La Dematerializzazione

alla luce del Codice dell'Amministrazione Digitale
Decreto legislativo 7 marzo 2005, n. 82

Prefettura di Reggio Calabria
19 dicembre 2011

Dematerializzazione 1/2

- Il termine dematerializzazione indica il progressivo incremento della gestione documentale informatizzata - all'interno delle strutture amministrative pubbliche e private - e la conseguente sostituzione dei supporti tradizionali della documentazione amministrativa in favore del documento informatico, a cui la normativa statale, fin dal 1997 riconosce pieno valore giuridico.

Dematerializzazione 2/2

- La dematerializzazione costituisce una delle linee di azione più significative per la riduzione della spesa pubblica, in termini sia di risparmi diretti (carta, spazi, ecc.), sia di risparmi indiretti (tempo, efficienza, ecc.) ed è uno dei temi centrali del Codice dell'Amministrazione Digitale (Decreto Legislativo 7 marzo 2005 n. 82).

STRUMENTI PER LA DEMATERIALIZZAZIONE

- Documento informatico
- Firma digitale
- Sistema di gestione informatica dei documenti
- Posta elettronica / PEC
- Sito web / Albo pretorio on-line

I parte

Documento informatico
Firma digitale

Definizione generale di documento

Il documento deve avere le seguenti caratteristiche:

1) Essere di natura materiale (carta, nastro magnetico)
2) Avere contenuto materiale (voce) o immateriale (segni espressivi che rappresentano un'idea)
3) Essere intelligibile (deve essere in grado di essere percepito dagli altri)
4) Avere la capacità di rappresentare in modo permanente un atto/fatto giuridico

Documento cartaceo

- Nel caso di un documento cartaceo c'è un legame diretto tra le informazioni contenute nel documento e il supporto atto a contenerle: il tipo di carta o di inchiostro utilizzato costituiscono proprietà distintive di un documento;
- l'identificazione dell'autore è affidata alla firma autografa: la calligrafia, infatti, è tradizionalmente considerata un elemento identificativo della persona, anche se lascia uno spazio notevole alle falsificazioni.

Documento informatico

Il cambiamento di supporto produce una differenza evidente:

- un documento informatico è riproducibile indefinitamente e modificabile con estrema facilità;
- non si può distinguere tra un documento originale e le corrispondenti copie;
- qualunque computer è infatti in grado di generare lo stesso documento.

Nel documento elettronico viene quindi a cadere il legame diretto tra informazione e relativo supporto, legame che, come è stato detto, caratterizza in qualche modo il documento cartaceo

Esempi

- Documento testuale: → Documento digitale

Lettera, atto, decreto, circolare, ecc.

- Documento precompilato: → Transazione digitale

Modelli, schemi, ecc.

Definizioni giuridiche di documento informatico

PENALE	AMMINISTRATIVO
Articolo 491-bis c.p.: supporto che contiene dati o informazioni aventi efficacia probatoria o programmi destinati ad elaborarli	Articolo 2, D.P.R. 513/97: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (D.P.R. 513/97).
Abolita dopo la ratifica della Convenzione di Budapest (2008)	Abrogato e recepito dal DPR 445/2000

CAD Art. 20 - Il documento informatico

1. Il documento informatico da chiunque formato, la memorizzazione 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 .

1-bis. L'idoneita' del documento informatico a soddisfare il requisito della forma scritta e' liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di **qualita', sicurezza, integrita' ed immodificabilita**', fermo restando quanto disposto dal comma 2.

Sottoscrizione

La sottoscrizione autografa

La sottoscrizione autografa consiste nella scrittura di pugno del patronimico (nome e cognome) in calce ad un documento. La sottoscrizione svolge tre funzioni fondamentali:

1) Funzione **indicativa**: identificare l'autore del documento
2) Funzione **dichiarativa**: permette di affermare che il documento a cui la sottoscrizione è stata apposta è stato formato per conto di chi sottoscrive
3) Funzione **probatoria**: consente di provare l'identità del firmatario

Evoluzione normativa della firma elettronica

1	Legge 15 marzo 1997, n. 59 (Legge "Bassanini"):	Documenti creati con strumenti informatici sono validi a tutti gli effetti di legge
2	D.P.R. 10 novembre 1997, n. 513	Definizione di documento informatico e firma digitale
3	D.P.C.M. 8 febbraio 1999	Regole tecniche dei documenti informatici
4	D.P.R. 28 dicembre 2000, n. 445	Testo unico in materia di documentazione amministrativa
5	D.Lgs. 23 gennaio 2002, n. 10	Definizione di firma elettronica
6	D.Lgs. 7 marzo 2006, n. 82	Codice dell'Amministrazione Digitale
7	D.Lgs. 4 aprile 2006, n. 159	Modifiche al Codice dell'Amministrazione Digitale

Codice Amministrazione Digitale

Dopo un lungo e contraddittorio iter legislativo l'articolo 1 del Codice dell'Amministrazione Digitale individua tre differenti tipologie di firma elettronica:

1. Firma elettronica semplice
2. Firma elettronica qualificata
3. Firma digitale

Firma elettronica semplice

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

- Si riferisce a metodi di identificazione aventi scarsi requisiti di sicurezza (PIN o password)
- Non viene considerata come procedura di sottoscrizione, ma al massimo come strumento di identificazione

Firma elettronica qualificata

Firma elettronica qualificata: è quella ottenuta attraverso una procedura informatica che garantisca:

- la connessione univoca al firmatario
- la sua univoca autenticazione informatica
- la presenza di un certificato qualificato
- la sua creazione mediante un dispositivo sicuro per la creazione della firma

Firma digitale

Firma digitale: è 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

Firma digitale e crittografia

La firma digitale è il risultato dell'applicazione al documento in forma elettronica di una coppia di **chiavi asimmetriche**, secondo determinati standards e procedure previste dalla legge

Tali chiavi sono il risultato di una particolare tecnica di **crittografia** nata con l'avvento della tecnologia informatica

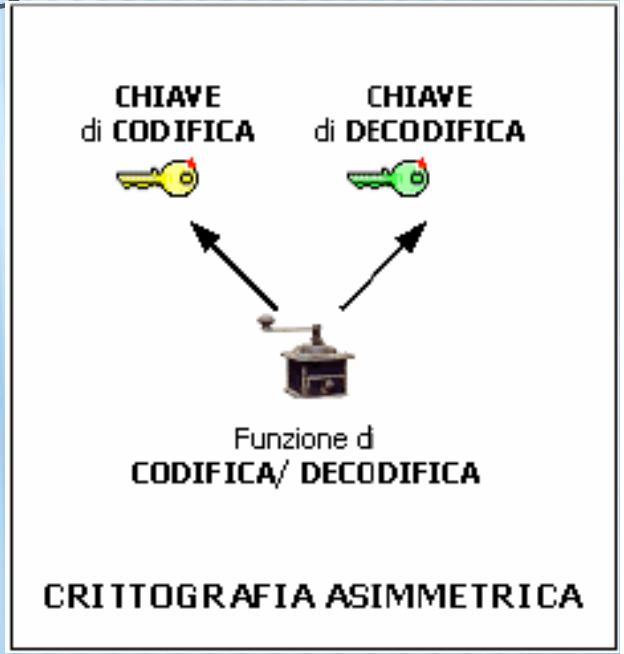
La **crittografia** consiste nella capacità di rendere segreto il contenuto di un messaggio ad eccezione del destinatario finale prescelto

Crittografia simmetrica

- Con **crittografia simmetrica** si intende una tecnica di **cifratura**. Uno schema di crittografia simmetrica è caratterizzato dalla proprietà che, data la chiave di cifratura “X", sia facilmente calcolabile la chiave di decifratura “Y". Nella pratica, tale proprietà si traduce nell'utilizzo di una sola chiave sia per l'operazione di cifratura che quella di decifratura. La forza della crittografia simmetrica è dunque riposta nella segretezza dell'unica chiave utilizzata dai due interlocutori che la usano, oltre che nella grandezza dello spazio delle chiavi, nella scelta di una buona chiave e nella resistenza dell'algoritmo agli attacchi di crittanalisi

Crittografia asimmetrica

- Con **crittografia asimmetrica** si intende un tipo di crittografia dove, ad ogni attore coinvolto, è associata una coppia di chiavi:
  - **chiave privata**: personale e segreta, viene utilizzata per decifrare un documento cifrato;
  - **chiave pubblica**: serve a cifrare un documento destinato alla persona che possiede la relativa chiave privata.



Questa funzione è utilizzata per implementare la firma digitale

Hash code=> Firma digitale

La funzione di firma digitale non si applica direttamente al documento da firmare, ma si utilizza su un'impronta, detto digest, del documento calcolato attraverso una funzione matematica detta di **hashing**

L'**hash code** è una funzione univoca operante in un solo senso (ossia, che non può essere invertita), atta alla trasformazione di un testo di lunghezza arbitraria in una stringa di lunghezza fissa, relativamente limitata

Il dispositivo di firma

Il dispositivo di firma può essere una smart card o un token usb contenente la chiave privata che associata ad un software specifico, genera la firma digitale apponendola ad un documento informatico.

Il dispositivo deve garantire che la firma sia:

1) Riservata
2) Protetta da contraffazioni
3) Protetta dall'uso da parte di terzi

Apposizione firma digitale

1. Si calcola, tramite una funzione di Hash, l'impronta del documento informatico
2. Al risultato della funzione si applica l'algoritmo di crittografia asimmetrico utilizzando la propria chiave privata presente sul dispositivo di firma
3. Si unisce il risultato dell'elaborazione, ovvero la firma, al documento originario

Verifica firma digitale

1. Si ricava il certificato del firmatario del documento informatico
2. Si verifica la validità temporale del certificato rispetto alla data di firma del documento
3. Si applica l'algoritmo di crittografia asimmetrico per decodificare l'impronta del documento, con la chiave pubblica del firmatario contenuta nel certificato
4. Si ricalcola l'impronta del documento informatico
5. Si confrontano i risultati della due funzioni:
   - se coincidono la firma è valida
   - altrimenti la firma è falsa

Le caratteristiche di un documento informatico firmato digitalmente

- **Integrità**
  Garanzia che il documento non è stato manomesso dopo la sottoscrizione.
- **Autenticità**
  Garanzia dell'identità di chi firma.
- **Non ripudio**
  L'autore non può disconoscere il documento firmato.
- **Valore legale**
  il documento elettronico sottoscritto digitalmente ha lo stesso valore legale di un documento cartaceo sottoscritto con firma autografa.

Il ruolo dei Certificatori

Il pieno collegamento soggettivo tra la firma digitale e il soggetto firmatario richiede l'intervento di un soggetto imparziale che agisca quale terza parte fidata per certificare la chiave pubblica e autenticare la firma

Il Codice dell'Amministrazione Digitale distingue in:

A) **Certificatori**: soggetti che prestano servizi di certificazione delle firme elettroniche

B) **Certificatori qualificati**: soggetti che rilasciano al pubblico certificati conformi ai requisiti indicati dal CAD e dalle regole tecniche

C) **Certificatori accreditati**: soggetti che intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato in termini di qualità e sicurezza inseriti in un apposito elenco gestito dal CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione

I certificati elettronici e la validazione temporale

I certificati sono documenti elettronici che contengono informazioni garantite circa il titolare della chiave. Si distinguono in elettronici e qualificati a secondo del contenuto del certificato e della qualità del certificatore.

La **validazione temporale** consente di attribuire ad uno o più documenti una data ed un orario opponibile a terzi, garantendo il momento della loro formazione e sottoscrizione.

Premesso che il certificato elettronico ha una durata limitata nel tempo è possibile protrarre l'effetto e la validità di un documento elettronico attraverso l'apposizione di una **marca temporale**.

La validazione temporale e la marca temporale sono servizi che deve necessariamente garantire l'ente certificatore.

Valore probatorio

CAD Art. 21. Valore probatorio del documento informatico sottoscritto

1. 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, integrita' e immodificabilita.
2. Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, 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.
3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

Efficacia del documento informatico

Firma elettronica "Semplice"	Il documento informatico a cui è stata apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio	Firma "debole" o "leggera"
Firma elettronica qualificata o firma digitale	Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile (scrittura privata con inversione dell'onere della prova)	Firma "sicura"
Firma elettronica autenticata	L'autenticazione della firma digitale o di altro tipo di firma elettronica qualificata avviene mediante attestazione di un Pubblico Ufficiale (articolo 2703 del codice civile)	Firma "autenticata"

Art. 22. Documenti informatici originali e copie. Formazione e conservazione

1. Gli atti formati con strumenti informatici, i dati e i documenti informatici delle pubbliche amministrazioni costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge.
2. Nelle operazioni riguardanti le attività di produzione, immissione, conservazione, riproduzione e trasmissione di dati, documenti ed atti amministrativi con sistemi informatici e telematici, ivi compresa l'emanazione degli atti con i medesimi sistemi, devono essere indicati e resi facilmente individuabili sia i dati relativi alle amministrazioni interessate, sia il soggetto che ha effettuato l'operazione.
3. Le copie su supporto informatico di documenti formati in origine su altro tipo di supporto sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'ambito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale e nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

Art. 23. Copie di atti e documenti informatici

1. All'articolo 2712 del codice civile dopo le parole: «riproduzioni fotografiche» è inserita la seguente: «, informatiche».
2. I duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi a tutti gli effetti di legge, se conformi alle vigenti regole tecniche.

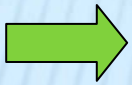
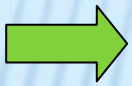
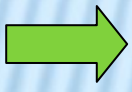
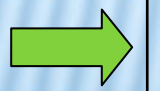
2-bis. Le copie su supporto cartaceo di documento informatico, anche sottoscritto con firma elettronica qualificata o con firma digitale, sostituiscono ad ogni effetto di legge l'originale da cui sono tratte se la loro conformita' all'originale in tutte le sue componenti e' attestata da un pubblico ufficiale a cio' autorizzato.

3. I documenti informatici contenenti copia o riproduzione di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata, da parte di colui che li spedisce o rilascia, una firma digitale o altra firma elettronica qualificata.

Art. 23. Copie di atti e documenti informatici

4. Le copie su supporto informatico di qualsiasi tipologia di documenti analogici originali, formati in origine su supporto cartaceo o su altro supporto non informatico, sostituiscono ad ogni effetto di legge gli originali da cui sono tratte se la loro conformità all'originale è assicurata da chi lo detiene mediante l'utilizzo della propria firma digitale e nel rispetto delle regole tecniche di cui all'articolo 71.
5. Con decreto del Presidente del Consiglio dei Ministri possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione ottica sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.
6. La spedizione o il rilascio di copie di atti e documenti di cui al comma 3, esonera dalla produzione e dalla esibizione dell'originale formato su supporto cartaceo quando richieste ad ogni effetto di legge.
7. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche dettate ai sensi dell'articolo 71 di concerto con il Ministro dell'economia e delle finanze.

Originale e Copia

Originale		Copia	
Cartaceo		Cartaceo	Copia Conforme Manuale
Cartaceo		Digitale	Copia Conforme Digitale
Digitale		Digitale	Copia Autentica
Digitale		Cartaceo	Copia Conforme Manuale

ART. 24. FIRMA DIGITALE

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.
2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.

----- esempio

Art. 36. Revoca e sospensione dei certificati qualificati

1. Il certificato qualificato deve essere a cura del certificatore:

   a. revocato in caso di cessazione dell'attività del certificatore salvo quanto previsto dal comma 2 dell'articolo 37;
   b. revocato o sospeso in esecuzione di un provvedimento dell'autorità;
   c. revocato o sospeso a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare, secondo le modalità previste nel presente codice;
   d. revocato o sospeso in presenza di cause limitative della capacità del titolare o di abusi o falsificazioni.

ART. 40. FORMAZIONE DI DOCUMENTI INFORMATICI

1. Le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71.
2. Fermo restando quanto previsto dal comma 1, la redazione di documenti originali su supporto cartaceo, nonchè la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità.

Pro

- Utilizzare il supporto cartaceo comporta costi considerevoli di materia prima e di personale addetto all'archiviazione e al reperimento dei documenti stessi. Senza contare il costo più rilevante, vale a dire il rallentamento nei processi decisionali dettato dall'uso del supporto cartaceo.

L'alternativa è di ricorrere al documento informatico.

- Questa alternativa è resa possibile dalla tecnologia della firma digitale. Tale possibilità tecnica apre nuovi scenari: il flusso documentale cartaceo può essere sostituito dal flusso documentale informatico. Il ciclo di vita dei documenti elettronici può quindi essere completamente gestito in maniera elettronica con conseguenti vantaggi sia in termini di incremento della velocità di trattamento delle informazioni sia economici.

Contro

I vantaggi scompaiono se il flusso documentale non è omogeneo: cartaceo o digitale

Ogni passaggio cartaceo-digitale o viceversa comporta:

- Incremento del lavoro di digitalizzazione
- Incremento dell'uso della carta
- Incremento delle azioni di autenticazione

II parte

Il sistema di gestione informatica dei documenti

Definizione 1

- E’ un servizio, obbligatorio negli enti pubblici ma che esiste anche in molte organizzazioni private, erogato da una apposita struttura, di solito denominata ufficio di protocollo.
- Ha il compito di trattare in maniera opportuna e sotto il duplice profilo giuridico e gestionale tutte le scritture o documenti in entrata ed in uscita dall’organizzazione, ed eventualmente anche documenti di rilievo esclusivamente interno.

Definizione 2

- Il servizio deve numerare, classificare ed archiviare tutti i documenti prodotti dall'ente, in modo da consentirne la corretta lavorazione, il rapido recupero delle informazioni associate, la loro autenticazione e la conservazione.
- Ogni documento viene assegnato ad una determinata categoria e sottocategoria (classe, fascicolo) oppure inserito in un registro, sulla base di un piano di classificazione (titolario) predefinito, che garantisce l'organizzazione fisica e logica dell'archivio corrente.

Definizione 3

Per poter garantire questo servizio la legge impone agli enti pubblici di protocollare (numerare, segnare, classificare ed archiviare) tutti i documenti in entrata (prima dell'assegnazione agli uffici competenti) e tutti i documenti in uscita (prima di essere resi accessibili o inviati ai destinatari);

Per poter far questo in maniera efficace deve:

- Essere un servizio dotato di autonomia operativa
- Essere unico, salvo casi particolari
- Utilizzare efficaci tecniche archivistiche per la catalogazione ed archiviazione dei documenti
- Conoscere l'intera struttura funzionale ed operativa dell'ente per strutturare di conseguenza l'organizzazione dei documenti

Valore giuridico e valore gestionale

- Valore giuridico probatorio: la registrazione di protocollo certifica che un determinato documento è autentico, cioè è possibile attribuirgli una provenienza certa ed una data certa.
- Valore gestionale: l'attività di classificazione almeno iniziale del documento, consente di inserire il documento nel contesto del procedimento e quindi in relazione con tutti i documenti in qualche modo correlati.
- Ai fini del valore giuridico probatorio, tutte le informazioni di registrazione di protocollo e la segnatura sul documento devono essere create in un'unica sessione e deve essere garantita la non modificabilità delle informazioni.

La precedente normativa sul protocollo

Prima della attuale riforma (DPR 445/2000) il protocollo era normato da due testi fondamentali:

- Per gli enti della PA centrale dal Regio Decreto 25 gennaio 1900 numero 35 avente per oggetto "*Regolamento per gli uffici di registratura e di archivio delle Amministrazioni Centrali*"
- Per gli enti locali dalla Circolare del Ministero degli Interni n. 17100/2 del 1 marzo 1897 avente per oggetto "*Istruzioni per la tenuta del protocollo e dell'archivio per gli uffici comunali*"

Il Protocollo informatico

- Il Protocollo informatico previsto dal DPR 445/2000 non è un software, ma è un nuovo servizio che tutte le PA devono attivare entro il 1/1/2004, che si avvale di diversi sistemi software integrati, per la registrazione, segnatura e gestione dei documenti informatici, inclusa la loro firma e trasmissione.

Il Codice dell'Amministrazione Digitale

Capo III - Formazione, Gestione e Conservazione dei Documenti Informatici

Art. 40. Formazione di documenti informatici
Art. 41. Procedimento e fascicolo informatico
Art. 42. Dematerializzazione dei documenti delle pubbliche amministrazioni
Art. 43. Riproduzione e conservazione dei documenti
Art. 44. Requisiti per la conservazione dei documenti informatici

Art. 40. Formazione di documenti informatici

- Le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71.
- Fermo restando quanto previsto dal comma 1, la redazione di documenti originali su supporto cartaceo, nonchè la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità.

Art. 41. Procedimento e fascicolo informatico

- Le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione, nei casi e nei modi previsti dalla normativa vigente.
- La pubblica amministrazione titolare del procedimento può raccogliere in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati; all'atto della comunicazione dell'avvio del procedimento ai sensi dell'articolo 8 della legge 7 agosto 1990, n. 241, comunica agli interessati le modalità per esercitare in via telematica i diritti di cui all'articolo 10 della citata legge 7 agosto 1990, n. 241.

Art. 42. Dematerializzazione dei documenti delle pubbliche amministrazioni

- Le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle regole tecniche adottate ai sensi dell'articolo 71.

Art. 43. Riproduzione e conservazione dei documenti

- I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione sia effettuata in modo da garantire la conformità dei documenti agli originali e la loro conservazione nel tempo, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.
- Restano validi i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento già conservati mediante riproduzione su supporto fotografico, su supporto ottico o con altro processo idoneo a garantire la conformità dei documenti agli originali.
- I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali.

Art. 44. Requisiti per la conservazione dei documenti informatici

Il sistema di conservazione dei documenti informatici garantisce:

- l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
- l'integrità del documento.
- la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi ì dati di registrazione e di classificazione originari;
- il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto.

Vantaggi del protocollo informatico

L'introduzione di un sistema di protocollo informatico consente di:

- eliminare i registri cartacei
- diminuire gli uffici di protocollo
- razionalizzare i flussi documentali
- rendere più efficace ed economica l'azione amministrativa
- favorire la trasparenza dell'azione amministrativa dei procedimenti

Funzionalità minime ed aggiuntive

Le Amministrazioni devono garantire la realizzazione di un sistema di protocollo informatico che comprenda almeno le cosiddette **funzionalità minime:**

- la certificazione della corrispondenza in ingresso ed in uscita
- l'adozione di un titolario di classificazione dei documenti protocollati a seconda dell'argomento cui essi fanno riferimento.

Relativamente alla **funzionalità aggiuntive**:

- automazione dei procedimenti amministrativi intra-ammistrazione o tra AOO diverse
- reingegnerizzazione dei processi di lavorazione dei documenti
- riorganizzazione delle diverse sezioni dell'archivio

Ciclo di vita del documento

1. Documenti in entrata
2. Sistema di Gestione interna dei documenti
3. Sistema di archiviazione e conservazione
4. Documenti in uscita

1 – Documenti in entrata

Dopo l’attivazione del protocollo informatico i documenti in entrata potranno essere:

1. Cartacei
2. Informatici
   (con firma digitale o elettronica)
3. Riproduzioni digitali

2 – Sistema di gestione interna dei documenti

Dopo l'attivazione del protocollo informatico, i dati di controllo (registro, segnatura) saranno informatici (nucleo minimo), il flusso dei documenti potrà essere:

1. Solo cartaceo: altamente inefficiente, non conforme alla normativa, presuppone la stampa di copie conformi di tutti i documenti informatici ricevuti
2. Solo informatico: altamente efficiente, evita la doppia gestione, riduce al minimo il cartaceo, ma presuppone la digitalizzazione di tutti o quasi tutti i documenti cartacei in ingresso
3. Misto: con gestione elettronica dei flussi dei documenti elettronici (ed eventuale digitalizzazione solo di parte dei documenti cartacei in ingresso)

3 – Sistema di archiviazione e conservazione dei documenti

Dopo l'attivazione del protocollo informatico, il sistema di archiviazione e conservazione dei documenti potrà essere:

1. Solo cartaceo: altamente inefficiente, non conforme alla normativa, presuppone la stampa di copie conforme di tutti i documenti informatici ricevuti
2. Solo informatico: altamente efficiente, presuppone la digitalizzazione di tutti i documenti cartacei in ingresso
3. Misto: archiviazione informatica per i documenti elettronici e cartacea per i documenti cartacei oppure cartaceo per fini legali e informatico per l'accesso o altre formule

4 – Documenti in uscita

Dopo l'attivazione del protocollo informatico i documenti in uscita potranno essere:

1. Solo informatici (in accordo con l'art 9, comma 1 DPR 445/2000), da cui possono essere tratte copie conformi su altri supporti (cartacei)
2. Solo cartacei, non conforme alla normativa (i documenti scambiati tra PA sono informatici)
3. Misto: altamente inefficiente, con doppia gestione documentale cartaceo/informatico

Strumenti presenti

Il nostro sistema di gestione documentale WEBARCH è anche un **sistema di gestione dei flussi documentali**

1. Documento digitale
2. Classificazione / Titolario
3. Registro di Protocollo
4. Fascicolo digitale / Faldone digitale
5. Procedimento digitale
6. Responsabile / Incaricato del procedimento
7. Posta elettronica certificata

Documento

Il documento in entrata può trovarsi in uno dei seguenti stati:

- Sospeso
- In lavorazione
- Rifiutato
- Agli atti
- In evidenza
- Presa visione
- Annullato

Il documento in uscita può trovarsi in uno dei seguenti stati:

- In risposta
- Non spedito
- Spedito
- Annullato

Fasciolo

Il fascicolo può trovarsi in uno dei seguenti stati:

- In trattazione
- Agli atti
- In evidenza

Procedimento

Il procedimento può trovarsi in uno dei seguenti stati:

- Aperto
- In evidenza
- Scaduto
- Chiuso

Al procedimento è associato un responsabile che ne cura la lavorazione:

1. Fase iniziativa
2. Fase istruttoria
3. Fase decisoria
4. Fase integrativa
5. Concluso

Workflow entrata 1

1. Arrivo del documento:
   - Digitale
   - Cartaceo -> digitalizzazione
2. Protocollazione
   - Classificazione
   - Assegnazione all'Ufficio di competenza

esempio

Workflow entrata 2

3. Presa in carico / rifiuto
4. Lavorazione del documento
    1. Avvio nuovo procedimento
    2. Archiviazione / Fascicolo
    3. Trattazione / evidenza

Workflow uscita 1

1. Predisposizione documento digitale
2. Protocollazione:
   - Archiviazione / Fascicolo
   - Classificazione
   - Invio tramite Posta elettronica

esempio

Workflow uscita 2

3. Caso invio in formato cartaceo
    1. Stampa documento
    2. Firma manuale
    3. Copia a fascicolo
    4. Imbustamento
    5. Ricevuta di ritorno

Workflow ricerca

- Ricerca per:
  - Numero Protocollo
  - Numero Fascicolo
  - Numero Procedimento
  - Data di Arrivo / Uscita / Protocollazione
  - Ufficio / Incaricato
  - Testo libero
  - Stato di lavorazione (Trattazione/Evidenza/Atti/ecc...)

Le criticità

Utilizzo distorto nell'applicazione della norma:

- la gestione documentale se attuata male implica a una gestione ridondante dei documenti non porta a nessuna razionalizzazione e nessuna semplificazione

Scarsa sicurezza in alcuni aspetti del quadro normativo:

- La mancata o limitata attuazione della gestione elettronica dei documenti è dovuta anche alla mancata soluzione dei problemi legati alla conservazione elettronica dei documenti

Possibili azioni di contrasto

Occorre definire delle linee guida sulla base di una sperimentazione pratica di attuazione delle norme vigenti sulla conservazione allo scopo di verificarne:

- la facilità di applicazione
- la sostenibilità dei costi
- la garanzia di un raggiungimento di un buon grado di efficienza a fronte di un rischio di perdita di informazione praticamente nullo
- la definizione chiara dei ruoli e dei compiti degli operatori

Occorre investire sulla formazione e sulle attività di change management

Possibili azioni di contrasto

Per ottenere una vera semplificazione occorre reingegnerizzare i processi o nel rispetto delle norme reinventare i processi amministrativi riducendo le prassi endoprocedimentali consolidate: la farraginosità di certi processi amministrativi causa una gestione documentale inefficiente e ridondante

- Top down – prima BPR poi attuazione (BPR non sia l'alibi per rinviare l'attuazione dei progetti)
- Bottom up - Non materializzare i file e "pensare digitale"

Possibili azioni di contrasto

- Evitare di materializzare e dematerializzare il file solo così si innesca un processo virtuoso che obbliga una analisi del Flussi
- Almeno tra PA comunicare con strumenti elettronici
- Adottare nuove modalità per verificare l'efficienza del processo
- Firma digitale solo per le comunicazioni all'esterno da parte di chi ha delega di firma

III Parte

Posta elettronica
Siti WEB

Il Codice dell'Amministrazione Digitale

Capo IV - Trasmissione Informatica dei Documenti

- Art. 45. Valore giuridico della trasmissione
- Art. 46. Dati particolari contenuti nei documenti trasmessi
- Art. 47. Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni
- Art. 48. Posta elettronica certificata
- Art. 49. Segretezza della corrispondenza trasmessa per via telematica

Art. 45. Valore giuridico della trasmissione

1. I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, ivi compreso il fax, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.
2. 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.

Art. 47. Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni

1. Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.
2. Ai fini della verifica della provenienza le comunicazioni sono valide se:
   - sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;
   - ovvero sono dotate di protocollo informatizzato;
   - ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71;
   - ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68

Art. 47. Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni

3. Entro otto mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni centrali provvedono a:

- istituire almeno una casella di posta elettronica istituzionale ed una casella di posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, per ciascun registro di protocollo;
- utilizzare la posta elettronica per le comunicazioni tra l'amministrazione ed i propri dipendenti, nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.

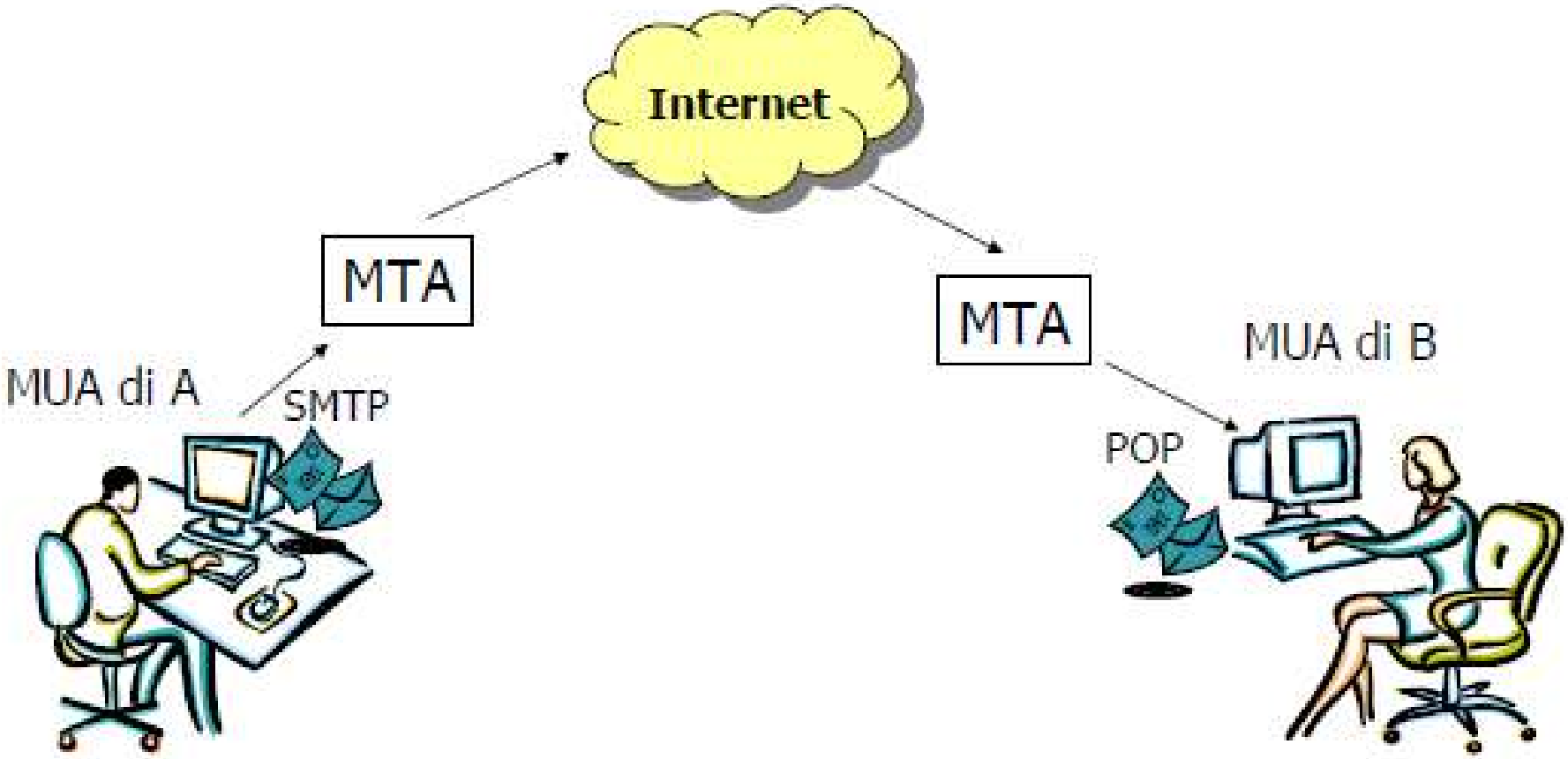
Art. 48. Posta elettronica certificata

1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.
2. La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta.
3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso mediante posta elettronica certificata sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche.

PEC - Definizione

- La Posta Elettronica Certificata è un sistema di posta elettronica con la quale si fornisce al mittente documentazione elettronica, con valore legale, attestante l'invio e la consegna di documenti informatici.
- "Certificare" l'invio significa fornire al mittente, dal proprio gestore di posta, una ricevuta che costituisce prova legale dell’avvenuta spedizione del messaggio.
- "Certificare" la ricezione significa inviare al mittente la ricevuta di avvenuta (o mancata) consegna con precisa indicazione temporale.

Posta elettronica ‘ordinaria‘
Richiamo - Schema generale



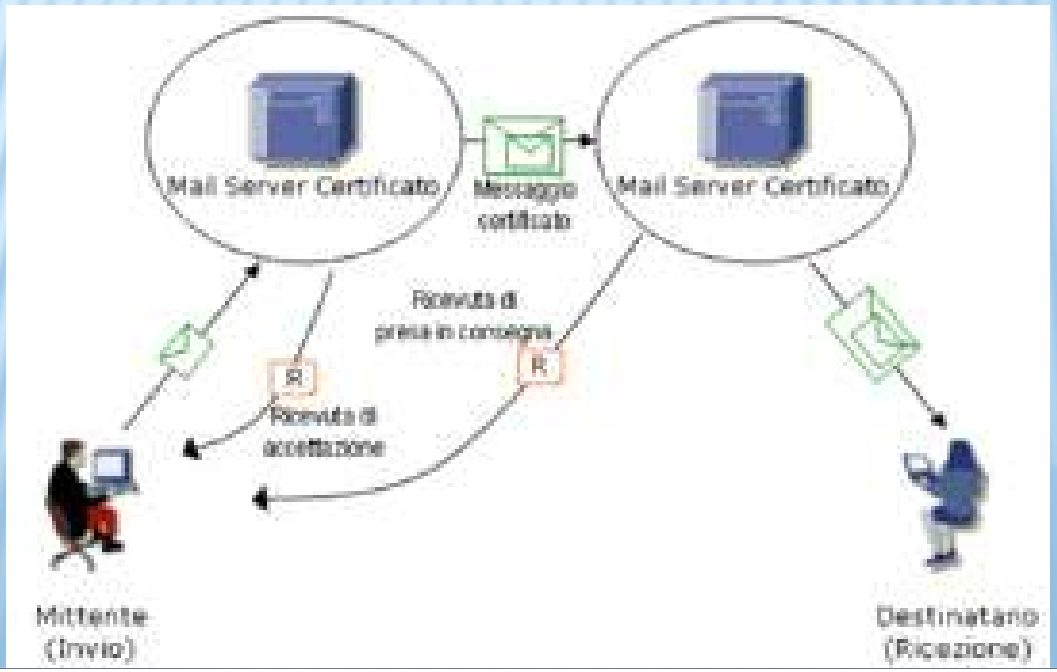
Posta elettronica ‘ordinaria’ Messaggi d’errore

- L’indirizzo di posta elettronica errato o inesistente
- Casella di posta elettronica piena

- In assenza di risposta il messaggio si considera consegnato.
- La conferma di lettura è un opzione facoltativa per il destinatario.

Posta elettronica certificata
Richiamo - Schema generale

- Rispetto allo schema generale della posta elettronica “ordinaria” ora gli MTA (Mail Transfer Agent) sia del mittente che del destinatario sono entrambi certificati secondo procedure e regolamenti stabiliti per legge.
- Le varie ricevute (accettazione, presa in consegna e ricezione) sono garantite a livello del sistema.



Sistema di invio e ricezione

Da un punto di vista più tecnico i messaggi di posta elettronica certificata utilizzano il protocollo S/MIME, la sicurezza del colloquio tra mittente e destinatario viene garantita in tutte le fasi dall'invio alla ricezione della mail certificata.

- Il mittente deve identificarsi presso il gestore di pec (autenticazione)
- L'integrità e la confidenzialità delle connessioni tra il gestore di posta certificata e l'utente devono essere garantite mediante l'uso di protocolli sicuri (utilizzo di protocolli quali TLS).
- I messaggi generati dal sistema di pec sono sottoscritti dai gestori mediate la firma digitale del gestore di posta elettronica certificata.
- Il colloquio tra i gestori deve avvenire con l'impiego del protocollo SMTP su trasporto TLS.
- Il destinatario deve identificarsi presso il gestore di pec (autenticazione) per potere leggere le mail in arrivo.

Attori

Gli attori coinvolti nel sistema della posta elettronica certificata sono :

- Gestori di posta elettronica certificata – sono dei provider di posta elettronica accreditati presso il CNIPA (Centro Nazionale per L'informatica nella Pubblica Amministrazione) con una procedura particolare. Devono sottostare a obblighi relativi alla gestione del servizio.
- Utilizzatori – utenti che fanno richiesta di una casella di posta certificata ai vari provider e che successivamente comunicano agli organismi interessati (PA, enti, associazioni etc...) di volersi avvalere del servizio PEC per le comunicazioni ufficiali.
- Il CNIPA (Centro Nazionale per L'informatica nella Pubblica Amministrazione) che è l'organo pubblico preposto al controllo ed alla vigilanza sulla attività dei gestori della posta elettronica certificata.

Gestori di PEC

Le società e/o enti che vogliono diventare provider di posta elettronica certificata devono essere accreditati presso il CNIPA e sottostare al D.M. del 2/11/2005 “Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata”

Il CNIPA nel riconoscimento del gestore valuta tra l’altro, adeguatezza del personale, processi atti a garantire la sicurezza dei dati e delle trasmissioni, ridondanza e servizi messi in atto in caso di emergenza.

L’elenco dei gestori di PEC è pubblico e consultabile presso il sito del CNIPA www.cnipa.gov.it

Gestore di PEC - Obblighi

I gestori della posta elettronica certificata devono sottostare a obblighi.

Alcuni tra questi garantire :

- l'interoperabilità dei servizi offerti
- l'inalterabilità dei documenti trasmessi
- tenere traccia delle operazioni svolte, in un apposito log, per una durata di trenta mesi garantendone la riservatezza, la sicurezza, l'integrità e l'inalterabilità oltre che le ricevute di avvenuta e/o mancata consegna in modo da poterle riprodurre nel caso in cui il mittente le smarrisca.
- individuare e gestire secondo le regole tecniche gli eventuali messaggi contenenti virus
- Garantire dei livelli minimi di servizio

Utilizzi

La posta elettronica certificata può essere paragonata ad una raccomandata con ricevuta di ritorno con però alcune differenze, cioè:

- La conoscenza del mittente cioè della casella del mittente (nel caso della raccomandata non è noto il mittente)
- La certificazione che il contenuto ricevuto è esattamente quello che era stato inviato (questo perchè alla ricevuta di ricezione viene allegato il documento spedito)

La PEC può essere utilizzata nella dematerializzazione dei documenti nella pubblica amministrazione garantendone la autenticità, temporalità e producendo documenti che hanno carattere legale.

esempio

Ambito operativo - Cittadino

Comunicazioni privato cittadino e PA.

Il privato cittadino può richiedere su base volontaria una casella di posta elettronica certificata ed utilizzarla (previa dichiarazione) nell'ambito di ciascun procedimento con la PA. La PA deve istituire almeno una casella di posta elettronica certificata (L. 82/05 art. 4).

www.postacertificata.gov.it

Ambito operativo – Pubblica Amministrazione

Comunicazioni tra PA e PA.

Il Codice dell'Amministrazione Digitale stabilisce relativamente alla posta elettronica certificata l'obbligo di istituire almeno una casella di posta elettronica certificata ed di utilizzare la PEC in tutti quei casi in cui è necessaria l'evidenza dell'avvenuto invio e ricezione del documento informatico.

L' utilizzo di PEC per le comunicazioni all'interno della PA determina uno snellimento a livello burocratico ed una velocizzazione di iter propri della PA come per esempio la gestione della protocollazione dei documenti che potrebbe essere fatta in automatico.

Ambito operativo – Imprese e Professionisti

Comunicazioni imprese, professionisti con la PA e tra di loro.

Le Camere di Commercio mettono a disposizione delle imprese una casella di Posta Elettronica Certificata che possono richiedere ed utilizzare sia per corrispondenza con la PA stessa ed altri enti. La casella di posta certificata di fatto assume il significato di domicilio a cui possono essere inviate comunicazione di vario tipo e natura con valore legale.

Le aziende possono utilizzare la posta elettronica certificata anche per comunicazioni di tipo economico e/o giuridico (es. l'invio di un contratto), per comunicazioni con la PA (dalla comunicazione di variazioni statutarie alla Camera di Commercio, alle comunicazioni con enti di previdenza INPS, INAIL, Fondi di previdenza ecc...)

Professionisti per la trasmissione di atti e comunicazioni alla Cancelleria del Tribunale, Prefetture etc...

Che cosa si certifica

Che cosa viene certificato con un messaggio inviato tramite servizio di posta elettronica certificata:

1) Autenticazione del mittente (provenienza certa del messaggio)
2) Autenticità del contenuto del messaggio (sia in termini di correttezza formale cioè assenza da virus, sia in termini di garanzia del contenuto e assenza di alterazione durante la trasmissione)
3) Avvenuta/mancata ricezione del messaggio da parte del provider del destinatario
4) Marcatura temporale opponibile a terzi.

Che cosa si certifica

Il servizio di PEC si dice “completo” cioè produce certificazioni a valore legale solo se sia mittente che destinatario utilizzano caselle di posta elettronica certificata (in questo caso il documento inviato con marcatura temporale è equivalente ad una raccomandata con ricevuta di ritorno e pertanto opponibile a terzi).

É comunque possibile inviare mail da indirizzo di posta elettronica certificata ad un indirizzo normale in questo caso l’unica ricevuta prodotta dal sistema è quella di accettazione. L’invio di mail da un indirizzo ordinario a un indirizzo pec invece potrebbe o non essere accettato dal gestore di PEC oppure arrivare al destinatario ma all’interno di una busta di anomalia.

Invio da PEC a server ordinario di posta

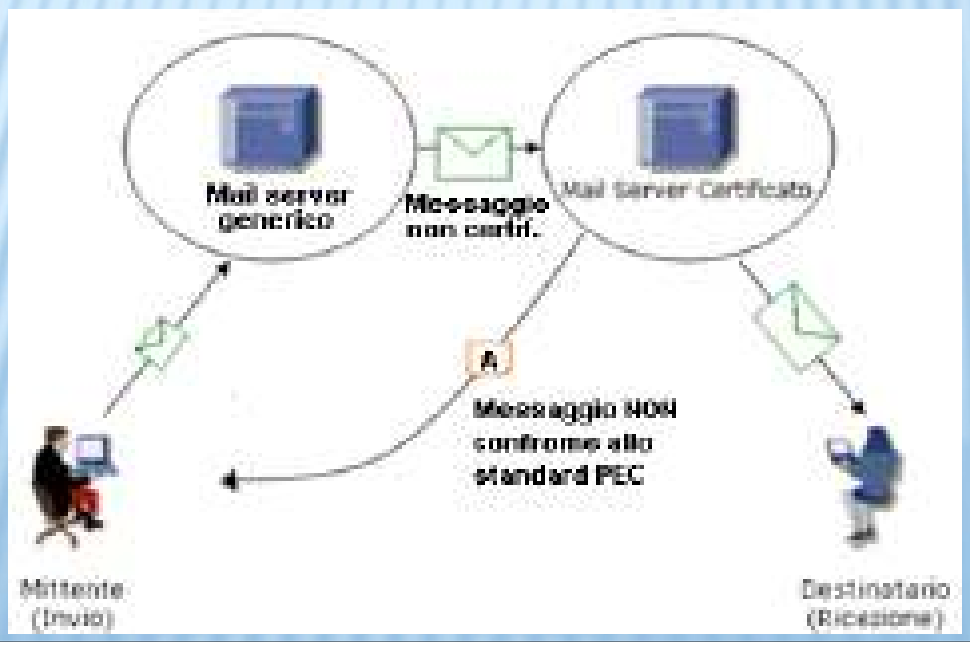
Invio di messaggio da server di posta elettronica certificata a server di posta ordinaria.

Il mittente ha solo evidenza dell'avvenuta ricezione (temporalmente valida) da parte del mail server di invio ma non della presa in consegna e lettura del messaggio da parte mail server del ricevente.

Invio da server ordinario di posta a server PEC

Invio di messaggio da server di posta elettronica generica a server di posta elettronica certificata

Il server PEC del ricevente può rigettare la mail ricevuta (quindi il destinatario pec non la leggerà) oppure ha la facoltà di inserirla in una busta di anomalia (non di errore) la quale segnala al mittente che il messaggio è leggibile ma non conforme allo standard PEC.



Vantaggi

I vantaggi dell'introduzione della PEC e del suo utilizzo sono:

- Certificazione dell'avvenuta consegna del messaggio
- Certificazione degli allegati del messaggio
- Possibilità di allegare al messaggio qualsiasi tipologia di informazione/documento in formato digitale
- Archiviazione (per 30 mesi) da parte del gestore di tutti gli eventi con le ricevute ed esclusione dei messaggi originali
- Semplicità di trasmissione, inoltro e ricerca dei messaggi
- Economicità rispetto alla raccomandata tradizionale
- Possibilità di invio multiplo a più destinatari
- Tracciabilità della casella del mittente
- Velocità di consegna (come la e-mail tradizionale)
- Consultazione della casella di posta anche al di fuori del proprio ufficio/abitazione
- Garanzia di privacy e sicurezza

ART. 54. CONTENUTO DEI SITI DELLE PUBBLICHE AMMINISTRAZIONI

1. I siti delle pubbliche amministrazioni contengono necessariamente i seguenti dati pubblici:
a. l'organigramma, l'articolazione degli uffici, le attribuzioni e l'organizzazione di ciascun ufficio anche di livello dirigenziale non generale, i nomi dei dirigenti responsabili dei singoli uffici, nonchè il settore dell'ordinamento giuridico riferibile all'attività da essi svolta, corredati dai documenti anche normativi di riferimento;

b. l'elenco delle tipologie di procedimento svolte da ciascun ufficio di livello dirigenziale non generale, il termine per la conclusione di ciascun procedimento ed ogni altro termine procedimentale, il nome del responsabile e l'unità organizzativa responsabile dell'istruttoria e di ogni altro adempimento procedimentale, nonchè dell'adozione del provvedimento finale, come individuati ai sensi degli articoli 2, 4 e 5 della legge 7 agosto 1990, n. 241;

c. le scadenze e le modalità di adempimento dei procedimenti individuati ai sensi degli articoli 2 e 4 della legge 7 agosto 1990, n. 241;

d. l'elenco completo delle caselle di posta elettronica istituzionali attive, specificando anche se si tratta di una casella di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68;

e. le pubblicazioni di cui all'articolo 26 della legge 7 agosto 1990, n. 241, nonchè i messaggi di informazione e di comunicazione previsti dalla legge 7 giugno 2000, n. 150;

f. l'elenco di tutti i bandi di gara e di concorso;

g. l'elenco dei servizi forniti in rete già disponibili e dei servizi di futura attivazione, indicando i tempi previsti per l'attivazione medesima.

ART. 54. CONTENUTO DEI SITI DELLE PUBBLICHE AMMINISTRAZIONI

2-ter. Entro il 30 giugno 2009, le amministrazioni pubbliche che già dispongono di propri siti sono tenute a pubblicare nella pagina iniziale del loro sito un indirizzo di posta elettronica certificata a cui il cittadino possa rivolgersi per qualsiasi richiesta ai sensi del presente codice. Le amministrazioni devono altresì assicurare un servizio che renda noti al pubblico i tempi di risposta, le modalità di lavorazione delle pratiche e i servizi disponibili.

Art. 54. Contenuto dei siti delle pubbliche amministrazioni

3. I dati pubblici contenuti nei siti delle pubbliche amministrazioni sono fruibili in rete gratuitamente e senza necessità di autenticazione informatica.
4. Le pubbliche amministrazioni garantiscono che le informazioni contenute sui siti siano conformi e corrispondenti alle informazioni contenute nei provvedimenti amministrativi originali dei quali si fornisce comunicazione tramite il sito.

4-bis. La pubblicazione telematica produce effetti di pubblicita' legale nei casi e nei modi espressamente previsti dall'ordinamento.

Art. 57. Moduli e formulari

1. Le pubbliche amministrazioni provvedono a definire e a rendere disponibili anche per via telematica l'elenco della documentazione richiesta per i singoli procedimenti, i moduli e i formulari validi ad ogni effetto di legge, anche ai fini delle dichiarazioni sostitutive di certificazione e delle dichiarazioni sostitutive di notorietà.
2. Trascorsi ventiquattro mesi dalla data di entrata in vigore del presente codice, i moduli o i formulari che non siano stati pubblicati sul sito non possono essere richiesti ed i relativi procedimenti possono essere conclusi anche in assenza dei suddetti moduli o formulari.

Art. 57-bis. Indice degli indirizzi delle pubbliche amministrazioni

1. Al fine di assicurare la trasparenza delle attività istituzionali è istituito l'indice degli indirizzi delle amministrazioni pubbliche, nel quale sono indicati la struttura organizzativa, l'elenco dei servizi offerti e le informazioni relative al loro utilizzo, gli indirizzi di posta elettronica da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti a tutti gli effetti di legge fra le amministrazioni e fra le amministrazioni ed i cittadini.

www.indicepa.gov.it

Art. 63. Organizzazione e finalità dei servizi in rete

1. Le pubbliche amministrazioni centrali individuano le modalità di erogazione dei servizi in rete in base a criteri di valutazione di efficacia, economicità ed utilità e nel rispetto dei principi di eguaglianza e non discriminazione, tenendo comunque presenti le dimensioni dell'utenza, la frequenza dell'uso e l'eventuale destinazione all'utilizzazione da parte di categorie in situazioni di disagio.
2. Le pubbliche amministrazioni centrali progettano e realizzano i servizi in rete mirando alla migliore soddisfazione delle esigenze degli utenti, in particolare garantendo la completezza del procedimento, la certificazione dell'esito e l'accertamento del grado di soddisfazione dell'utente.
3. Le pubbliche amministrazioni collaborano per integrare i procedimenti di rispettiva competenza al fine di agevolare gli adempimenti di cittadini ed imprese e rendere più efficienti i procedimenti che interessano più amministrazioni, attraverso idonei sistemi di cooperazione.

Art. 64. Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni

1. La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'autenticazione informatica.
2. Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'autenticazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano di accertare l'identità del soggetto che richiede l'accesso. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.

Art. 65. Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica

1. Le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica ai sensi dell'articolo 38, commi 1 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sono valide:

   a. se sottoscritte mediante la firma digitale, il cui certificato è rilasciato da un certificatore accreditato;
   b. ovvero, quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente;
   c. ovvero quando l'autore è identificato dal sistema informatico con i diversi strumenti di cui all'articolo 64, comma 2, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente e fermo restando il disposto dell'articolo 64, comma 3.c-bis) ovvero quando l'autore è identificato dal sistema informatico attraverso le credenziali di accesso relative all'utenza personale di posta elettronica certificata di cui all'articolo 16-bis del decreto-legge 29 novembre 2008, n. 185, convertito con modificazioni, dalla legge 28 gennaio 2009, n. 2.

Conclusioni

Organizzazione delle PP.AA.

Art. 12. Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa

- Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione.

Formazione

Art. 13. Formazione informatica dei dipendenti pubblici

- Le pubbliche amministrazioni nella predisposizione dei piani di cui all'articolo 7-bis, del decreto legislativo 30 marzo 2001, n. 165, e nell'ambito delle risorse finanziarie previste dai piani medesimi, attuano anche politiche di formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione.

Riorganizzazione

Art. 15. Digitalizzazione e riorganizzazione

- La riorganizzazione strutturale e gestionale delle pubbliche amministrazioni volta al perseguimento degli obiettivi di cui all'articolo 12, comma 1, avviene anche attraverso il migliore e più esteso utilizzo delle tecnologie dell'informazione e della comunicazione nell'ambito di una coordinata strategia che garantisca il coerente sviluppo del processo di digitalizzazione.
- In attuazione del comma 1, le pubbliche amministrazioni provvedono in particolare a razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese, assicurando che l'utilizzo delle tecnologie dell'informazione e della comunicazione avvenga in conformità alle prescrizioni tecnologiche definite nelle regole tecniche di cui all'articolo 71.

Obbligatorietà?

Art. 2. Finalità e ambito di applicazione

comma 2 bis

- Tutte le disposizioni previste dal presente codice per le pubbliche amministrazioni si applicano, ove possibile tecnicamente e a condizione che non si producano nuovi o maggiori oneri per la finanza pubblica ovvero, direttamente o indirettamente, aumenti di costi a carico degli utenti, anche ai soggetti privati preposti all'esercizio di attività amministrative.

Obbligatorietà?

Art. 2. Finalità e ambito di applicazione
Comma 6

- Le disposizioni del presente codice non si applicano limitatamente all'esercizio delle attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, e consultazioni elettorali

Grazie per l’attenzione

www.vincenzocalabro.it