



UFFICI DI PROSSIMITÀ

la giustizia più vicina ai cittadini

**Servizio pubblico di informazione
e assistenza per la volontaria giurisdizione**

**INTRODUZIONE ALL'INFORMATICA GIURIDICA E GIUDIZIARIA
STRUMENTI DI INFORMATICA GIURIDICA: PEC E FIRMA DIGITALE**

Arianna Toniolo



Informatica giuridica e informatica giudiziaria

L'informatica giuridica è diretta alla conoscenza delle norme e delle decisioni adottate, permette cioè accedere a dati aggregati confrontandoli tra loro (cd. Information retrieval) e risponde ad una esigenza sempre più diffusa nella società moderna esigenza sentita non solo da parte degli operatori del diritto: giudici, avvocati, pubblici funzionari ma anche, e sempre di più, dai privati cittadini. Pensiamo alla diffusione dei siti e delle banche dati consultabili liberamente sul web.

L'informatica giudiziaria rappresenta l'applicazione della tecnologia informatica e telematica all'interno del sistema giudiziario, con l'obiettivo di semplificare, velocizzare e ottimizzare i processi giuridici.

L'informatica giudiziaria va oltre la semplice archiviazione digitale di atti e documenti. Essa comprende una vasta gamma di strumenti e soluzioni che supportano i magistrati, gli avvocati e il personale degli uffici giudiziari in molteplici attività dalla gestione delle pratiche al momento della decisione



Quando si parla di digitalizzazione PA si parla sempre (almeno) di CAD

Il Codice dell'Amministrazione Digitale (CAD), istituito con **decreto legislativo n. 82 del 7 marzo 2005**, rappresenta la norma di riferimento più importante quando si parla della digitalizzazione della PA.

Il CAD è nato per favorire **la digitalizzazione dell'attività amministrativa**, per semplificare le procedure burocratiche e incentivare l'accesso degli utenti a tutta la documentazione e ai servizi online della PA stessa. Inoltre con questo testo unico si è cercato di incrementare **l'interconnessione e l'interscambio tra PA** anche di Paesi diversi.

Strutturalmente è un **Testo Unico** che riunisce e organizza le norme, per lo più aventi carattere programmatico, volte a promuovere l'utilizzo delle nuove tecnologie nella PA al fine di agevolare le attività dei cittadini e delle imprese.

Il CAD di fatto costituisce il primo **corpus organico di disposizioni relativo all'uso delle tecnologie informatiche e telematiche nella PA** e sancisce veri e propri diritti dei cittadini e delle imprese in materia di uso delle tecnologie nei rapporti con le PA **[negli intendimenti ma...]**.

Esso contiene, inoltre, **definizioni fondamentali** il cui ambito di applicazione non è limitato al solo diritto amministrativo ma si estende ad altri campi del diritto sia civile che processuale ed in particolare al processo telematico.



Diritto di accesso ai servizi online e il «vocabolario digitale italiano»

L'obiettivo perseguito dal complesso di tali disposizioni è la realizzazione di una comunicazione efficiente tra la PA e il cittadino, garantendo al contempo la celerità e la sicurezza delle trasmissioni digitali.

Gli articoli 3-bis, 5-bis, 6 e 7 regolamentano il diritto all'accesso ai servizi on-line e all'invio dei documenti digitali, il diritto a ricevere comunicazioni dalle PA in forma elettronica, il diritto a reperire on line tutti i moduli e i formulari validi e aggiornati.

Ma quindi quel che devo sapere è tutto nel CAD?



Non solo CAD – Le linee guida AGID

Come precisato dal Consiglio di Stato - nell'ambito del parere reso sullo schema di decreto legislativo del correttivo al CAD, n. 2122/2017 del 10.10.2017 - le Linee Guida adottate da AGID, ai sensi dell'art. 71 del CAD, hanno carattere vincolante e assumono valenza erga omnes. Ne deriva che, nella gerarchia delle fonti, anche le presenti Linee Guida sono inquadrate come un atto di regolamentazione, seppur di natura tecnica, con la conseguenza che esse sono pienamente azionabili davanti al giudice amministrativo in caso di violazione delle prescrizioni ivi contenute. Nelle ipotesi in cui la violazione sia posta in essere da parte dei soggetti di cui all'art. 2, comma 2 del CAD, è altresì possibile presentare apposita segnalazione al difensore civico, ai sensi dell'art. 17 del CAD4 .

Non solo CAD – Il regolamento EIDAS per le firme digitali

Non solo CAD – Normativa specifica Processo civile e del PCT



Il documento informatico

Il Codice dell'Amministrazione Digitale (CAD-DLgs 82/2005) definisce il documento informatico come

"rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" in contrapposizione al documento analogico ("rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti").

Il Regolamento eIDAS n. 910/2014 definisce il documento elettronico come

"qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva".



Documento informativo vs documento analogico

Documento informatico

Art. 1 lett. p
Codice dell'Amministrazione
Digitale



Documento analogico

Art. 1 lett. p-bis
Codice dell'Amministrazione
Digitale

La rappresentazione
informatica di atti, fatti o dati
giuridicamente rilevanti.



La rappresentazione non
informatica di atti, fatti o dati
giuridicamente rilevanti.



Le caratteristiche

Regolamento eIDAS n. 910/2014 : documento elettronico costituito da **qualsiasi** contenuto conservato in forma elettronica,
in particolare testo o registrazione sonora, visiva o audiovisiva.

Il documento informatico



Documento **originariamente** informatico



Creato tramite utilizzo di software



Documento divenuto informatico **per acquisizione**



Creato tramite trasformazione del documento analogico



Validità ed efficacia probatoria dei documenti informatici

Art. 20 CAD Validità ed efficacia probatoria dei documenti informatici

...

1-bis. Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'[articolo 2702 del Codice civile](#) quando vi è **apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID** ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. **La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida.**

1-ter. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria.

1-quater. **Restano ferme le disposizioni concernenti il deposito degli atti e dei documenti in via telematica secondo la normativa, anche regolamentare, in materia di processo telematico.**

...



Introduzione alla firma digitale

Esistono **quattro** tipi diversi di **firme elettroniche**, con caratteristiche specifiche e valore giuridico differente.

Le prime 3 sono definite all'art. 3 del Regolamento UE 910/2014 (eIDAS).

1) la **firma elettronica semplice**: è una firma debole ed il valore di un documento firmato con la stessa è liberamente valutabile in giudizio. La definizione è volutamente generica e nel novero delle firme elettroniche semplici rientrano strumenti del più vario e differente tipo. **Sono firme elettroniche semplici, ad esempio, il pin del bancomat, la login e la password per accedere alla propria casella di posta elettronica.**

2) la **firma elettronica avanzata**: consente di collegare in modo univoco il firmatario al documento firmato. Ciò è possibile grazie all'uso di strumenti di firma sui quali il firmatario mantiene un controllo esclusivo. Una delle più diffuse firme elettroniche avanzate è la firma **grafometrica**, che si appone tramite apposite lavagne sensibili al tocco disegnando con una apposita penna la propria firma, in modo analogo alla firma su carta. A livello giuridico, la firma elettronica avanzata apposta su un documento informatico fornisce allo stesso il valore di una scrittura privata.



3) la firma elettronica qualificata: si tratta di un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma. Possono rilasciare certificati di firma qualificati solo **enti certificatori accreditati presso AgID** (in modo analogo a quanto avviene per il rilascio delle caselle PEC).

Mentre il Codice dell'Amministrazione digitale definisce all'art. 1 lettera s):

4) la firma digitale: “è 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”.

L'apposizione della firma digitale su un documento informatico permette di accertarne la paternità e l'integrità. Ciò è possibile grazie all'uso della crittografia, che consente di rendere il documento immutabile, o, più precisamente, di tracciare qualsiasi modifica effettuata allo stesso dopo l'apposizione della firma.



Come funziona la firma digitale

L'integrità è garantita dall'impossibilità di modificare il documento una volta firmato senza che ne sia compromessa la verifica, qualsiasi modifica successiva al documento è infatti tracciata ed evidenziata durante la validazione della firma.

L'elemento di sicurezza aggiuntivo della firma digitale, rispetto alla firma elettronica qualificata, è l'uso di **due chiavi asimmetriche**, una privata, segreta ed in possesso del solo titolare, ed una pubblica.

La chiave privata è utilizzata per generare la firma digitale, mentre grazie alla chiave pubblica, disponibile in pubblici elenchi, è possibile verificare l'autenticità della firma.

La certezza che solo il titolare abbia firmato il documento (presunzione di utilizzo prevista dalla normativa) si basa sulla necessità di **uso congiunto del dispositivo fisico** (in possesso esclusivo del firmatario) e del **codice PIN** (segreto ed in possesso del solo titolare), mentre il certificatore garantisce la correttezza delle informazioni anagrafiche presenti sul certificato di firma.

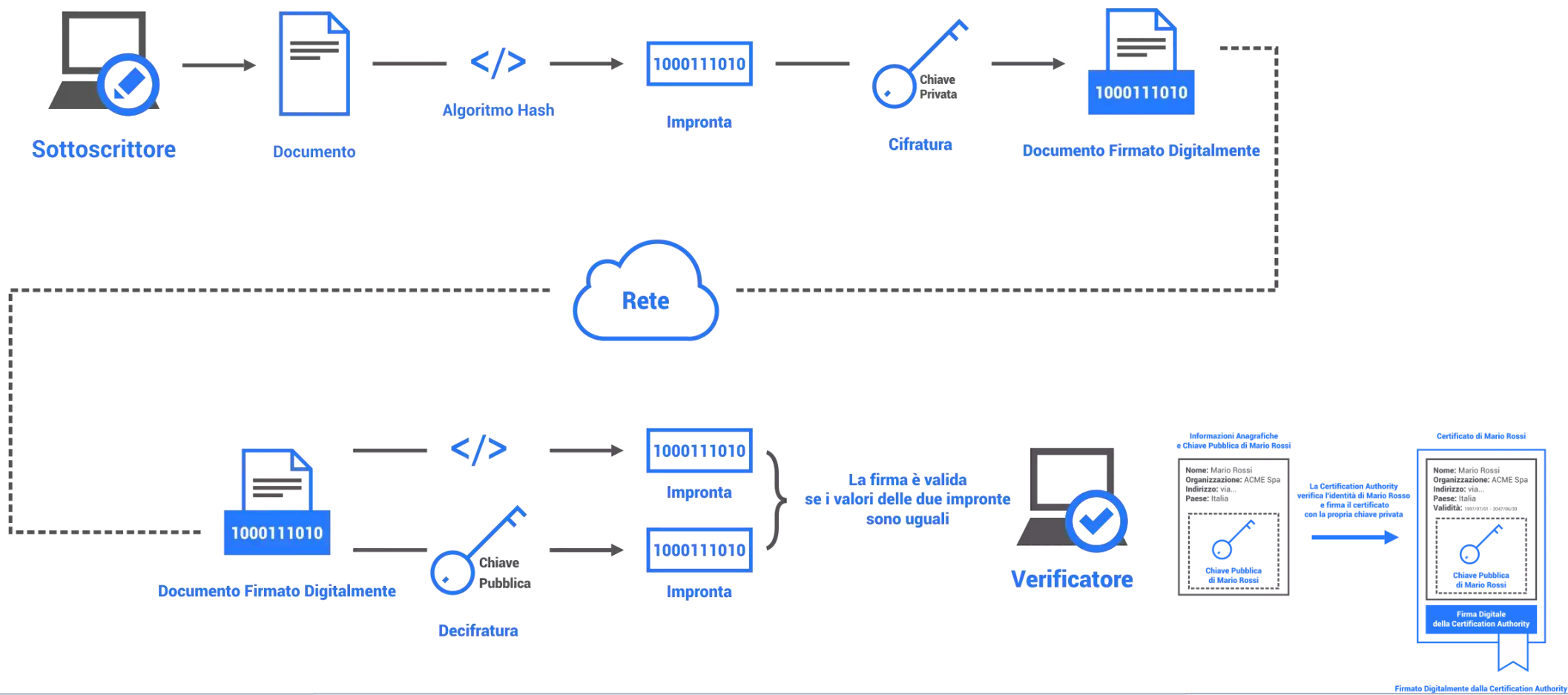




UFFICI DI PROSSIMITÀ

la giustizia più vicina ai cittadini

Servizio pubblico
di informazione
e assistenza per la
volontaria giurisdizione





I formati di firma

La **decisione di esecuzione (UE) 2015/1506** della Commissione dell'8 settembre 2015 prevede **3 differenti formati** per la sottoscrizione di documenti informatici con firme elettroniche avanzate:

- Il **formato CAdES**, consistente in una busta crittografica di firma con estensione P7M - E' possibile firmare qualsiasi tipo di file in CAdES, non essendoci particolari restrizioni di formato (sono consentiti documenti PDF, doc, xls, immagini, eseguibili, file di testo e binari di qualsivoglia tipo), tuttavia, per leggerne il contenuto, una volta firmato, è necessario utilizzare specifici software in grado di estrarre dalla busta crittografica il documento sottoscritto. Non è prevista la storicizzazione del file;
- Il **formato PAdES**, che integra la firma all'interno di file di tipo Portable Document Format (PDF) secondo lo standard ISO/IEC 32000. Firma solo PDF, per la lettura di un documento firmato in PaDES non sono necessari programmi specifici consente il versionamento
- Il **formato XAdES**, di scarsa diffusione ed utilizzo, che prevede la sottoscrizione in linguaggio XML.



Domande a questo punto

Ma lo SPID invece?

lo SPID è un sistema di autenticazione che permette a cittadini e imprese di accedere ai servizi online della pubblica amministrazione e dei privati aderenti con un'identità digitale unica, costituita da credenziali (nome utente e password) che vengono rilasciate all'utente e che permettono l'accesso a tutti i servizi online

Chi ha lo SPID ha anche la firma digitale?

I servizi prevedono l'accesso con credenziali SPID di livello 2, in questo modo il cittadino ha la possibilità di dimostrare con certezza la sua identità e ottenere la firma digitale.

Quante firme digitali può avere una persona?

Una persona può essere in possesso di più di una firma digitale. Nonostante infatti sia valido il principio dell'univocità e della titolarità della firma elettronica, questo non vuol dire che la stessa persona non possa avere più firme digitali

La firma digitale che ho è associata dell'ENTE?

La firma digitale è associata alla persona. Qualche ordine professionale ha richiesto l'emissione di una «firma digitale con il ruolo» ma è un attributo non richiesto dalla normativa



Introduzione alla PEC

Art. 48

(Posta elettronica certificata)

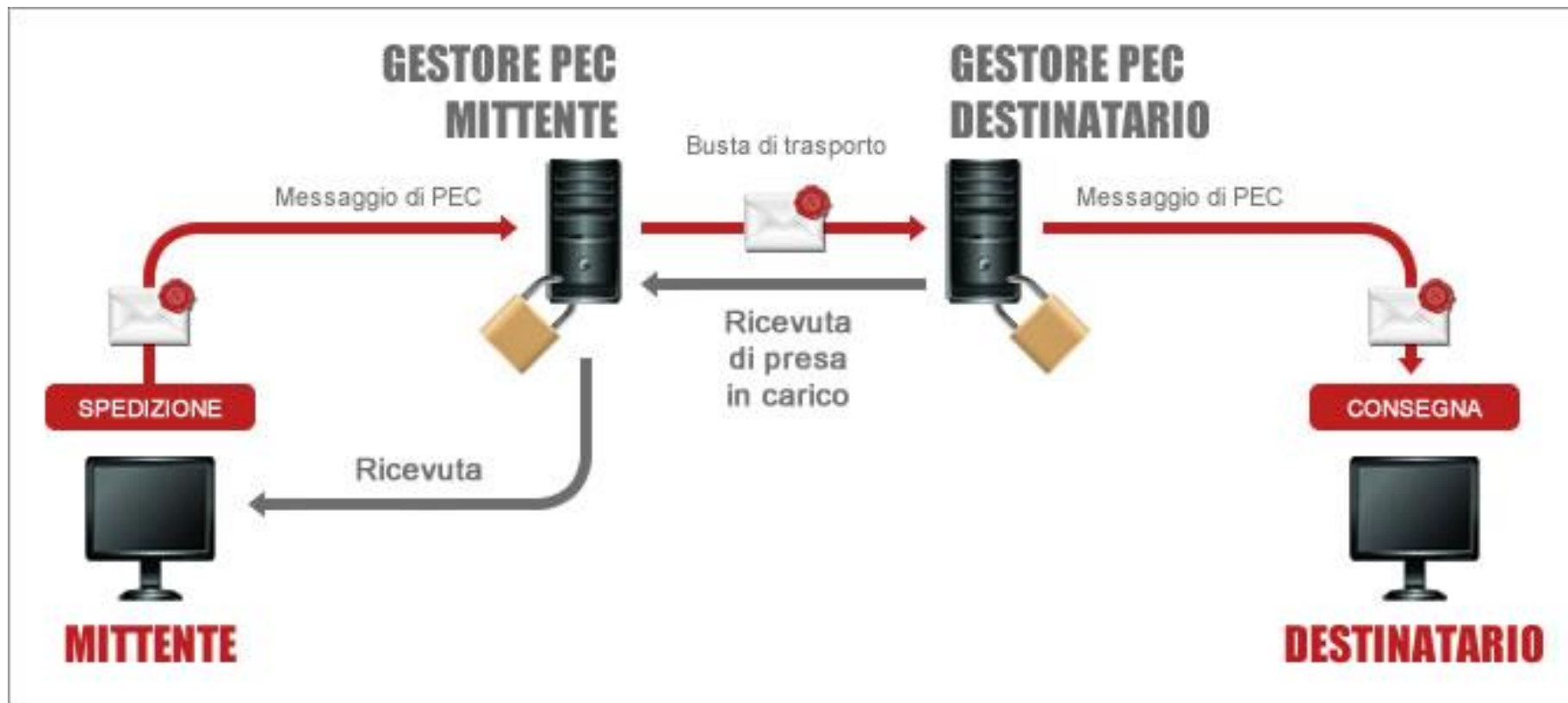
1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del [decreto del Presidente della Repubblica 11 febbraio 2005, n. 68](#), o mediante altre soluzioni tecnologiche individuate con le Linee guida.
2. La trasmissione del documento informatico per via telematica, effettuata ai sensi del comma 1, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta.
3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso ai sensi del comma 1 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, ovvero conformi alle Linee guida.



UFFICI DI PROSSIMITÀ

la giustizia più vicina ai cittadini

Servizio pubblico
di informazione
e assistenza per la
volontaria giurisdizione





Come funziona la PEC

La validità della trasmissione e ricezione del messaggio di posta elettronica certificata è attestata, rispettivamente, dalla **ricevuta di accettazione (RAC)** e dalla **ricevuta di avvenuta consegna (RdAC)**, di cui all'articolo 6 del DPR.

La **ricevuta di avvenuta consegna (RdAC)** è rilasciata contestualmente alla consegna del messaggio di posta elettronica certificata nella casella, indipendentemente dall'avvenuta lettura da parte del soggetto destinatario.

Se invece il messaggio di posta elettronica certificata non risulta consegnabile, come previsto dall'art. 8, il gestore PEC comunica al mittente, entro le 24 successive ore all'invio, **l'avviso di mancata consegna (AMC)**.

L'avviso di mancata consegna si può verificare nei seguenti casi:

- l'indirizzo email del destinatario è errato oppure non attivo
- lo spazio della casella del destinatario è esaurito e non può ricevere nuovi messaggi



Il salvataggio dei messaggi e l'archiviazione dei messaggi PEC

Come le caselle di posta elettronica tradizionali, anche le caselle PEC hanno uno **spazio** ed una **dimensione limitata** per poter **archiviare** i messaggi ricevuti e quelli inviati (in genere almeno 1 GB (gigabyte)). Una volta saturato lo spazio disponibile della casella PEC, l'utilizzo della stessa è compromesso. Oltre a non poter ricevere nuovi messaggi, la casella PEC piena rappresenta, infatti, uno dei casi di mancata consegna del messaggio (**mailbox full**) ed anche l'invio di nuovi messaggi non riesce a perfezionarsi.

Per evitare la saturazione dello spazio della casella PEC, senza necessità di dover cancellare definitivamente i singoli messaggi dalla webmail, il consiglio è di scaricare i messaggi ricevuti in locale su computer, in tal modo liberando lo spazio disponibile sul server. A tal scopo tutti i gestori PEC forniscono le istruzioni per la configurazione dei più comuni **client di posta elettronica**, in ambiente Windows, Apple, nonché Linux.

I gestori PEC si limitano a conservare per 30 mesi i log ed, una volta cancellati dall'utente i messaggi dal server, non vi è più la possibilità di recuperarli dal fornitore stesso. E' quindi di fondamentale importanza il salvataggio e la conservazione delle PEC in modo da preservare il contenuto dei messaggi e dei loro allegati, sia che si tratti di una notificazione a mezzo PEC che della prova del deposito telematico di un atto.



Le copie informatiche possono avere **diversa origine**, motivo per cui la normativa (art. 1 comma 1 CAD) distingue fra:



1) Copia informatica di documento analogico

Costituisce copia informatica il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto (art. 1 comma 1 lett. i-bis CAD). Di fatto, la copia informatica consiste nella **scansione** del documento cartaceo.



2) Copia informatica di documento informatico

Costituisce copia informatica il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari (art. 1 comma 1 lett. i-quater CAD). Di fatto, la copia informatica consiste nella copia del documento informatico generato, ad esempio, con l'attività di **copia-incolla**.



3) Copia analogica di documento informatico

Costituisce copia analogica il documento analogico (cartaceo) avente contenuto identico a quello del documento informatico da cui è tratto.



1) Copia immagine di un documento analogico: la scansione

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o, nel caso di esigenze di dematerializzazione massiva di documenti analogici, attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia. I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 "Certificazione di Processo".

Fermo restando quanto previsto dall'art. 22 comma 3 del CAD8 nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia per immagine ad un documento analogico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata o altro tipo di firma ai sensi dell'art. 20 comma 1bis, ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto



2) Duplicati, copie ed estratti informatici di documenti informatici

Un duplicato informatico ha lo stesso valore giuridico del documento informatico da cui è tratto se è ottenuto mediante la memorizzazione della medesima evidenza informatica, sullo stesso dispositivo o su dispositivi diversi; ad esempio, effettuando una copia da un PC ad una pen-drive di un documento nel medesimo formato.

La copia di un documento informatico è un documento il cui contenuto è il medesimo dell'originale ma con una diversa evidenza informatica rispetto al documento da cui è tratto, come quando si trasforma un documento con estensione “.doc” in un documento “.pdf”.

L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto. Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine se la stessa conformità non viene espressamente disconosciuta.

In particolare, la validità del documento informatico per le copie e/o estratti di documenti informatici è consentita mediante uno dei due metodi: **● raffronto dei documenti; ● certificazione di processo**



UFFICI DI PROSSIMITÀ

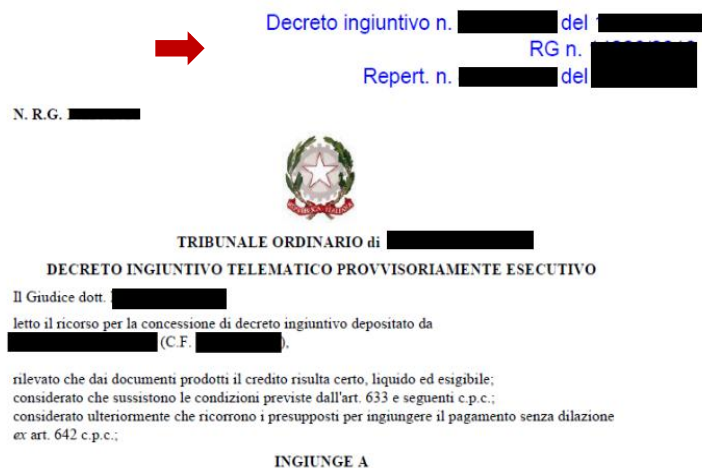
la giustizia più vicina ai cittadini

Servizio pubblico
di informazione
e assistenza per la
volontaria giurisdizione

L'estrazione degli atti e/o provvedimenti può avvenire discrezionalmente nella forma della copia informatica oppure del duplicato informatico. Al di là della identità o meno dell'impronta informatica del documento (cd. **Hash**), la percezione della differenza fra copia e duplicato di un documento estratto dai registri ministeriali di Cancelleria è altresì visiva.

COPIA INFORMATICA

La copia informatica riporta le stampigliature di colore blu che vengono automaticamente apposte dai Registri in fase di caricamento del documento.



DUPLICATO INFORMATICO

Il duplicato informatico è privo di qualsivoglia distinzione grafica essendo esente da qualunque tipo di alterazione.





Art. 16 bis comma 9 bis D.L.179/2012

Le copie analogiche ed informatiche, anche per immagine, estratte dal fascicolo informatico e munite dell'attestazione di conformità a norma del presente comma, **equivalgono all'originale**.





3) Copie analogiche di documenti informatici: la stampa

1. Le copie su supporto analogico di documento informatico, **anche sottoscritto** con firma elettronica avanzata, qualificata o digitale, hanno **la stessa efficacia probatoria** dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un **pubblico ufficiale a ciò autorizzato**.
2. Le copie e gli estratti su supporto analogico del documento informatico, conformi alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale se la loro conformità non è espressamente disconosciuta. **Resta fermo, ove previsto l'obbligo di conservazione dell'originale informatico.**
3. Sulle copie analogiche di documenti informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con le regole tecniche di cui all'articolo 71, tramite il quale è possibile accedere al documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica.



UFFICI DI PROSSIMITÀ

la giustizia più vicina ai cittadini

Servizio pubblico di informazione
e assistenza per la volontaria giurisdizione

**UFFICI DI PROSSIMITÀ
DELLA REGIONE SICILIANA**

