REGIONE SICILIANA

Sicilia e-Servizi

CENTRI SERVIZI TERRITORIALI

Posta Elettronica Certificata e Firma Digitale

***CST Monterraneo**, 6 Aprile 2011*

Agenda

Posta Elettronica Certificata

- *Cos'è*
- *Riferimenti normativi*
- *Soggetti*
- *Flusso dei messaggi*
- *Vantaggi*
- *PEC nella Pubblica Amministrazione*
- *Modalità di richiesta della PEC*
- *Pec per il cittadino*
- *Definizioni*

Firma Digitale

- *Cos'è*
- *Riferimenti normativi*
- *Soggetti*
- *Elementi per firmare*
- *Come funziona*
- *Vantaggi*
- *Definizioni*

Cos'è

La **Posta Elettronica Certificata (PEC)** è un tipo speciale di **e-mail** che consente di inviare e ricevere messaggi di testo allegati con lo stesso valore legale di una raccomandata con avviso di ricevimento.

La **Posta Elettronica Certificata** fornisce al mittente la documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici.

E' quindi un sistema in grado di sfruttare al meglio le potenzialità della posta elettronica tradizionale superandone le "debolezze".

Rappresenta
la soluzione ideale per quei contesti nei quali è necessario avere prova certa dell'invio e della consegna di un determinato documento.

Riferimenti normativi 1/3

I principali riferimenti normativi in materia di Posta Elettronica Certificata sono:

- ***DPR 68/2005***
  Definisce i soggetti del servizio di PEC, l'obbligo per i gestori di garantire l'interoperabilità, la garanzia circa l'integrità del messaggio trasmesso, l'obbligo per i gestori di tenere traccia delle operazioni svolte, le regole per la gestione dei messaggi contenenti virus, l'obbligo per i gestori di garantire livelli minimi di servizio, definizione dell'elenco pubblico dei gestori di PEC, l'elenco dei requisiti che devono possere i gestori PEC, l'assegnazione al DigitPA (ex CNIPA) delle funzioni di vigilanza e controllo sull'attività dei gestori, i limiti di utilizzo delle caselle di PEC.

- ***Decreto Ministeriale 2/11/2005***
  Definisce le regole tecniche relative alle modalità di realizzazione e funzionamento della posta elettronica certificata di cui al DPR 68/2005 ed i requisiti tecnico/funzionali necessari alla realizzazione della piattaforma software per l'erogazione del servizio.

- ***Circolare di accreditamento DigitPA CR/49 24-11-2005***
  Definisce le modalità per la presentazione delle domande di iscrizione all'elenco pubblico dei gestori di posta elettronica certificata.

- ***Circolare di vigilanza DigitPA CR/51 7/12/2006***
  Fornisce gli elementi di dettaglio in relazione alle modalità con le quali il DigitPA esercita la vigilanza nei confronti dei gestori iscritti nell'elenco pubblico.

Riferimenti normativi 2/3

- ***D.L 185/2008 convertito in Legge n°2/2009***
  Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale (G.U. n. 280 del 29 novembre 2008, S.O. n. 263)
  La legge introduce l'obbligatorietà della PEC per le imprese costituite in forma societaria e per i per i professionisti iscritti agli Ordini. Gli Enti pubblici sono invece tenuti a pubblicare i propri indirizzi PEC sull'Indice delle PA. Inoltre, tutte le comunicazioni tra Enti pubblici, professionisti ed imprese possono avvenire via PEC, senza che il destinatario debba dichiarare la propria disponibilità ad accettarne l'utilizzo.

- ***DCPM 6 maggio 2009***
  Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini.
  Il decreto stabilisce di concedere gratuitamente una casella di posta certificata a tutti i cittadini che ne facciano richiesta, in attuazione dell'articolo 8 del CAD, per il quale lo Stato deve promuovere iniziative volte a favorire l'alfabetizzazione informatica dei cittadini, anche al fine di favorire l'utilizzo dei servizi telematici delle PA.

Riferimenti normativi 3/3

- ***NUOVO Codice dell'Amministrazione Digitale (CAD):*** *Dlgs 82/2005* – Codice dell'Amministrazione digitale", modificato dal d. lgs. 235/2010:

  - Principale mezzo di comunicazione per il cittadino nella presentazione di istanze verso le pubbliche amministrazioni;
  - Lo strumento che le pubbliche amministrazioni sono tenute ad utilizzare quando a fare richiesta in tale senso è il cittadino stesso;
  - La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, salvo che la legge non disponga diversamente (*nei casi consentiti dalla legge)* alla notificazione per mezzo della posta;
  - Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono (di norma) mediante l'utilizzo della posta elettronica e sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza:
    - Segnatura di protocollo;
    - Firma digitale o firma elettronica qualificata;
    - PEC;
    - Le comunicazioni inviate via PEC devono essere protocollate (art. 40 bis);
    - Obbligo per le amministrazioni a pubblicare nell'Indice delle Pubbliche amministrazioni –IPA – almeno una PEC per ogni registro di protocollo;
    - Le amministrazioni possono accedere agli elenchi di titolari di casella di posta elettronica certificata (regole tecniche con Garante).

Valore aggiunto della PEC 1/2

Rispetto alla **e-mail tradizionale**, la PEC assicura:

- opponibiltà a terzi delle ricevute di invio e ricezione dei messaggi,
- certificazione dell'invio e della consegna del messaggio elettronico,
- livelli minimi di qualità del servizio e di sicurezza delle comunicazioni stabiliti per legge.

Rispetto al **Fax**, la PEC assicura:

- semplicità ed economicità di trasmissione,
- inoltro, produzione, archiviazione e ricerca,
- possibilità di invii multipli a più destinatari contemporaneamente con costi economici molto più contenuti,
- opponibiltà a terzi delle ricevute di invio e ricezione dei messaggi.

Rispetto alla **Consegna brevi manu,** la PEC assicura:

- semplicità ed economicità di trasmissione,
- inoltro, produzione, archiviazione e ricerca,
- possibilità di invii multipli a più destinatari contemporaneamente con costi economici molto più contenuti,
- velocità di comunicazione,
- sistema di comunicazione asincrono che non prevede la necessaria presenza del destinatario al momento della consegna.

Valore aggiunto della PEC 2/2

Rispetto alla **Raccomandata A/R**, la PEC assicura:

- semplicità ed economicità di trasmissione,
- inoltro, produzione, archiviazione e ricerca,
- possibilità di invii multipli a più destinatari contemporaneamente con costi economici molto più contenuti,
- velocità di comunicazione e sistema di comunicazione asincrono che non prevede la necessaria presenza del destinatario al momento della consegna,
- integrazione nella ricevuta di consegna del contenuto del messaggio originale.

La tabella seguente contiene in sintesi il valore aggiunto dell'utilizzo della PEC.

	Valore aggiunto della PEC
PEC vs. e-mail	Certezza consegna – Valore legale – Certezza casella mittente
PEC vs. FAX	Velocità e semplicità – Valore legale – Ubiquità
PEC vs. Consegna Brevi Manu	Velocità e semplicità – Costi - Ubiquità
PEC vs. raccomandata A/R	Certezza del contenuto – Ubiquità – Velocità e semplicità – Costi – Tracciabilità mittente

Soggetti

La normativa definisce i soggetti che intervengono nell'utilizzo di una casella PEC per l'invio di un messaggio di posta elettronica.

- ***Mittente***

  Utente che si avvale del servizio di posta elettronica certificata per la trasmissione di documenti prodotti medianti strumenti informatici.

- ***Destinatario***

  Utente che si avvale del servizio di posta elettronica certificata per la ricezione di documenti prodotti mediante strumenti informatici.

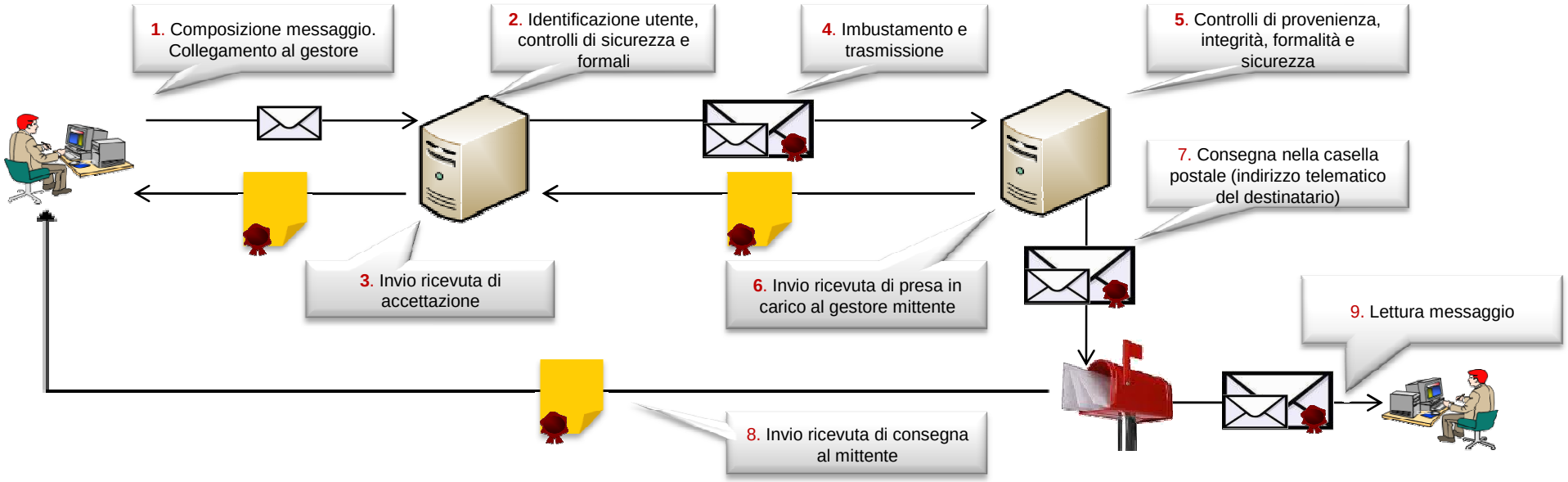
- ***Gestore del servizio***

  Soggetto pubblico o privato che eroga il servizio e gestisce domini di PEC. In particolare deve:
  - soddisfare i requisiti necessari per l'iscrizione all'elenco pubblico dei certificatori, definiti dalla normativa vigente,
  - Garantire l'interoperabilità con gli altri gestori, i livelli minimi di servizio ed il il tracciamento delle operazioni svolte, in un apposito log, per una durata di trenta mesi, garantendone la riservatezza, la sicurezza, l'integrità e l'inalterabilità

- ***Digit PA***

  Ha competenze sia nei confronti dei gestori sia nei confronti degli Enti pubblici.

Flusso dei messaggi 1/2



1. L'utente predispone l'oggetto e si fa riconoscere dal sistema di PEC del proprio gestore.

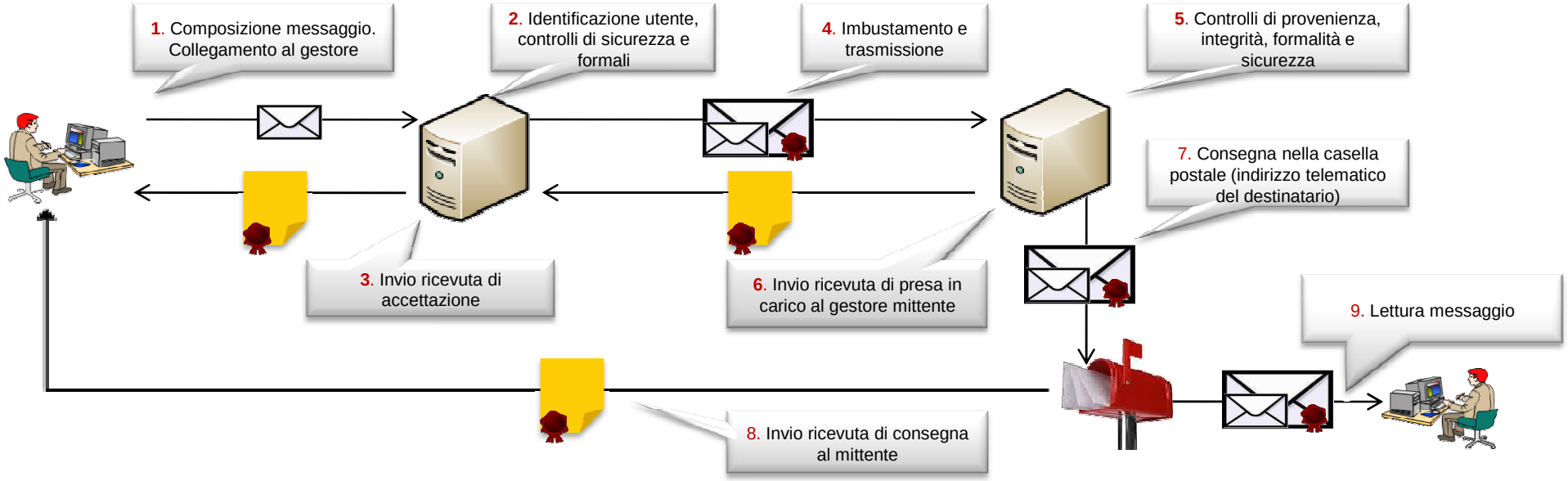
2. Il messaggio viene ricevuto dal gestore del mittente che procede all'identificazione dell'utente, ai controlli formali e di sicurezza.

3. Terminati i controlli, il gestore del mittente invia la ricevuta di accettazione del messaggio al mittente.

4. Il gestore del mittente procede ad inserire, come allegato, il messaggio preparato dal mittente e a firmarlo digitalmente (busta di trasporto) e, quindi, lo invia al Gestore destinatario.

5. Il messaggio imbustato viene ricevuto dal gestore del destinatario che procede ai controlli di provenienza, integrità, formali e di sicurezza.

Flusso dei messaggi 2/2



6 Terminati i controlli, il gestore del destinatario invia la ricevuta di presa in carico del messaggio elettronico al gestore del mittente.

7 Il gestore del destinatario inoltra nella casella postale del destinatario, all'indirizzo telematico, il messaggio di posta.

8 Dalla casella di posta del destinatario viene inviata la ricevuta di consegna del messaggio al mittente. Tale ricevuta attesta che il messaggio inviato dal mittente è stato depositato nella casella del destinatario ed è firmata elettronicamente dal gestore destinatario al fine di garantire la validità giuridica della stessa nei casi di utilizzo.

9 Infine, l'utente destinatario procede alla lettura del messaggio di posta.
N.B. Il sistema PEC certifica la consegna nella casella del destinatario, non la lettura del messaggio.

Vantaggi della PEC

I maggiori vantaggi derivanti dall'utilizzo di una casella di Posta Elettronica Certificata sono i seguenti.

- **Certificazione dell'avvenuta consegna** del messaggio nella casella di posta del destinatario del messaggio e dei suoi contenuti.
- **Certificazione degli allegati** al messaggio.
- **Opponibilità a terzi** della provenienza e del recapito del messaggio, della data e dell'ora di trasmissione e della ricezione di un messaggio.
- **Archiviazione** da parte del gestore di tutti gli eventi associati ad invii e ricezioni, per un periodo di trenta mesi.
- **Inalterabilità** del messaggio.
- **Tracciabilità** della casella mittente e, quindi, del suo titolare.

PEC nella Pubblica Amministrazione

La diffusione della PEC rientra nelle attuali priorità del processo di "dematerializzazione" della burocrazia. All'interno del **Piano di e-Governement 2012** è incluso il progetto "**Casella elettronica Certificata**" che mira a digitalizzare completamente i flussi documentali tra amministrazione e cittadini.

Nell'ambito della Pubblica Amministrazione la PEC costituisce un'opportunità e, al contempo, un obbligo.

Obblighi

- Obbligo di istituzione e pubblicazione di una casella di posta certificata per ciascun registro di protocollo.
- Utilizzo della posta elettronica certificata per la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna (art.48 - codice amministrazione digitale).
- Pubblicazione nei siti delle amministrazioni pubbliche di un indirizzo di posta elettronica certificata a cui il cittadino possa rivolgersi per qualsiasi richiesta ai sensi del codice.
- Diritto per i cittadini di ottenere l'utilizzo della PEC da parte delle amministrazioni.

Benefici

- Riduzione dei costi
- Aumento di efficienza
- Velocizzazione della lavorazione delle pratiche
- Riduzione dei conteziosi in merito alla ricezione e invio di documenti

Modalità di richiesta della PEC per la PA

La Pubblica Amministrazione può acquisire la PEC ricorrendo al mercato mediante un Gestore che offre il servizio a pagamento oppure richiederla gratuitamente come nei casi di seguito indicati.

1

Nella sezione informativa del portale www.postacertificata.gov.it sono indicate le istruzioni per richiedere il servizio PostaCertificat@.

Condizione necessaria è la preventiva iscrizione della Pubblica Amministrazione **all'indice della Pubblica Amministrazione (IPA).**

Per poter avere informazioni sul servizio, la Pubblica Amministrazione potrà contattare il Call Center accessibile al numero verde **800.104.464** (da rete fissa) oppure al **199.135.191**, disponibile dalle 8:00 alle 20:00, dal lunedì al sabato.

ATTENZIONE: La casella PostaCertificat@ presenta delle limitazioni di utilizzo indicate nei manuali

2

Anci, l'Associazione Nazionale dei Comuni Italiani, propone gratuitamente a tutti i Sindaci l'attivazione di un proprio account di posta elettronica certificata, secondo lo standard **nome.cognome@pec.anci.it**.

Il sito di riferimento è **http://www.pec.ancitel.it/index.cfm?m=8**

3

In fase di realizzazione: PEC per i dipendenti pubblici per tutte le comunicazioni con gli Enti di riferimento (PAC,INPS, INPDAP…)

PEC per il Cittadino

Ad aprile 2010 è stata avviata l'iniziativa CEC-PAC Postacertificat@: PEC gratuita ai cittadini per le comunicazioni con le PA iscritte all'indice IPA

La PostaCertificat@ è un servizio di comunicazione elettronica tra Cittadino e Pubblica Amministrazione. Il servizio è offerto a titolo gratuito e si rivolge a tutti i cittadini italiani maggiorenni che ne facciano richiesta (anche se residenti all'estero).

I cittadini accettano automaticamente l'invio di atti e provvedimenti che li riguardano da parte delle pubbliche amministrazioni una volta dichiarato il proprio indirizzo PEC

Possono trovare gli indirizzi di PEC dei diversi enti all'indirizzo: www.indicepa.gov.it.

Riferimenti utili

Per informazioni tecniche e quesiti sul servizio PEC in generale contattare i seguenti numeri:

- Numero verde gratuito gestito da Formez PA (Linea Amica): 803.001;
- Da rete fissa numero verde gratuito: 800.104. 464 .

Per informazioni sull'iniziativa Postacertificat@ al Cittadino contattare:

- Da rete mobile il numero: 199.135.191;
  (numeri gestiti da Poste Italiane assieme a Telecom Italia e Postecom);
- Sito web : www.postacertificata.gov.it

Definizioni 1/3

- **Punto di accesso:** è il punto che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione, di imbustamento del messaggio originale nella busta di trasporto.

- **Punto di ricezione:** è il punto che riceve il messaggio all'interno di un dominio di posta elettronica certificata, effettua i controlli sulla provenienza/correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta di anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta ordinaria e delle buste di trasporto.

- **Punto di consegna:** è il punto che compie la consegna del messaggio nella casella di posta elettronica certificata del titolare destinatario. Verifica la provenienza/correttezza del messaggio, emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna.

- **Ricevuta di accettazione:** è la ricevuta, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta elettronica certificata. La ricevuta di accettazione è firmata con la chiave del gestore di posta elettronica certificata del mittente.

- **Avviso di non accettazione:** è l'avviso che viene emesso quando il gestore mittente è impossibilitato ad accettare il messaggio in ingresso. La motivazione per cui non è possibile accettare il messaggio è inserita all'interno del testo della ricevuta che esplicita inoltre che il messaggio non potrà essere consegnato al destinatario. L'avviso di non accettazione è firmato con la chiave del gestore di posta elettronica certificata del mittente.

Definizioni 2/3

- **Ricevuta di presa in carico:** è emessa dal punto di ricezione verso il gestore di posta elettronica certificata mittente per attestare l'avvenuta presa in carico del messaggio da parte del dominio di posta elettronica certificata di destinazione. Nella ricevuta di presa in carico sono inseriti i dati di certificazione per consentirne l'associazione con il messaggio a cui si riferisce. La ricevuta di presa in carico è firmata con la chiave del gestore di posta elettronica certificata del destinatario.

- **Ricevuta di consegna:** il punto di consegna fornisce al mittente la ricevuta di avvenuta consegna nel momento in cui il messaggio è inserito nella casella di posta elettronica certificata del destinatario. È rilasciata una ricevuta di avvenuta consegna per ogni destinatario al quale il messaggio è consegnato. La ricevuta di avvenuta consegna è firmata con la chiave del gestore di posta elettronica certificata del destinatario.

- **Avviso di mancata consegna:** Nel caso in cui il gestore di posta elettronica certificata sia impossibilitato a consegnare il messaggio nella casella di posta elettronica certificata del destinatario, il sistema emette un avviso di mancata consegna per indicare l'anomalia al mittente del messaggio originale.

- **Messaggio originale:** è il messaggio originale inviato da un utente di posta elettronica certificata prima del suo arrivo al punto di accesso. Il messaggio originale è consegnato al titolare destinatario per mezzo di una busta di trasporto che lo contiene.

- **Busta di trasporto:** è il messaggio creato dal punto di accesso, all'interno del quale sono inseriti il messaggio originale inviato dall'utente di posta elettronica certificata ed i relativi dati di certificazione. La busta di trasporto è firmata con la chiave del gestore di posta elettronica certificata mittente. La busta di trasporto è consegnata immodificata nella casella di posta elettronica certificata di destinazione per permettere la verifica dei dati di certificazione da parte del ricevente.

Definizioni 3/3

- **Busta di anomalia:** quando un messaggio errato/non di posta elettronica certificata deve essere consegnato ad un titolare, esso viene inserito in una busta di anomalia per evidenziare al destinatario detta anomalia. La busta di anomalia è firmata con la chiave del gestore di posta elettronica certificata del destinatario.

- **Dati di certificazione:** è un insieme di dati che descrivono il messaggio originale e sono certificati dal gestore di posta elettronica certificata del mittente. I dati di certificazione sono inseriti nelle varie ricevute e sono trasferiti al titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto. Tra i dati di certificazione sono compresi: data ed ora di invio, mittente, destinatario, oggetto, identificativo messaggio, ecc.

- **Marca temporale:** E' un'evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi.

Agenda

Posta Elettronica Certificata

- *Cos'è*
- *Riferimenti normativi*
- *Soggetti*
- *Flusso dei messaggi*
- *Vantaggi*
- *La PEC nella Pubblica Amministrazione*
- *Modalità di richiesta della PEC*
- *Definizioni*

Firma Digitale

- *Cos'è*
- *Riferimenti normativi*
- *Soggetti*
- *Elementi per firmare*
- *Come funziona*
- *Vantaggi*
- *Definizioni*

La **Firma Digitale** consente:

- all'**autore** di un documento informatico, di renderne manifesta l'autenticità, analogamente a quanto avviene apponendo la firma autografa su un documento cartaceo di cui assume il medesimo valore legale.
- al **destinatario** del documento di verificarne la provenienza e l'integrità.

	Firme elettroniche prima del D.Lgs 235/2010
Firma elettronica	Insieme dei dati connessi tramite associazione logica ad altri dati elettronici utilizzati come metodo di identificazione informatica.
Firma elettronica qualificata	Basata su certificato qualificato, generata tramite un dispositivo sicuro.
Firma digitale	Basata su un certificato qualificato, generata tramite un dispositivo sicuro, basata su chiavi asimmetriche

Tipologie di firme dopo il D.Lgs 235/2010

	Definizione di firma digitale prevista dal Codice dell'Amministrazione Digitale
Firma elettronica	Insieme dei dati connessi tramite associazione logica ad altri dati elettronici utilizzati come metodo di identificazione informatica.
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.
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;
Firma elettronica qualificata	Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma

SARANNO EMANATE NUOVE REGOLE TECNICHE

Riferimenti normativi

I principali riferimenti normativi in materia Firma digitale sono:

- ***Direttiva europea 1999/93/CE***
  E' volta ad agevolare l'uso delle firme elettroniche e a contribuire al loro riconoscimento giuridico.

- ***D.lgs n° 10/2002***
  Reca le disposizioni legislative per il recepimento della direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche.

- ***DPR n° 445/2000 –***
  Testo unico delle disposizioni legislatice e regolamentari in materia di documentazione amministrativa.

- ***DPR n°137/2003***
  Regolamento recante disposizioni di coordinamento in materia di firme elettroniche. Modifica alcuni dei contenuti del DPR n°445/2000.

- **D. lgs 82/2005**
  Codice dell'amministrazione digitale (modificato dal d. lgs 159/2006 e d.lgs 235/2010)

- **DPCM 30 marzo 2009**
  Stabilisce, ai sensi degli articoli 20, 24 comma 4, 27, 28, 29, 30 e 32 del codice, le regole tecniche per la generazione, apposizione e verifica delle firme elettroniche qualificate e per la validazione temporale, nonché per lo svolgimento delle attività dei certificatori qualificati.

Soggetti

I soggetti che intervengono nell'utilizzo della Firma Digitale prima .

- ***Titolare***

  E' il possessore della coppia di chiavi asimmetriche che ha l'esigenza di firmare un documento informatico.

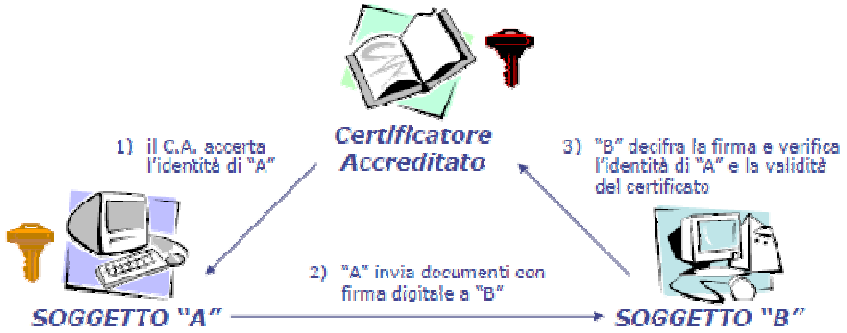
- ***Destinatario***

  Utente al quale è destinato il documento informatico firmato digitalmente e che decifra la firma e verifica l'identità del mittente e del certificato.

- ***Certificatore accreditato***

  Soggetto pubblico o privato che emette certificati conformi alla direttiva europea e alla normativa nazionale ed ha il compito di:
  - verificare e attestare l'identità del richiedente;
  - stabilire il termine di scadenza dei certificati, il periodo di validità delle chiavi e degli usi per i quali sono impiegate;
  - emettere e pubblicare il certificato, in un archivio pubblico gestito dallo stesso Certificatore;
  - revocare o sospendere i certificati.

  .



Elementi per firmare

Gli elementi necessari per apporre una firma digitale sono:

- Un dispositivo sicuro per la generazione delle firme quale, ad esempio, una smart card o un token usb.

- Un lettore di smart card, nel caso in cui non si utilizzi il token usb.
- Un software per la gestione del dispositivo e per la generazione delle firme digitali.
- Un certificato qualificato rilasciato da un Certificatore e deve riportare le seguenti informazioni:
  - Numero di serie.
  - Validità temporale.
  - Certificatore emittente.
  - Informazioni anagrafiche.
  - Chiave pubblica.
  - Firma del certificatore.
  - Limiti d'uso del certificato.

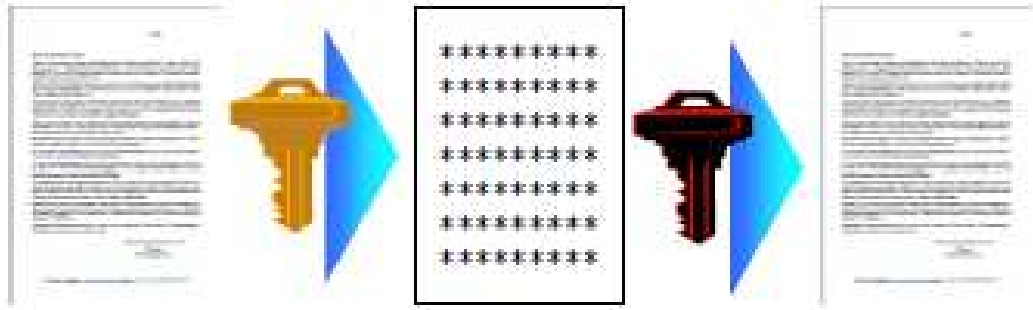
Come funziona 1/5

La firma digitale si basa su un sistema di crittografia **evoluto**, che utilizza una coppia di chiavi asimmetriche attribuite univocamente a un titolare.

La **chiave privata** è a disposizione esclusiva del titolare ed è protetta da un codice segreto conosciuto solo da lui. E' l'elemento della coppia di chiavi asimmetriche utilizzato dal titolare per apporre la firma digitale.

La **chiave pubblica**, anch'essa associata al titolare, è invece contenuta in un "Certificato Digitale" (documento informatico) reso accessibile a tutti su Internet dai **Certificatori Accreditati**. E' l'elemento della coppia di chiavi asimmetriche con il quale si verifica la firma digitale.

Un documento elettronico firmato (cifrato) con la chiave privata può essere verificato (de-cifrato) **esclusivamente** utilizzando la corrispondente chiave pubblica.



Come funziona 2/5

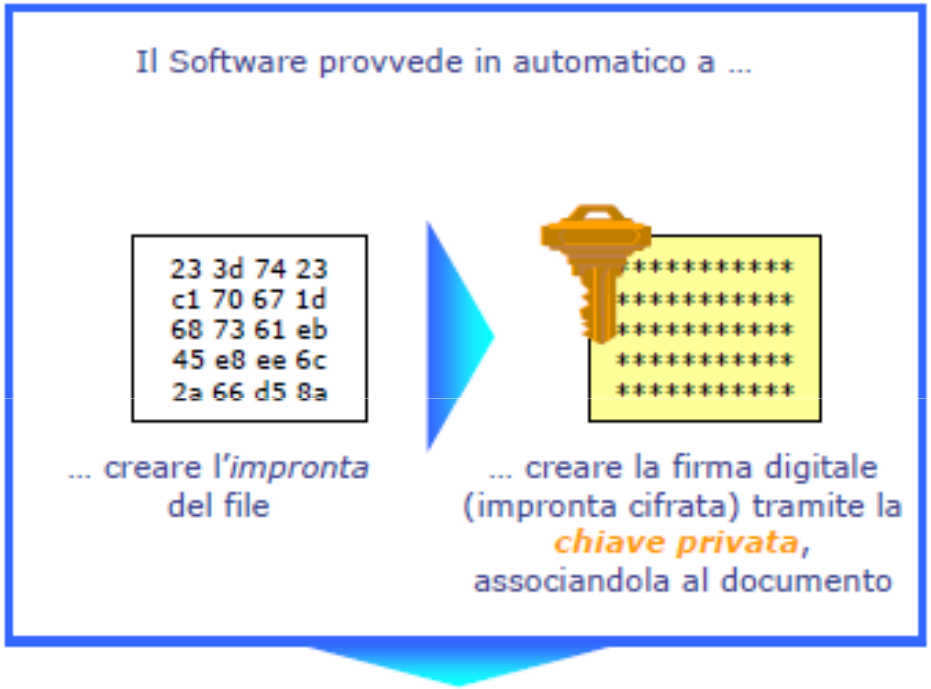
1

Cosa deve fare il soggetto **"A"** per apporre la propria firma digitale su un documento da inviare al soggetto **"B"*** .

* Data la varietà di sistemi e operatori presenti sul mercato il processo di seguito illustrato è a titolo esemplificativo.

Come funziona 3/5

2 Cosa fa il software quando **"A"** digita il comando di apposizione della firma.



L'**IMPRONTA** è una sorta di "riassunto" del documento: più breve, ma costruita in modo da risultare diversa anche a seguito di variazioni in uno solo dei caratteri digitati.

Il suo utilizzo evita al Software di cifrare l'intero documento.

Come funziona 4/5

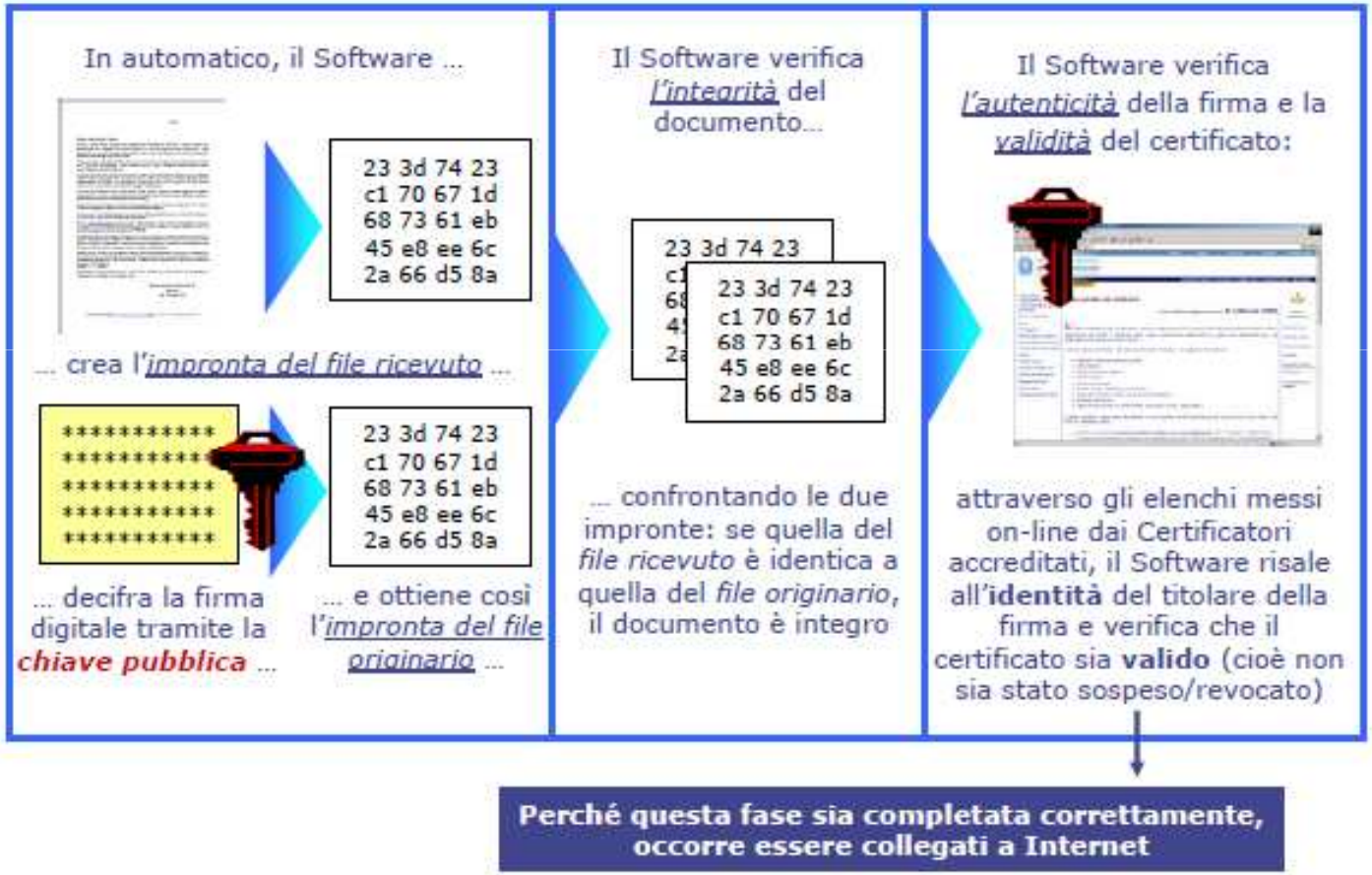
3

Cosa deve fare il soggetto **“B”** per verificare l’autenticità (integrità e paternità) del documento ricevuto da **“A”**

“B” deve semplicemente aprire il file affinché il software visualizzi un report sull’esito della verifica

Come funziona 5/5

4 Cosa fa il software quando **"B"** apre il file firmato.



Vantaggi

I vantaggi derivanti dall'utilizzo della firma digitale sono:

- **Autenticità** del sottoscrittore la cui identità è sempre nota e certa.
- **Integrità** del documento informatico che non può essere stato modificato dopo la sua sottoscrizione.
- **Non ripudio,** poichè il documento informatico sottoscritto con Firma Digitale ha piena validità legale e non può, quindi, essere ripudiato dal sottoscrittore.
- **Eliminazione dei documenti cartacei**

Definizioni 1/2

Di seguito sono riportate le definizioni descritte nel nuovo CAD:

- **Certificato qualificato:** insieme di informazioni che creano una stretta ed affidabile correlazione fra una chiave pubblica e i dati che identificano il Titolare. Sono certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva n. 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva.

- **Chiave privata:** la chiave della coppia utilizzata nel processo di sottoscrizione di un documento informatico L'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico.

- **Chiave pubblica:** la chiave della coppia utilizzata da chiunque esegua la verifica di una firma digitale l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche.

- **Dispositivo di firma:** insieme di dispositivi hardware e software che consentono di sottoscrivere con firma digitale documenti informatici.

- **Documento informatico:** è' costituito da qualunque oggetto informatico (file) che contenga atti, fatti o dati giuridicamente rilevanti.

- **Firma elettronica:** l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

- **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.

Definizioni 2/2

- **Firma elettronica qualificata:** un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.

- **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;

Link utili

- **DigitPA:**
  - http://www.digitpa.gov.it/pec
  - http://www.digitpa.gov.it/firma-digitale

- **Posta certificata:**
  - www.postacertificata.gov.it
  - http://www.pec.ancitel.it/index.cfm?m=8
  - www.indicepa.gov.it/