronica è il "Codice dell'amministrazione digitale" (Decreto Legislativo 7 marzo 2005, n. 82) che ha subito nel corso del tempo varie modifiche (da ultimo a opera del d.l. 18 ottobre 2012 n. 179 nel testo integrato dalla legge di conversione 17 dicembre 2012 n. 221).

Attualmente la legge italiana prevede 4 tipologie di firma elettronica:

1 **firma elettronica generica** (chiamata anche nella prassi firma elettronica "semplice"): 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 avanzata**: insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.

3 **firma elettronica qualificata**: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato rilasciato da un certificatore accreditato e realizzata mediante un dispositivo sicuro per la creazione della firmare.

4 **firma digitale**: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e 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.

La firma digitale è quindi solo un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro.

La firma elettronica qualificata ha in più della firma elettronica avanzata l'utilizzo di un dispositivo di firma sicuro e di un certificato qualificato rilasciato da un certificatore autorizzato.

La firma elettronica avanzata deve garantire una connessione univoca al firmatario, essere creata con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.

Tutti gli altri metodi di identificazione informatica sono firme elettroniche semplici.

Sotto il profilo probatorio è stata ribadita dal dlg. 82/2005 nel testo vigente la potenziale idoneità del documento informatico, anche non sottoscritto, a integrare la forma scritta: "L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilita', fermo restando quanto disposto dall'articolo 21" (comma 1 bis art. 20).

Inoltre il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità (comma 1 art. 21).

L'efficacia automatica di scrittura privata e la presunzione semplice che il dispositivo di firma siariconducibile al titolare, in precedenza appannaggio della sola firma elettronica qualificata, sono attribuite anche alla firma elettronica avanzata: "Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilita' dell'autore, l'integrita' e l'immodificabilita' del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria" (comma 2 art. 21).

Contrariamente al passato è stata però riservata alla sola firma elettronica qualificata la possibilità di sottoscrizione dei seguenti atti: contratti che, in relazione a beni immobili, ne trasferiscano la proprietà, costituiscano, modifichino o trasferiscano l'usufrutto, il diritto di superficie, il diritto del concedente o dell'enfiteuta, la comunione su tali diritti, le servitù prediali, il diritto di uso, il diritto di abitazione, atti di rinuncia dei diritti precedenti, contratti di affrancazione del fondo enfiteutico, contratti di anticresi, contratti di locazione per una durata superiore a nove anni; contratti di società o di assicurazione con i quali si conferisce il godimento di beni immobili o di altri diritti reali immobiliari per un tempo eccedente i nove anni o per un tempo determinato; gli atti che costituiscono rendite perpetue o vitalizie, salve le disposizioni relative alle rendite di Stato; gli atti di

divisione di beni immobili e di altri diritti reali immobiliari; le transazioni che hanno per oggetto controversie relative ai diritti di cui sopra.

Il nuovo comma 2 bis dell'art. 21 infatti prevede che "Salvo quanto previsto dall'articolo 25, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale."

Inoltre lo stesso comma prevede che "Gli atti di cui all'articolo 1350, numero 13), del codice civile soddisfano comunque il requisito della forma scritta se sottoscritti con firma elettronica avanzata, qualificata o digitale".

Si tratta degli altri atti (rispetto a quelli sopra indicati) per cui sia prevista la forma scritta ad substantiam e tra questi ci sono contratti importanti come i contratti bancari e di intermediazione mobiliarie. Per questi atti la legge prevede quindi espressamente che "comunque" (cioè a prescindere da una ulteriore valutazione del giudice rispetto alla sussistenza dei requisiti della tipologia di firma) la forma scritta è integrata anche da una firma elettronica avanzata.

È quindi da ritenere che tale ultima disposizione precluda solo al giudice ulteriori indagini una volta ritenuta nella firma la natura di firma elettronica avanzata ma non impedisca, attraverso una gamma più ampia di valutazioni su tutti gli elementi di fatto acquisiti, che anche la firma elettronica semplice possa integrare la forma scritta.

La titolarità della firma elettronica qualificata è garantita dai "certificatori" (disciplinati dagli articoli 26-32bis), soggetti con particolari requisiti di onorabilità e che garantiscano affidabilità organizzativa, tecnica e finanziaria. In particolare i certificatori hanno il compito di tenere i registri delle chiavi pubbliche, al fine di verificare la titolarità del firmatario di un documento elettronico. I certificatori, inoltre, possono essere accreditati presso l'Agenzia per l'Italia digitale (già Centro Nazionale per l'Informatica nella Pubblica Amministrazione o CNIPA, successivamente DigitPA) e in tal caso vengono chiamati certificatori accreditati. Fra le caratteristiche per svolgere l'attività di certificatore di firma elettronica vi è quella per cui occorre essere una società con capitale sociale non inferiore a quello richiesto per svolgere l'attività bancaria (2.000.000€, come una S.p.A). I certificatori non sono quindi soggetti singoli (come i notai), ma piuttosto grosse società (per esempio, un certificatore è la società Postecom (Poste Italiane)).

L'acquisizione di una coppia di chiavi per i soggetti privati (chiave privata, inserita nel dispositivo di firma sicuro, e chiave pubblica, inserita nel certificato) è a pagamento, attraverso la sottoscrizione di un contratto con il certificatore accreditato, nonostante il fatto che la firma (sia manuale che digitale) sia un mezzo legale per l'esercizio di diritti naturali della persona. La coppia di chiavi ha una scadenza temporale, al momento 3 anni.

È chiaramente fondamentale che il rilascio avvenga previa identificazione certa del firmatario da parte del certificatore perché sia certa l'associazione che il certificato effettua tra chiave pubblica e dati anagrafici del titolare della firma.

1.7 La Firma Elettronica Qualificata nell'Ente Provincia di Brindisi

Il nostro Ente ha sottoscritto con l'Ente Certificatore Telecom Italia Trust Technologies S.r.l. un contratto per la fornitura del servizio *FirmaSicura* (servizio di Certificazione della Firma Elettronica Qualificata). Il settore Sistemi Informativi, abilitato al rilascio dei certificati, ha emesso, dapprima, certificati di firma alle figure vertice dell'Ente (Presidente, Segretario Generale, Dirigenti), successivamente ai titolari di Posizione Organizzativa (Funzionari ed Istruttori Direttivi) ed infine ai responsabili di procedimento (Istruttori e Collaboratori Prof.li). L'utilizzo ha riguardato diversi campi di applicazione, quali ad esempio, la firma di contratti, di documenti inviati in formato elettronico.

elettronico. L'ultima emissione di certificati, a favore dei responsabili di procedimento, ha come finalità principale la sostituzione della firma autografa apposta sugli atti prodotti dall'Ente con la Firma Digitale.

2. Posta Elettronica Certificata

La posta elettronica certificata (PEC) è un tipo particolare di posta elettronica, disciplinata dalla legge italiana, che permette di dare a un messaggio di posta elettronica lo stesso valore legale di una raccomandata con avviso di ricevimento tradizionale garantendo così il non ripudio. Anche il contenuto può essere certificato e firmato elettronicamente oppure criptato garantendo quindi anche autenticazione, integrità dei dati e confidenzialità.

La disciplina normativa è principalmente contenuta nel D.P.R. 11 febbraio 2005 n. 68 e nel decreto legislativo 7 marzo 2005 n. 82 (cosiddetto codice dell'amministrazione digitale).

Nell'aprile 2011 Francesco Gennai, Alba Shahin (ISTI-CNR), Claudio Petrucci e Alessandro Vinciarelli (CNIPA) hanno redatto l'Internet RFC 6109 al fine di rendere accessibili alla comunità Internet l'architettura e i protocolli PEC.

Dal 1° luglio 2013 le comunicazioni tra imprese e pubblica amministrazione devono avvenire solo via PEC, non essendo più accettate le comunicazioni in forma cartacea[1].

2.1 Funzionamento

Per poter utilizzare la PEC si deve disporre di un'apposita casella di PEC, gratuitamente fornita dal Governo Italiano (su un dominio specifico, senza firma digitale, ed esclusivamente per comunicazioni tra cittadino e Pubblica Amministrazione e viceversa) oppure a pagamento fornita da gestori autorizzati (comunicazione con qualsiasi tipo di casella postale elettronica e completa funzionalità).

La pubblicazione dell'elenco dei gestori autorizzati e quello della Pubblica Amministrazione, la vigilanza e il coordinamento nei confronti dei gestori e della Pubblica Amministrazione è demandata all'Ente nazionale per la digitalizzazione della Pubblica Amministrazione (DigitPA).

Al momento dell'invio di una mail PEC il gestore PEC del mittente si occuperà di inviare al mittente una ricevuta che costituirà valore legale dell'avvenuta (o mancata) trasmissione del messaggio con precisa indicazione temporale del momento in cui la mail PEC è stata inviata. In egual modo il gestore del destinatario, dopo aver depositato il messaggio PEC nella casella del destinatario, fornirà al mittente una ricevuta di avvenuta consegna, con l'indicazione del momento temporale nel quale tale consegna è avvenuta. In caso di smarrimento di una delle ricevute presenti nel sistema PEC è possibile disporre, presso i gestori del servizio, di una traccia informatica avente lo stesso valore legale in termini di invio e ricezione, per un periodo di **trenta mesi**, secondo quanto previsto dalle normative.

Dal punto di vista dell'utente, una casella di posta elettronica certificata non si differenzia dunque da una casella di posta normale; cambia solo per quello che riguarda il meccanismo di comunicazione sul quale si basa la PEC e sulla presenza di alcune ricevute inviate dai gestori PEC al mittente e al destinatario. L'utente destinatario non visualizza l'e-mail del mittente, ma un messaggio automatico generato dal gestore di posta del mittente, che contiene due allegati: la e-mail "originale" del mittente con relativi allegati, e un file di ".xml" (file di testo o apribile con apposito software) con le stesse informazioni della notifica di invio trasmessa al mittente (ID del messaggio, luogo data e ora di invio, e dati di intestazione quali e-mail del destinatario tipo PEC / non-PEC, oggetto). La posta elettronica certificata, infatti, per essere tale, deve seguire le regole fissate dal D.P.R. n. 68/2005 e dalle successive regole da esso previste. Queste norme, insieme ad altre (in particolare il Codice dell'Amministrazione Digitale, Decreto legislativo n. 235/2010), ne stabiliscono la validità legale, le regole e le modalità di utilizzo.
In particolare:

Il servizio può essere erogato esclusivamente dai gestori accreditati presso il CNIPA che è l'organo pubblico preposto al controllo della posta elettronica certificata.
Per la PEC devono essere usati domini dedicati (un dominio di PEC non contiene caselle email non PEC).

Ogni gestore PEC nel rispetto della norma deve sottoporsi a una serie di test d'interoperabilità, espressamente individuati e disponibili sul sito ufficiale del CNIPA[2]. I test d'interoperabilità vengono eseguiti per valutare la correttezza tecnico/funzionale del servizio di PEC erogato dal gestore. Come indicato nella documentazione ufficiale sono presenti espliciti test per verificare l'invio e la ricezione con caselle di posta elettronica tradizionale. Si ricorda che le regole tecniche PEC, allegate al Decreto Ministeriale 2 novembre 2005, prevedono la gestione di messaggi di posta elettronica tradizionale, tanto che viene definita un'apposita busta di trasporto atta a contenere e-mail provenienti da indirizzi di posta non PEC. Inoltre la ricevuta di accettazione, emanata all'atto dell'invio, evidenzia la tipologia di indirizzi di posta con apposite diciture (es. Posta Certificata - Posta non Certificata). Chiaramente, l'eventuale destinatario non PEC, pur ricevendo correttamente il messaggio, potrà generare gli avvisi di avvenuta/mancata consegna (e lettura del messaggio), ma senza alcun valore legale che invece avrebbe un destinatario di PEC.

2.2 Vantaggi della PEC

Il servizio PEC, per sua stessa natura, mostra una serie di vantaggi rispetto all'atto giudiziario tradizionale. I principali sono:

- Ogni formato digitale può essere inviato tramite posta elettronica certificata;
- I messaggi possono essere consultati da ogni computer o smartphone connesso alla rete Internet;
- L'avvenuta consegna al provider della mail viene garantita; nel caso non sia possibile recapitare il messaggio al destinatario, il mittente viene informato;
- Le ricevute di consegna hanno piena validità legale, anche se il messaggio non è stato effettivamente letto dal destinatario (su cui grava l'onere della prova di non aver ricevuto il messaggio), in maniera simile alla c.d. "compiuta giacenza" dell'atto giudiziario cartaceo (la differenza è che la notifica "cartacea" per compiuta giacenza si perfeziona dopo 10 giorni dal deposito presso l'ufficio postale, mentre la notifica elettronica è pressoché istantanea);
- Tracciabilità della casella mittente;
- Vi è certezza sulla destinazione dei messaggi;
- L'invio dei messaggi può avere costi inferiori a quello delle raccomandate. Per una giusta valutazione deve essere preso in considerazione il costo di invio di una raccomandata cartacea tradizionale, che cresce in funzione del numero di pagine e del peso del plico, e il numero di comunicazioni inviate annualmente. Queste informazioni devono poi essere comparate con le tariffe del gestore PEC, che solitamente rende disponibile una casella PEC con un costo calcolato su base annuale. Solitamente una volta pagato il canone annuale l'utente può inviare un numero illimitato di messaggi PEC. Va anche calcolato il "total cost of ownership" del servizio legato alle necessità di archiviazione locale, copia di sicurezza (backup), indicizzazione e recupero-estrazione delle ricevute, specie in grandi organizzazioni che generano rilevanti quantità di corrispondenza;
- Elevati requisiti di qualità e continuità del servizio. I Service Level Agreement (SLA) di legge prevedono una disponibilità del servizio del 99,8% su base quadrimestrale. Gli SLA della disponibilità del servizio PEC non valgono per la connettività. In altri termini, i server del gestore PEC possono essere disponibili nel 99,8% dell'anno, ma la connettività per raggiungerli (offerta da una terza parte) potrebbe avere SLA differenti;
- Obbligo da parte del gestore di archiviare tutti gli eventi associati a invii e ricezioni di messaggi PEC, per un periodo di trenta mesi;

- Obbligo da parte del gestore di applicare le procedure atte a garantire il rispetto delle misure di sicurezza previste dal Codice dei dati personali e la sicurezza della comunicazione.
- Esiste una funzionalità che permette, a chi invia, di chiedere una ricevuta di consegna "completa" (cioè che contiene anche una copia esatta, firmata digitalmente dal proprio gestore di posta, del messaggio spedito): tale ricevuta "completa" fa piena prova del contenuto inviato (al contrario di quanto avviene con la tradizionale posta raccomandata cartacea).

2.3 Regole tecniche

Una descrizione più tecnica e approfondita delle operazioni che vengono svolte all'interno della posta elettronica certificata e finalizzate ad aumentarne la tracciabilità, l'affidabilità e la sicurezza del sistema, è contenuta nella normativa tecnica di riferimento (Decreto Ministeriale 2 novembre 2005, *"Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata"* e allegato). In modo sommario è comunque possibile individuare alcuni comportamenti specifici della PEC, indicati di seguito.
Alla trasmissione di un messaggio PEC partecipano diverse entità:

- Il mittente, che vuole inviare un messaggio PEC
- Il destinatario, al quale il mittente vuole recapitare il messaggio PEC
- Il gestore del mittente, che mantiene un rapporto contrattuale con il mittente per quanto riguarda i servizi PEC
- Il gestore del destinatario, che mantiene un rapporto contrattuale con il destinatario per quanto riguarda i servizi PEC
- La rete internet (più in generale la rete di comunicazione)
- Il messaggio PEC

Si ponga quindi il caso di un invio di messaggio PEC corretto da parte del mittente, il corretto funzionamento dei gestori mittente e destinatario e la corretta consegna del messaggio PEC nella casella del destinatario. In questo caso il processo che guida la trasmissione di un messaggio PEC segue i seguenti passi:

- Il mittente predispone il messaggio PEC e lo sottopone al gestore mittente. Il gestore mittente riconoscerà il mittente solo dopo la sua autenticazione, ad esempio attraverso l'inserimento di user name e password.
- Il gestore mittente verifica la correttezza formale del messaggio PEC e, in caso positivo, restituisce al mittente la ricevuta di accettazione come riconoscimento dell'avvenuto invio del messaggio. La ricevuta è firmata digitalmente dal gestore e garantisce l'integrità dell'intero messaggio con i suoi allegati.
- Il gestore mittente invia il messaggio al gestore destinatario inserendolo in una busta di trasporto firmata per permettere al gestore destinatario di verificarne l'inalterabilità durante il trasporto. La busta, per definizione, contiene il messaggio e i suoi allegati, che quindi sono a loro volta protetti dalla firma del gestore.
- Il gestore destinatario, una volta ricevuto il messaggio PEC, consegnerà al gestore mittente una ricevuta di presa in carico che attesta il passaggio di consegne tra i due gestori. Il gestore destinatario verifica in fase di ricezione la correttezza del messaggio (anche avuto riguardo all'integrità, grazie alla verifica della firma digitale) e si accerta che non siano presenti virus informatici.
- Nel caso il messaggio superi i suddetti controlli, viene consegnato alla casella di posta del destinatario che può quindi leggerne il contenuto.
- Al mittente perviene una ricevuta di avvenuta consegna, che attesta la disponibilità del messaggio presso il destinatario. La ricevuta è ancora una volta firmata digitalmente e attesta l'integrità del contenuto trasmesso (a meno di scegliere intenzionalmente una forma molto leggera di ricevuta).

È importante sottolineare che la posta elettronica certificata offre la garanzia della consegna del messaggio e non della sua lettura da parte del destinatario. In altre parole nulla è detto sul fatto che il destinatario abbia letto o meno il messaggio PEC, ma si hanno garanzie sull'avvenuto recapito. Il che, in termini legali, equivale alla raccomandata con ricevuta di ritorno, ma con in più la prova certa del contenuto, tuttavia va evidenziato che il suo valore legale è effettivo solo se la mail PEC viene inviata a un'altra mail PEC. Se invece il destinatario è in possesso solo di posta elettronica di tipo ordinario sia la PEC-mail inviata sia quest'ultima non hanno valore probatorio.

Riassumendo quindi nel circuito PEC vengono rilasciate tre ricevute ai fini della certificazione del messaggio di posta elettronica certificata:

- Di accettazione, che attesta l'avvenuto invio della mail dal gestore di posta elettronica certificata del mittente.
- Di presa in carico, che attesta il passaggio di responsabilità tra due distinti gestori di posta certificata, mittente e destinatario. Questa ricevuta viene scambiata tra i due gestori e non viene percepita dagli utilizzatori del servizio.
- Di avvenuta consegna, che attesta che il messaggio è giunto a buon fine e che il destinatario ne ha piena disponibilità nella sua casella (anche se non ha ancora ricevuto il messaggio).

In caso di situazione **negativa** esistono inoltre tre tipi di avvisi rilasciati dal sistema PEC:

- Di non accettazione (per virus o utilizzo di un mittente falso o utilizzo di destinatari in copia nascosta, vietati dalla PEC, o altri problemi).
- Di mancata consegna, che sarà inviata al mittente entro 24 ore.
- Di rilevazione di virus informatici.

Si aggiunge che i messaggi in ingresso al sistema PEC possono essere "imbustati" dal gestore in due differenti tipologie di buste:

- Di trasporto, se il messaggio proviene da una casella di PEC e supera tutti i controlli di esistenza, provenienza e validità della firma.
- Di anomalia, se il messaggio proviene da una casella email non PEC oppure è malformato.

Si aggiunge che i gestori e i domini da loro gestiti, in virtù del quadro normativo di riferimento di seguito descritto, sono tutti censiti all'interno di un'apposita struttura. Pertanto viene istituito un sistema di fiducia fondamentale per offrire all'utente tutte le garanzie di sicurezza caratteristiche di questo servizio.

2.3.1 Log dei messaggi e loro conservazione

Ogni gestore PEC deve conservare per trenta mesi i log dei messaggi e renderli disponibili su richiesta del titolare della casella PEC. Questa direttiva è stata prevista in sede di redazione e approvazione del D.P.R. 11 febbraio 2005, n. 68. Nei log sono contenuti tutti gli eventi associati a invii e ricezioni di messaggi nell'ambito del circuito PEC.

È importante evidenziare che log dei messaggi non significa contenuto dei messaggi stessi, ma solo traccia dell'avvenuta transazione.

Secondo quanto previsto nelle regole tecniche allegate al D.M. 2 novembre 2005 i campi dovranno contenere almeno informazioni circa:

- Message-ID, codice identificativo del messaggio originale
- data dell'evento
- ora dell'evento
- mittente

- destinatario
- oggetto del messaggio
- tipo di evento (ad esempio ricevuta di accettazione o avvenuta consegna)
- Message-ID dei messaggi correlati
- gestore mittente

2.4 Il quadro normativo di riferimento

2.4.1 Vigilanza nei confronti dei gestori e della Pubblica Amministrazione

La normativa sulla posta elettronica certificata attribuisce al DigitPA differenti compiti. In particolare indica tale soggetto come custode e gestore delle regole tecniche. È inoltre compito del DigitPA provvedere alla pubblicazione di aggiornamenti, in coerenza con gli standard specificati nella normativa di riferimento. Il DigitPA, all'interno del proprio sito istituzionale, rende disponibile un'apposita sezione riguardante la posta elettronica certificata, contenente una versione scaricabile di tutta la documentazione valida ai fini di legge e riguardante la PEC.

2.4.2 Legislazione italiana

Il quadro normativo di riferimento relativo alla Posta Elettronica Certificata è il seguente:

- Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3." (G.U. 28 aprile 2005, n. 97)[7]
- Decreto legislativo 7 marzo 2005, n. 82, "Codice dell'amministrazione digitale".[8]
- Decreto Ministeriale 2 novembre 2005, "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" (G.U. del 15 novembre 2005, n. 266)[4]
- Circolare CNIPA CR/49 24 novembre 2005, "Modalità per la presentazione delle domande di iscrizione all'elenco pubblico dei gestori di posta elettronica certificata" (G.U. 5 dicembre 2005, n. 283)[9]
- Circolare 7 dicembre 2006, n. 51, "Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di posta elettronica certificata (PEC), di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, «Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3»."[10]
- Legge 28 gennaio 2009, n. 2. Conversione in legge, con modificazioni, del decreto-legge 29 novembre 2008, n. 185, recante misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale. (G.U. 28 gennaio 2009, n. 22, supplemento ordinario 14/L)[11]
- Decreto del Presidente del Consiglio dei ministri del 6 maggio 2009, "Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini".[12]
- Legge 18 giugno 2009, n. 69. "Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile".[13]
- Decreto legislativo 30 dicembre 2010, n. 235.[14]
- Legge 17 dicembre 2012, n. 221. Conversione in legge, con modificazioni, del decreto-legge 18 ottobre 2012, n. 179, recante ulteriori misure urgenti per la crescita del Paese.[15]

2.4.3 Legge 28 gennaio 2009 n. 2

Tra i contenuti della legge n. 2/2009 vengono indicate direttive che riguardano:

- le imprese costituite in forma societaria, che devono indicare nella domanda di iscrizione al registro delle imprese il proprio indirizzo di posta elettronica certificata 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. Per quelle già esistenti, la medesima comunicazione deve avvenire entro tre anni.
- i professionisti iscritti in albi, che devono comunicare ai rispettivi ordini o collegi il proprio indirizzo di posta elettronica certificata o analogo indirizzo di posta elettronica come previsto al punto precedente entro un anno. È poi cura degli ordini la pubblicazione in un elenco riservato, consultabile in via telematica esclusivamente dalle pubbliche amministrazioni, i dati identificativi degli iscritti con il relativo indirizzo di posta elettronica certificata.
- le amministrazioni pubbliche, che qualora non avessero già provveduto alla comunicazione di una casella PEC secondo quanto previsto dal Codice dell'amministrazione digitale, dovranno istituire una casella di posta certificata o analogo indirizzo di posta elettronica come previsto al punto precedente per ciascun registro di protocollo.
- ulteriori direttive importanti riguardano le comunicazioni tra i soggetti poc'anzi descritti. In particolare si legge che queste ultime «possono essere inviate attraverso la posta elettronica certificata o analogo indirizzo di posta elettronica di cui al comma 6, senza che il destinatario debba dichiarare la propria disponibilità ad accettarne l'utilizzo».
- infine, vengono citati anche i cittadini, che a mediante opportuna richiesta potranno ottenere una casella di PEC «con effetto equivalente alla notificazione per mezzo della posta. Le comunicazioni che transitano per la predetta casella di posta elettronica certificata sono senza oneri». Tuttavia le modalità di rilascio e di uso della casella di posta elettronica certificata saranno note entro novanta giorni dalla data di entrata in vigore della legge.

2.4.4 Il decreto 6 maggio 2009

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 6 maggio 2009 - Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini.

In tale decreto il Consiglio dei ministri definisce le modalità di rilascio della casella di posta elettronica certificata. Tra gli aspetti salienti, viene enunciata la gratuità della stessa qualora questa sia richiesta al Dipartimento per l'innovazione e le tecnologie.

L'INPS e l'Automobile Club d'Italia, a seguito di un protocollo sottoscritto con il ministro senza portafoglio per la Pubblica Amministrazione e l'Innovazione, concedono una casella di posta elettronica certificata gratuitamente. Poste Italiane gestisce invece il servizio "CEC-PAC" ufficiale del Governo italiano, conosciuto anche col nome di "*PostaCertificat@*" e disponibile sul sito *Posta Certificat@ - PostaCertificat@ Mobile – Home*. Si tratta sì di una casella di Posta Elettronica Certificata gratuita, ma con alcune limitazioni d'uso: una CEC-PAC (Comunicazione Elettronica Certificata tra Pubblica Amministrazione e Cittadino), infatti, non consente l'invio o la ricezione di posta se non con caselle PEC della Pubblica Amministrazione. Viene esclusa quindi la possibilità di comunicazioni fra privati o professionisti o imprese.

2.5 La Posta Elettronica Certificata nell'Ente Provincia di Brindisi

Il nostro Ente ha sottoscritto con l'Ente Certificatore Telecom Italia Trust Technologies S.r.l. un contratto per la fornitura di caselle di Posta Elettronica Certificata, registrando un dominio pec.provincia.brindisi.it. Così come previsto dalla normativa, è stata creata una casella di PEC istituzionale (provincia@pec.provincia.brindisi.it), regolarmente registrata all'IPA (Indice delle Pubbliche Amministrazioni in modo che sia Enti che cittadini titolari di casella di posta CEC-PAC

(descritta nel paragrafo precedente) potessero colloquiare con il ns. Ente. Sono state create successivamente delle caselle PEC per ogni Servizio.

3. Dematerializzazione

La dematerializzazione è la conversione di un qualunque documento cartaceo in un formato digitale, fruibile con mezzi informatici, finalizzata alla distruzione della materialità, così da beneficiare dei netti vantaggi di maneggevolezza offerti dalla tecnologia.

In ambito giuridico, la dematerializzazione dei documenti è il processo mediante il quale gli atti transazionali (compravendite, incassi, pagamenti, assunzione o assolvimento di obbligazioni, ecc.) tra due o più soggetti e, in generale, quelli riguardanti la formazione di documenti rilevanti sotto il profilo giuridico, si realizzano senza altro supporto che quello informatico e/o telematico per l'acquisizione degli elementi costitutivi, l'elaborazione, l'archiviazione, il trasporto e la conservazione, con pieno valore tra le parti e verso i terzi.

Il risultato è una stringa digitale che soddisfa i requisiti tecnici e legali previsti per ciascun tipo di documento elettronico nominato (per esempio, la "fattura elettronica") o, in termini più estesi, le convenzioni stabilite dalla comunità nella quale il documento assume pieno valore. Particolare rilevanza nell'ambito dei documenti assoggettabili a dematerializzazione ha la dematerializzazione degli strumenti finanziari, disciplinata con il d.lgs. n. 213/1998.

Il documento dematerializzato è considerato il nuovo paradigma della società dell'informazione e rappresenta una rilevante discontinuità nella struttura dei rapporti interpersonali e sociali, le cui conseguenze sono al momento solo in parte evidenti (riduzione degli oneri di processo, maggiore trasparenza, maggiore velocità nel perfezionamento delle operazioni di cui il documento costituisce espressione, integrabilità con altre filiere cui esso è concatenato).

Il lemma "dematerializzazione", caratterizzato dalle particella "de" (privativo), indica la trasformazione del documento materiale- che storicamente possiede la concretezza necessaria a renderlo immediatamente riconoscibile, trasmissibile e utilizzabile presso una data comunità - in una grandezza fisica digitale la quale per essere prodotta, riconosciuta e interpretata come documento necessita di strumenti elaborativi atti a (i) interfacciare i sensi umani e (ii) garantire il rispetto dei requisiti idonei alla sua legittimazione, richiesti di volta in volta dai casi d'uso. Nella sostanza, la dematerializzazione dei documenti implica lo svolgimento di un processo che per migliorare le funzioni tipiche dei documenti basati su supporti materiali e convenzioni applicabili in via analogica, adotta le tecnologie dell'informazione e della comunicazione e le regole tecniche pro-tempore accettate nella società presso cui i documenti assumono valore.

3.1 La Dematerializzazione in Italia

Sebbene in Italia la diffusione dei documenti elettronici sia meno ampia che in altri contesti industrialmente avanzati, sono noti e riconosciuti taluni casi di eccellenza a livello internazionale nel campo della dematerializzazione dei documenti. Se ne occupa l'Agenzia per l'Italia Digitale che ha sostituito il DigitPA Ente nazionale per la digitalizzazione della Pubblica Amministrazione con D.Lgs. 179/2012, che ha a sua volta sostituito per D.Lgs. 177 del 1/12/2009 il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA).

3.2 La Dematerializzazione nell'Ente Provincia di Brindisi

Il processo di dematerializzazione nel ns. Ente è iniziata nello scorso 2013, con l'introduzione del Flusso Documentale integrato nelle procedure di Protocollo ed Atti Formali.
La corrispondenza in arrivo all'Ente, se in forma cartacea, viene trasformata in formato elettronico e, dopo essere stata classificata, viene memorizzata all'interno del fascicolo del Flusso Documentale ed infine assegnata al destinatario.

La corrispondenza interna, inoltre, viene da tempo gestita attraverso la Posta Elettronica Ordinaria. Inoltre, da diversi anni, tutti i dipendenti sono titolari di una casella PEO con la quale vengono trasmesse circolari, cedolini paga, e qualsiasi tipo di corrispondenza. L'accesso alla PEO è possibile, inoltre, anche dall'esterno dell'Ente, attraverso smartphone e palmari connessi alla rete internet.

4. Conservazione sostitutiva

La conservazione sostitutiva è una procedura legale/informatica regolamentata dalla legge italiana, in grado di garantire nel tempo la validità legale di un documento informatico, inteso come una rappresentazione di atti o fatti e dati su un supporto sia esso cartaceo o informatico (delibera CNIPA 11/2004).

La conservazione sostitutiva equipara, sotto certe condizioni, i documenti cartacei con quelli elettronici e dovrebbe permettere ad aziende e all'amministrazione pubblica di risparmiare sui costi di stampa, di stoccaggio e di archiviazione. Il risparmio è particolarmente alto per la documentazione che deve essere, a norma di legge, conservata per più anni.

Conservare digitalmente significa sostituire i documenti cartacei, che per legge alcuni soggetti giuridici sono tenuti a conservare, con l'equivalente documento in formato digitale che viene "bloccato" nella forma, contenuto e tempo attraverso la firma digitale e la marca temporale.È infatti la tecnologia della firma digitale che permette di dare la paternità e rendere immodificabile un documento informatico, affiancata poi dalla marcatura temporale permette di datare in modo certo il documento digitale prodotto.

4.1 Normativa

Con l'introduzione delle recenti normative sulla conservazione sostitutiva, il documento informatico acquista valore probatorio ai fini fiscali e legali. Infatti, con l'introduzione del Decreto del 23 gennaio 2004 del Ministero dell'Economia e delle Finanze e con la Deliberazione del Centro Nazionale per l'Informatica nella Pubblica Amministrazione n° 11 del 19 febbraio 2004, oggi è possibile archiviare e conservare su supporti ottici i documenti cartacei e, utilizzando la firma elettronica qualificata e la marcatura temporale, si può anche decidere di eliminarli. Negli ultimi tempi l'interesse verso le soluzioni di Document Management è aumentato in maniera significativa in Italia dovuto anche alla recente legge che autorizza, secondo certi criteri ben definiti, l'utilizzo di metodologie di archiviazione ottica sostitutiva e trattamento dei documenti anche di quelli considerati a valore fiscale (es. fatture, libro IVA, ecc). Si tratta della cosiddetta legge "Bassanini" seguita dalle varie norme emesse dal CNIPA che garantiscono ai documenti informatici piena validità ai fini probatori, legali e fiscali e, dunque, possono pienamente sostituire i tradizionali metodi di conservazione delle registrazioni aziendali. Questo provvedimento apre innumerevoli vantaggi per le aziende e non solo: basti pensare alla riduzione degli spazi di conservazione dei documenti, all'incredibile risparmio cartaceo, all'abbattimento dei costi "nascosti" di gestione, alla velocità di ricerca dei documenti a distanza e molto altro. La dimensione del mercato è vastissima, ed è frutto dell'introduzione di tutta una serie di normative in ambito di archiviazione la cui storia è di seguito riassunta.

D.L. 10 giugno 1994 n. 357 Art. 7: Si è stabilita la possibilità di conservare scritture e documenti contabili sotto forma di registrazioni su supporti di immagini, a condizione, comunque, che le registrazioni corrispondano ai documenti e possano essere trasformate in qualsiasi momento in un esemplare leggibile del documento da cui sono state formate. Ma nel 1994 non erano ancora pienamente sviluppate le tecniche di riproduzione elettronica dei documenti.

D.L. 15 marzo 1997 n. 59 Art. 15: Riconosce la validità a tutti gli effetti di legge degli atti, dati e documenti formati ed i contratti stipulati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, rinviando, tuttavia, per la sua attuazione ad un apposito regolamento.

D.P.R. 10 novembre 1997 n. 513: Definiti i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici. Art. 15: Conservare su supporti informatici i libri, i repertori e le scritture di cui sia obbligatoria la tenuta. Per le regole tecniche è tutto demandato all'AIPA: Autorità per l'Informatica nella Pubblica Amministrazione.