Corso di formazione online

L'implementazione dei servizi con autenticazione SPID e CIE

Parte normativa e Provvedimenti

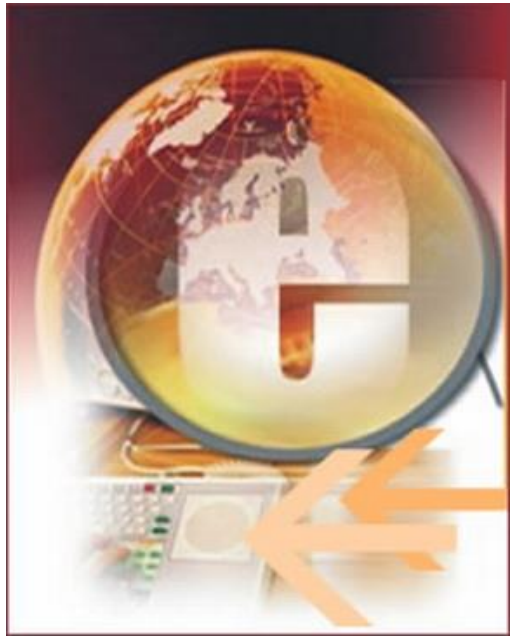
Docente: avv. Michele Iaselli

La digitalizzazione dei servizi nel campo della pubblica amministrazione rimane uno degli argomenti più complessi e di difficile realizzazione sia per il proliferare di norme che spesso hanno disciplinato la materia in modo confusionario e non sempre attento sia per le concrete problematiche di carattere organizzativo e tecnologico.

La stessa digitalizzazione oggi ha assunto un grande rilevanza poiché il PNRR del nostro Governo tra le sue missioni annovera: digitalizzazione, innovazione, competitività, cultura e turismo; rivoluzione verde e transizione ecologica; infrastrutture per una mobilità sostenibile; istruzione e ricerca; inclusione e coesione; salute.

La normativa

L'E-Government



Una tappa fondamentale è stata sicuramente il piano di e-government varato nel giugno 2000 dal Consiglio dei Ministri su iniziativa del Ministro della Funzione Pubblica, Franco Bassanini contraddistinto da una 1^ ed una 2^ fase. Tale progetto aveva come suo obiettivo fondamentale proprio quello di garantire ai cittadini l'accesso on-line a tutti i servizi erogati dalle pubbliche amministrazioni nell'ottica di quella che rappresentava la nuova frontiera di Internet.

Protagoniste dell'innovazione dovevano essere le amministrazioni locali, che nel modello decentrato e federale dello Stato rappresentavano il *front-office* dell'intero sistema amministrativo a disposizione diretta dei cittadini, mentre le amministrazioni centrali dovevano svolgere per lo più il ruolo di *back-office*.

L'idea di fondo era quella della realizzazione di un grande processo di innovazione tecnologica che coinvolgesse tutto il sistema pubblico italiano mettendolo così sullo stesso piano rispetto a quello di altri paesi più progrediti nelle nuove tecnologie della comunicazione.

Ma già allora ci si rese conto che per realizzare un simile processo c'era bisogno di una serie di condizioni che rendessero possibile l'integrazione fra le diverse attività e funzioni delle varie pubbliche amministrazioni e la loro fruibilità da parte dei cittadini.

Si ricorda che la seconda fase dell'e-government ha avuto come prerequisito la definizione di una visione strategica comune tra Stato, Regioni ed Enti locali, che è contenuta nel documento *"L'e-government per un federalismo efficiente: una visione condivisa, una realizzazione cooperativa"*.

La seconda fase di attuazione dell'e-government ha avuto come obiettivo principale l'allargamento alla maggior parte delle amministrazioni locali dei processi di innovazione già avviati, sia per ciò che riguarda la realizzazione dei servizi per cittadini e imprese, sia per ciò che riguarda la realizzazione di servizi infrastrutturali in tutti i territori regionali.

Essa prevedeva pertanto la realizzazione di cinque linee di azione: Lo sviluppo dei servizi infrastrutturali locali (Sistema Pubblico di Connettività); la Diffusione territoriale dei servizi per cittadini ed imprese; l'inclusione dei comuni piccoli nell'attuazione dell' e-government; l'avviamento di progetti per lo sviluppo della cittadinanza digitale (e-democracy); la promozione dell'utilizzo dei nuovi servizi presso cittadini e imprese.

Purtroppo, come è noto, il progetto di e-government, per quanto ambizioso, non è riuscito a raggiungere gli obiettivi voluti per forti resistenze innanzitutto di carattere mentale oltre che per obiettive carenze infrastrutturali e professionali.

L’agenda Digitale

Sicuramente il lento ma inesorabile percorso del nostro paese verso la completa digitalizzazione di tutte le fondamentali attività di rilevanza pubblicistica ha conosciuto con l'Agenda digitale, i cui principi informatori sono contenuti nel Decreto-legge 18 ottobre 2012, n. 179 convertito dalla legge di conversione 17 dicembre 2012, n. 221, un momento importante e nello stesso tempo molto delicato poiché il nostro paese si dota di uno strumento normativo che, si spera, costituirà un'efficace leva per la crescita economica ed occupazionale.

Come noto i "pilastri" dell'Agenda Digitale europea sono:

1. Mercato digitale unico
2. Internet veloce e superveloce
3. Interoperabilità e standard
4. Fiducia e sicurezza informatica
5. Ricerca e innovazione
6. Alfabetizzazione informatica
7. ICT per la società.

Le misure dell'Agenda digitale italiana

Il documento digitale unificato

Anagrafe nazionale e censimento della popolazione

PEC e domicilio digitale

Comunicazioni telematiche

Biglietto elettronico e trasporto intelligente

Open data

Scuola digitale

Sanità digitale

Banda larga e digital divide

Pagamenti elettronici

Giustizia digitale

Comunità intelligenti

Il Codice dell'Amministrazione Digitale

Come è noto tutte le norme - emanate per favorire la diffusione delle nuove tecnologie e l'ammodernamento delle strutture pubbliche – sono state raccolte in un codice approvato con *il decreto legislativo del 7 marzo 2005, n. 82 recante il "Codice dell'Amministrazione Digitale" (CAD).*

Quest'ultimo decreto legislativo ha subito diverse modifiche ed integrazioni:

- D. Lgs. 4 aprile 2006, n. 159
- Legge 24 dicembre 2007, n. 244
- Legge 28 gennaio 2009 n. 2
- Legge 18 giugno 2009, n. 69
- Legge 3 agosto 2009,
- D.lgs. 30 dicembre 2010, n. 235
- Legge n. 221/2012
- Legge n. 98/2013 (decreto del fare)
- L.lgs. n. 179 del 26 agosto 2016
- L.lgs n. 217 del 13 dicembre 2017
- Legge di conversione 11 settembre 2020 n. 120 del DL 16 luglio 2020, n. 76.

Con le ultime riforme non solo si è proceduto ad una modifica ed integrazione delle norme del CAD ma ne sono state abrogate diverse anche attraverso vari accorpamenti e semplificazioni.

L'obiettivo è innanzitutto quello di promuovere e rendere effettivi i diritti di cittadinanza digitale dei cittadini e delle imprese, garantendo, contestualmente, il diritto di accesso ai dati, ai documenti e ai servizi di loro interesse in modalità digitale, semplificando le modalità di accesso ai servizi alla persona e realizzando - come indicato dal titolo con cui è rubricato l'art. 1 della legge n. 124 del 2015 - una vera e propria "*carta della cittadinanza digitale*".

Altro obiettivo fondamentale è quello di spostare l'attenzione dal processo di digitalizzazione ai diritti digitali di cittadini e imprese. Con la "carta della cittadinanza digitale" si riconoscono direttamente diritti a cittadini e imprese e si costituisce la base giuridica per implementare Italia Login, la piattaforma di accesso che, attraverso il Sistema pubblico d'identità digitale (SPID) e l'Anagrafe nazionale della popolazione residente, permetterà ai cittadini di accedere ai servizi pubblici - e a quelli degli operatori privati che aderiranno - con un unico nome utente e un'unica *password* (prenotazioni di visite mediche, iscrizioni a scuola, pagamento dei tributi).

Il sistema SPID assume sempre di più un ruolo centrale in questo nuovo CAD e viene definito come un insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'AgID, secondo modalità definite con specifico decreto ministeriale, identificano cittadini, imprese e pubbliche amministrazioni per consentire loro l’accesso ai servizi in rete.

Lo SPID, quindi, è un insieme di credenziali per accedere in rete a tutti i servizi della pubblica amministrazione e a quelli degli operatori commerciali che vi aderiranno. Lo SPID consente agli utenti di avvalersi di gestori dell'identità digitale e di gestori di attributi qualificati per permettere ai fornitori di servizi l'immediata verifica della propria identità e di eventuali attributi qualificati che li riguardano.

Con l'istituzione dello SPID le pubbliche amministrazioni possono consentire l'accesso in rete ai propri servizi, oltre che con lo stesso SPID, solo mediante la carta d'identità elettronica e la carta nazionale dei servizi che alla fine avranno in tal senso una funzione solo residuale. La possibilità di accesso con carta d'identità elettronica e carta nazionale dei servizi resta comunque consentito indipendentemente dalle modalità predisposte dalle singole amministrazioni.

E’ chiaro, quindi, l’intento del legislatore di semplificare al massimo l’accesso ai servizi on line dei cittadini, superando le difficoltà connesse alle carte elettroniche, ma il pericolo “sicurezza” incombe sempre, poiché è evidente che con tale sistema si moltiplicano le identità digitali di un cittadino, che saranno diverse per ogni servizio e la prospettiva lascia perplessi. E’ anche vero che il sistema è continuamente monitorato dall’Autorità Garante giustamente preoccupata, ma è anche vero che se una singola identità digitale crea problemi figuriamoci tante.

L'opportunità delle ultime riforme dell'intero CAD nasce anche dalla necessità di adeguare lo stesso al Regolamento comunitario n. 910/2014 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari nel mercato interno pubblicato nella G.U. dell'Unione Europea del 28 agosto 2014 che è entrato in vigore nel nostro ordinamento il 1 luglio 2016.

Il Regolamento è noto con l'acronimo e-IDAS che sta per electronic IDentification Authentication and Signature (eTS electronic Trust Services) e stabilisce le condizioni per il riconoscimento reciproco in ambito di identificazione elettronica e le regole comuni per le firme elettroniche, l'autenticazione web ed i relativi servizi fiduciari per le transazioni elettroniche.

Il Regolamento, quindi, innanzitutto disciplina l'identificazione elettronica intesa come "*il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica*", preoccupandosi del riconoscimento reciproco fra gli Stati membri dei mezzi di identificazione e autenticazione elettroniche per accedere a un servizio prestato da un organismo del settore pubblico online in uno Stato membro.

L'identificazione elettronica va distinta dalla c.d. "autenticazione" intesa come "*un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica*".

Particolare attenzione viene rivolta dal Regolamento ai prestatori di servizi fiduciari qualificati e non qualificati che devono rispettare determinati requisiti, alle firme elettroniche, alla validazione temporale elettronica (marca temporale), ai servizi elettronici di recapito certificato.
Viene creato anche un nuovo strumento il c.d. "sigillo elettronico", creato per le specifiche esigenze dell'e-business, che è da intendersi come "dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi".

I concetti cardine del CAD

Le tematiche (*normative*) dell'amministrazione digitale

Il responsabile per la transizione al digitale

La figura del responsabile della transizione digitale rimane ancora una figura poco chiara nell'ambito della pubblica amministrazione che non va confusa con quella del difensore civico digitale disciplinata dalla stessa norma (art. 17, comma 1-quater, del CAD) ma prerogativa ormai dell'Agenzia per l'Italia Digitale (AgID) che a seguito di quanto previsto dalla più recente riforma del 2017 ha organizzato uno specifico ufficio per tale esigenza.

In effetti il responsabile della transizione digitale nasce con la riforma Madia (d.lgs. n. 179/2016) che con l'art. 15 riformulava l'art. 17 del CAD, prevedendo che "le pubbliche amministrazioni garantiscano l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo in coerenza con le regole tecniche di cui all'art. 71 del CAD, attraverso l'affidamento ad un unico ufficio dirigenziale generale della transizione alla modalità operativa digitale e dei processi di riorganizzazione finalizzati alla realizzazione di una amministrazione digitale aperta". In precedenza, difatti, si parlava sempre di un unico ufficio dirigenziale generale, ma responsabile solo del coordinamento funzionale.

Con l'avvento della più recente riforma del CAD (d.lgs. n. 217/2017) il relativo art. 17 oltre a sostituirne la rubrica, ha apportato modifiche di drafting al comma 1 dell'articolo 17 del decreto legislativo 7 marzo 2005, n. 82, prevedendo anche nuovi compiti di questa figura dirigenziale.

Nel complesso, quindi, le funzioni di questo ufficio sono:

a) coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;

b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;

c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;

d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;

e) analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;

f) cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);
g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni;
i) promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'articolo 64-bis;
j-bis) pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale.

In considerazione, quindi, degli innumerevoli compiti che vengono attribuiti al predetto ufficio è evidente che si richiedano, almeno per il responsabile, come specificato dalla norma, delle adeguate competenze tecnologiche, di informatica giuridica e manageriali e tenuto conto della stessa delicatezza della funzione, lo stesso responsabile dovrà rispondere, con riferimento ai compiti relativi alla transizione alla modalità digitale, direttamente all'organo di vertice politico.

Proprio per supportare le PP.AA. in questo percorso e favorire un'accelerazione delle procedure di nomina, AgID e Ministro hanno creato una struttura organizzativa, la Conferenza dei RTD, che si riunisce periodicamente per condividere esperienze di buone pratiche e incentivare la diffusione della cultura dell'innovazione nella PA.

La Conferenza, nata anche a seguito della circolare ministeriale n. 3/2018 è, quindi, uno strumento di dialogo, raccordo e supporto verso i RTD delle amministrazioni italiane al fine di promuovere la trasformazione digitale inclusiva delle PA.

La necessità di supportare le pubbliche amministrazioni verso una trasformazione al digitale ha comportato originariamente la nascita del Ministero per l'innovazione tecnologica e la digitalizzazione, attualmente sostituito dal Ministero per l'Innovazione Tecnologica e la Transizione digitale, nonché di un vero e proprio Dipartimento per la trasformazione digitale costituito presso la Presidenza del Consiglio con DPCM 19 giugno 2019 e preposto alla definizione delle politiche per la modernizzazione del paese con le tecnologie digitali e al coordinamento ed all'attuazione dei programmi di trasformazione digitale.

Gli open data

L’art. 7 del d.lgs. n. 33/2013 prevede i c.d. open data sancendo che i documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria ai sensi della normativa vigente, resi disponibili anche a seguito dell'accesso civico di cui all'articolo 5, sono pubblicati in formato di tipo aperto ai sensi dell'articolo 68 del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, e sono riutilizzabili ai sensi del decreto legislativo 24 gennaio 2006, n. 36, del decreto legislativo 7 marzo 2005, n. 82, e del decreto legislativo 30 giugno 2003, n. 196, senza ulteriori restrizioni diverse dall'obbligo di citare la fonte e di rispettarne l'integrità.

Per Open data si intendono i dati aperti, cioè informazioni che sono liberamente accessibili a chiunque. Fra i principi essenziali degli open data troviamo:
- *accessibilità*, intesa come disponibilità nel potervi entrare, cioè poter leggere il dato senza particolari difficoltà;
- *disponibilità*, cioè assenza di restrizioni, limitazioni di alcun genere (brevettuali o di diritto d'autore) alla loro accessibilità;
- *replicabilità*, nel senso che questi dati devono poter essere facilmente riproducibili e riutilizzabili, permettendo all'utente che li voglia utilizzare di poterne leggere e riprodurre il contenuto;
- *trasparenza*, poter leggere un dato senza doversi munire di specifici strumenti tecnici o interpretativi per avvicinarsi al contenuto dei dati;
- *intelligibilità*, cioè dati comprensibili senza dover utilizzare particolari conoscenze a riguardo;
- *non discriminazione*, tutti devono essere in grado di usare, riutilizzare e ridistribuire i dati;
- *neutralità tecnologica*, nel senso che bisogna evitare di imporre vincoli tecnologici ed economici agli utenti.

Per garantire i principi su esposti è necessario che i dati pubblicati (anche detti *datasets*) abbiano specifici requisiti, cioè che siano:

- *completi*, nel senso che i dati devono essere equipaggiati con metadati, che consentano di esportarli, utilizzarli on line e off line, integrarli e aggregarli con altre risorse e diffonderli in Rete;
- *primari*, cioè devono essere strutturati in modo tale da essere utilizzati in formato elementare, privi di manipolazioni di alcun genere;
- *tempestivi*, nel senso di rapidità di accesso da parte degli utenti che navigano in Rete;
- *accessibili*, i dati devono poter essere raggiungibili senza necessità di far ricorso a particolari tecnologie;
- *leggibili da computer*, poiché si predilige la funzione *machine-readable* dei documenti per essere facilmente processabili da parte del computer;

- *in formati non proprietari*, al fine di garantire una leggibilità senza obblighi di acquistare licenze proprietarie;
- *liberi da licenze che ne limitino l'uso*, in modo da tutelare la maggiore semplicità di utilizzo e riproduzione dei dati stessi;
- *riutilizzabili*, cioè riproducibili con facilità, per creare nuove risorse e nuovi progetti di ricerca;
- *ricercabili*, senza una facilità di ricerca, quei dati corrono il rischio di restare nascosti nell'oscurità di qualche sito web di antica realizzazione;
- *permanenti*, in grado, cioè, di essere disponibili nel tempo;
- *sicuri*, nel senso che deve essere garantita un'ampia tutela da malware di ogni genere;
- *interoperabili*, poiché i dati hanno un valore più elevato se è possibile effettuare correlazioni fra *datasets* indipendenti l'uno dall'altro, ma interoperabili nel formato.

Viene, quindi, raccomandato, dalle linee guida per i siti web delle pubbliche amministrazioni l'uso dei seguenti formati aperti e standardizzati: Html/Xhtml per la pubblicazione di informazioni pubbliche su Internet; Pdf con marcatura (standard Iso/Iec 32000-1:2008); Xml per la realizzazione di database di pubblico accesso ai dati; Odf e Ooxml per documenti di testo; Png per le immagini; Ogg per i file audio; Theora per i file video; Epub per i libri elettronici.

Non bisogna, peraltro, dimenticare che gli open data oltre a rappresentare in senso tecnico il formato "aperto" con cui i dati digitali possono essere distribuiti nel web per rendere i dati accessibili, riusabili, ed integrabili, rappresentano un vero e proprio movimento che ha alla base i principi fondamentali dell'open source. Lo stesso concetto va, quindi, visto in diretto collegamento con il riuso dei dati pubblici che dovrebbe portare all'elaborazione di un altro ambizioso concetto e cioè quello di Open Government, con il quale si cerca di evidenziare l'apertura e la trasparenza delle pubbliche amministrazioni.

Si ricorda, infine, che l'AgID ha adottato il 31 luglio 2013 la prima versione (alla quale è succeduta la versione 2014) delle Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico, attuando così le disposizioni di cui all'articolo 52, comma 7, del Codice dell'Amministrazione Digitale.
Le linee guida indirizzano le pubbliche amministrazioni verso un processo di produzione e rilascio dei dati pubblici standardizzato e interoperabile su scala nazionale. Propongono, tra l'altro, schemi operativi e organizzativi, identificano standard tecnici e best practice di riferimento e suggeriscono aspetti di costo e di licencing da tenere in considerazione.

Inoltre nel settembre 2015, in occasione della riunione dell'OGP (Open Government Partnership) svoltasi a margine dell'Assemblea Generale delle Nazioni Unite, è stata approvata la Carta internazionale degli Open Data.
Il documento si fonda su sei principi cardine:

- Dati Aperti Automaticamente
- Tempestività e completezza
- Accessibilità ed Usabilità per tutti
- Comparabilità ed interoperabilità
- Rilascio dei Dati per una Governance Migliore
- Rilascio dei Dati per lo sviluppo e l'Innovazione

Documento informatico

Il documento informatico è definito dal CAD come «il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti».

Il valore giuridico e probatorio di un documento informatico è sicuramente collegato al tipo di firma elettronica che lo contraddistingue.

Allo stato attuale alla luce di quanto disciplinato dal Codice dell'Amministrazione digitale ed anche da provvedimenti conseguenti (vedi le linee guida AgID contenenti le Regole Tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD, oppure le Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici) è possibile distinguere tra cinque tipologie di firma e cioè:

- Firma elettronica pura e semplice
- Firma elettronica avanzata
- Firma elettronica qualificata
- Firma digitale
- Firma con Spid

Firma elettronica pura e semplice

Essa è definita dal CAD come l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

In merito alla rilevanza di tale tipologia di firma il decreto ingiuntivo del Tribunale di Cuneo n. 848 del 15 dicembre 2003 fece nascere un vero e proprio caso.
Difatti nel decreto ingiuntivo citato, il giudice sosteneva che:
1) l'e-mail rappresenta senza dubbio un documento informatico, nell'accezione fornita dall'articolo, 1, comma 1, lettera b), del D.P.R. 445/2000, a mente del quale per documento informatico si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
2) in particolare, l'e-mail costituisce documento informatico sottoscritto con firma elettronica "leggera", "*in quanto il mittente, per poter creare ed inviare detta mail, deve eseguire un'operazione di validazione inserendo il proprio username e la propria password*";
3) tale processo di validazione è da considerare equivalente alla firma elettronica leggera, così come definita in precedenza.

Tale pronuncia dette origine ad un orientamento giurisprudenziale per certi versi favorevole al riconoscimento di forza legale ai messaggi di posta elettronica semplice: in quegli anni, infatti, furono numerosi i decreti ingiuntivi emessi sulla base di semplici scambi di email tra le parti.
Significativa, in tal senso, è una sentenza del 9/4/2005 emessa dal Tribunale di Ancona che riconobbe valore giuridico alla corrispondenza scambiata tra due aziende a mezzo di semplici email: secondo i giudici del tribunale, lo scambio di epistole digitali sarebbe stato sufficiente a confermare - in via d'urgenza - le ragioni di una delle parti in causa.

Firma elettronica avanzata

Firma elettronica avanzata:

- una firma elettronica che è connessa unicamente al firmatario;

- che è idonea a identificare il firmatario;

- che è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;

- che è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati (artt. 3 e 26 del regolamento e-IDAS).

Firma elettronica qualificata

Si tratta di una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche (art. 3 del Regolamento e-IDAS).

Firma digitale

E’ un particolare tipo di firma 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.

La firma digitale è il risultato di una procedura informatica (validazione) che consente al sottoscrittore di rendere manifesta l' autenticità del documento informatico ed al destinatario di verificarne la provenienza e l'integrità.

Per generare una firma digitale è necessario utilizzare una coppia di chiavi digitali asimmetriche, attribuite in maniera univoca ad un soggetto detto Titolare della coppia di chiavi. La prima, chiave privata destinata ad essere conosciuta solo dal Titolare, è utilizzata per la generazione della firma digitale da apporre al documento, la seconda, chiave da rendere pubblica, viene utilizzata per verificare l'autenticità della firma. Caratteristica di tale metodo, detto crittografia a doppia chiave, è che, firmato il documento con la chiave privata, la firma può essere verificata con successo esclusivamente con la corrispondente chiave pubblica.

La Certification Authority rilascia il certificato che associa la persona fisica alla chiave pubblica, e custodisce la chiave pubblica in una lista consultabile

Il mittente firma con la sua chiave privata un documento

Il messaggio firmato, insieme al certificato del mittente rilasciato dalla CA, raggiunge il destinatario

Il destinatario, usando la chiave pubblica del mittente, riesce a determinare l'autenticità dello stesso e l'integrità del messaggio

Firma con SPID

Alla luce delle ultime riforme l'intenzione è quella di garantire maggiore certezza giuridica in materia di formazione, gestione e conservazione dei documenti digitali prevedendo che non solo quelli firmati digitalmente - o con altra firma elettronica qualificata - ma anche quelli firmati con firme elettroniche diverse, al ricorrere di specifiche condizioni identificate dall'AgiD, possano produrre gli stessi effetti giuridici e disporre della stessa efficacia probatoria senza che debba essere un giudice, caso per caso, a valutare al riguardo.

Si tratta di un'iniziativa che mira a promuovere l'adozione e l'utilizzo da parte di soggetti pubblici e privati di soluzioni digitali moderne e semplici da usare senza rinunciare al rispetto della disciplina vigente laddove impone il ricorso alla forma scritta per il compimento di taluni atti e contratti.

In particolare, il nuovo art. 20 del CAD - modificando la previgente disciplina che demandava esclusivamente agli organi giudicanti la possibilità di valutare liberamente in giudizio l'idoneità dei documenti informatici a fini probatori - prevede che il documento informatico soddisfi il requisito della forma scritta e abbia l'efficacia di cui all'art. 2702 c.c. qualora sia sottoscritto con una firma digitale, qualificata o avanzata, o, nel caso di documenti sottoscritti con firme elettroniche differenti, qualora rispetti gli standard tecnici individuati dall'AgID con specifiche linee guida, mentre, nei restanti casi, il valore probatorio del documento informatico è rimesso al libero giudizio degli organi giudicanti.

La norma testualmente dice che: «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 applicazione di tale disposizione l'Agenzia per l'Italia Digitale (AgID) ha emanato, con determinazione n. 157/2020 del 23 marzo 2020, le Linee Guida che consentono di firmare documenti online con SPID, proprio in conformità all'art. 20 del CAD.

Le Linee Guida sono state emanate al termine del naturale percorso di consultazione pubblica, che si è svolto dal 21 novembre al 28 dicembre 2019, e sono state pubblicate sulla Gazzetta Ufficiale n. 90 del 4 aprile 2020.

Obiettivo delle Linee Guida è quello di favorire il processo di completa digitalizzazione dei documenti.

A seguito dell'entrata in vigore di questo documento, sarà possibile firmare atti e contratti attraverso SPID con lo stesso valore giuridico della firma autografa, soddisfacendo, così, il requisito della forma scritta e producendo gli effetti dell'art. 2702 del codice civile.
Destinatari delle Linee guida sono i fornitori di servizi e i gestori dell'identità che intendono realizzare quanto previsto dal sopracitato articolo 20; gli utenti in qualità di fruitori del servizio.

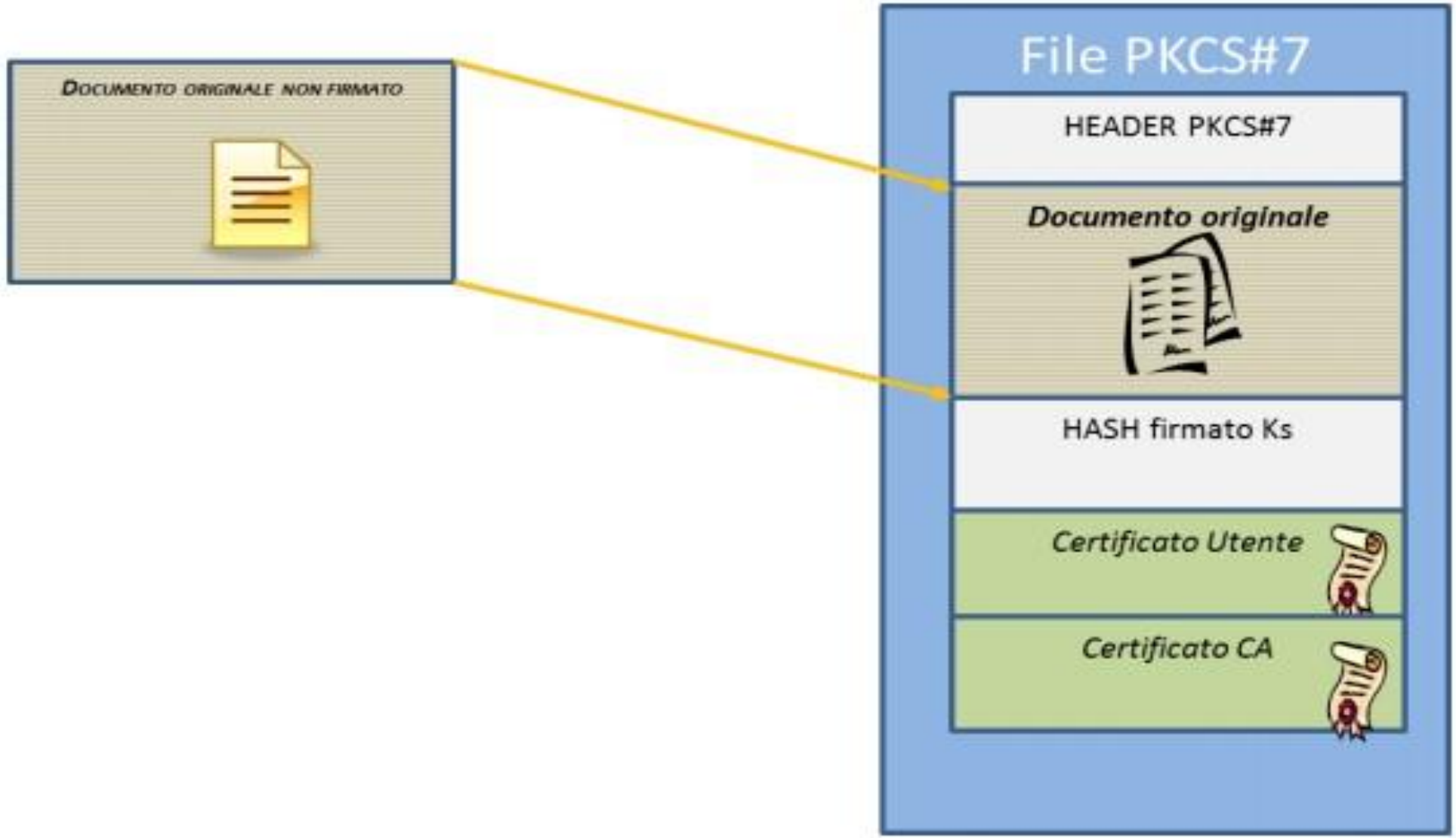
Il processo di cui all'articolo 20 comma 1-bis del CAD non può essere adoperato utilizzando identità digitali SPID per persona giuridica; possono essere utilizzate esclusivamente le identità digitali della persona fisica e le identità digitali per uso professionale (queste ultime regolamentate dalle LL.GG. identità digitali uso professionale).

Le firme multiple

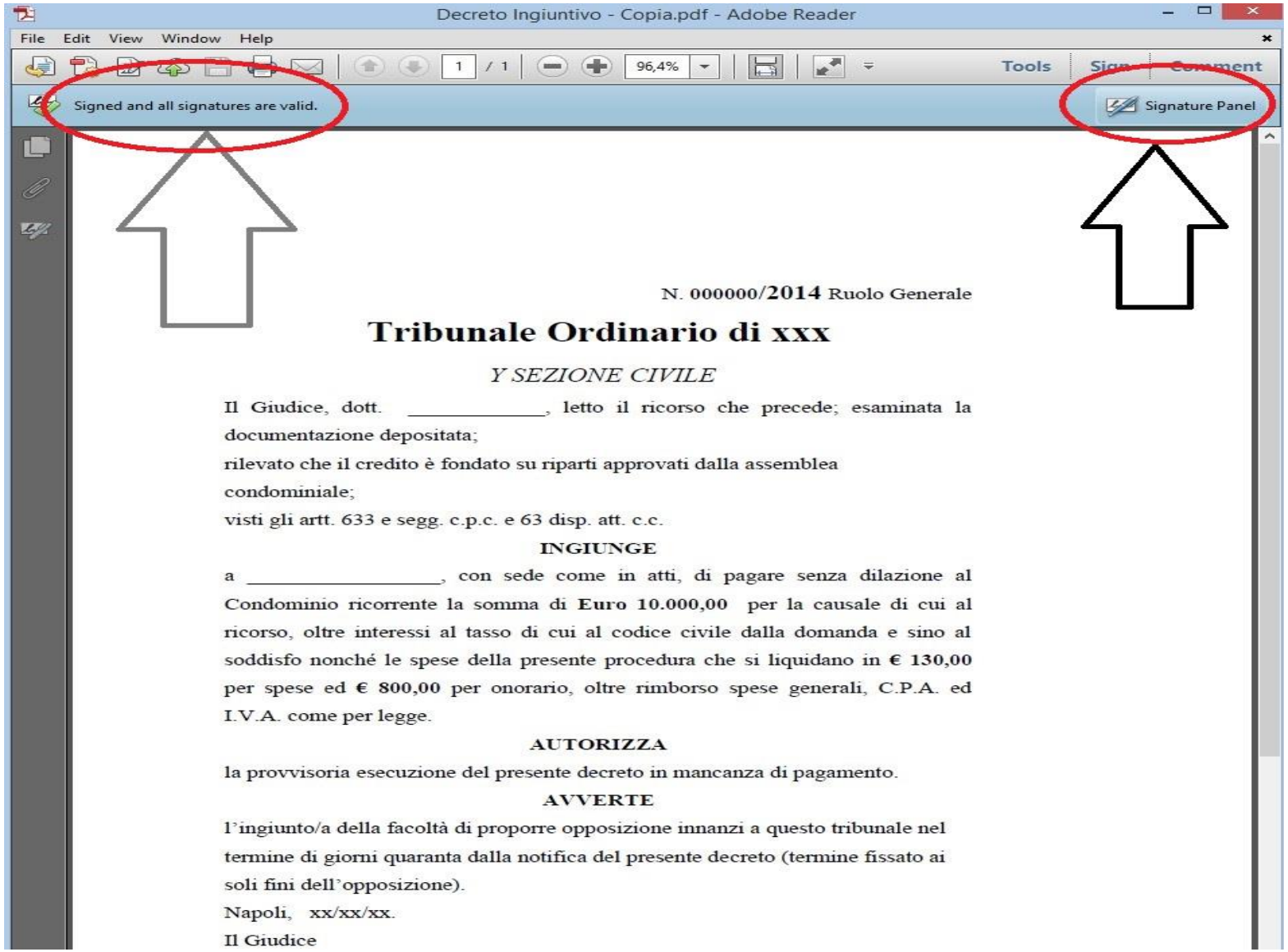
Talvolta accade che sia necessario apporre più firme su un medesimo documento o si intenda aggiungere dei dati dopo la sottoscrizione, ad esempio, allo scopo di riportare gli estremi della segnatura di protocollo di un documento spedito o ricevuto da una pubblica amministrazione.

Tenuto conto di tale finalità è opportuno distinguere tra formati di firma CAdES (file con estensione p7m) e PAdES (file con estensione pdf) e la loro attitudine ad ospitare più firme e informazioni disponibili solo dopo la generazione della firma digitale. (v. circolare dell'Agenzia per l'Italia Digitale dell'aprile 2014)

In particolare la busta CAdES è un file con estensione .p7m, il cui contenuto è visualizzabile solo attraverso idonei software in grado di "sbustare" il documento sottoscritto. Tale formato permette di firmare qualsiasi tipo di file, ma presenta lo svantaggio di non consentire di visualizzare il documento oggetto della sottoscrizione in modo agevole. Infatti, è necessario utilizzare un'applicazione specifica.


Documento originale non firmato
File PKCS#7
HEADER PKCS#7
Documento originale
HASH firmato Ks
Certificato Utente
Certificato CA

La firma digitale in formato PAdES è un file con estensione .pdf, leggibile con i comuni reader disponibili per questo formato.
Questa tipologia di firma, nota come "firma PDF", prevede diverse modalità per l'apposizione della firma, a seconda che il documento sia stato predisposto o meno ad accogliere le firme previste ed eventuali ulteriori informazioni, rende il documento più facilmente accessibile, ma consente di firmare solo documenti di tipo PDF.



N. 000000/**2014** Ruolo Generale

Tribunale Ordinario di xxx

Y SEZIONE CIVILE

Il Giudice, dott. _____, letto il ricorso che precede; esaminata la documentazione depositata;

rilevato che il credito è fondato su riparti approvati dalla assemblea condominiale;

visti gli artt. 633 e segg. c.p.c. e 63 disp. att. c.c.

INGIUNGE

a _____, con sede come in atti, di pagare senza dilazione al Condominio ricorrente la somma di **Euro 10.000,00** per la causale di cui al ricorso, oltre interessi al tasso di cui al codice civile dalla domanda e sino al soddisfo nonché le spese della presente procedura che si liquidano in **€ 130,00** per spese ed **€ 800,00** per onorario, oltre rimborso spese generali, C.P.A. ed I.V.A. come per legge.

AUTORIZZA

la provvisoria esecuzione del presente decreto in mancanza di pagamento.

AVVERTE

l'ingiunto/a della facoltà di proporre opposizione innanzi a questo tribunale nel termine di giorni quaranta dalla notifica del presente decreto (termine fissato ai soli fini dell'opposizione).

Napoli, xx/xx/xx.

Il Giudice

Il formato PDF consente inoltre di gestire diverse versioni dello stesso documento senza invalidare le firme digitali apposte.

Le copie dei documenti informatici

L'articolo 22 ("*Copie informatiche di documenti analogici*") del CAD prevede che i documenti informatici, le scritture private ed i documenti in genere, abbiano piena efficacia quando vi è apposta una firma digitale, un altro tipo di firma elettronica qualificata o avanzata o comunque qualora siano stati formati previa identificazione del suo autore, in modo da garantire la sicurezza, l'integrità e l'immodificabilità dei documenti stessi e la loro riconducibilità agli autori. Viene, inoltre, aggiunto un ulteriore comma 1 bis in cui si prevede che la copia per immagine su supporto informatico di un documento analogico deve essere prodotta mediante processi e strumenti che garantiscano che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto.

L’art. 23 del CAD dispone che 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.

Sulle copie analogiche di documenti informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con le Linee guida, tramite il quale è possibile accedere al documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa del pubblico ufficiale e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico.

L’art. 23-bis del CAD sancisce, inoltre, che i duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle linee guida.

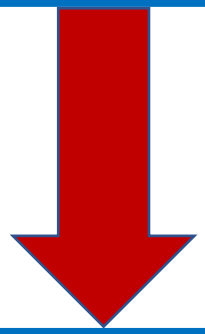
Riguardo i documenti amministrativi informatici l'art. 23-ter del CAD chiarisce che la copia su supporto informatico di documenti formati dalle pubbliche amministrazioni in origine su supporto analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto identico a quello del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza del contenuto dell'originale e della copia.

Inoltre le copie su supporto informatico di documenti formati dalla pubblica amministrazione in origine su supporto analogico ovvero da essa detenuti, hanno il medesimo valore giuridico, ad ogni effetto di legge, degli 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 o di altra firma elettronica qualificata e nel rispetto delle linee guida.

Si ricorda che alla luce delle specifiche tecniche previste dall'articolo 34, comma 1 del decreto del Ministro della giustizia in data 21 febbraio 2011 n. 44, dispone che:
"L'atto del processo in forma di documento informatico, da depositare telematicamente all'ufficio giudiziario, rispetta i seguenti requisiti:
a) è in formato PDF;
b) è privo di elementi attivi;
c) è ottenuto da una trasformazione di un documento testuale, senza restrizioni per le operazioni di selezione e copia di parti; non è pertanto ammessa la scansione di immagini;
d) è sottoscritto con firma digitale o firma elettronica qualificata esterna secondo la struttura riportata ai commi seguenti;
e) è corredato da un file in formato XML, che contiene le informazioni strutturate nonché tutte le informazioni della nota di iscrizione a ruolo, e che rispetta gli XSD riportati nell'Allegato 5; esso è denominato DatiAtto.xml ed è sottoscritto con firma digitale o firma elettronica qualificata".

La struttura del documento informatico

Le Linee guida sulla formazione, gestione e conservazione dei documenti informatici



Modalità di realizzazione del documento informatico

Utilizzo di strumenti software o servizi cloud qualificati

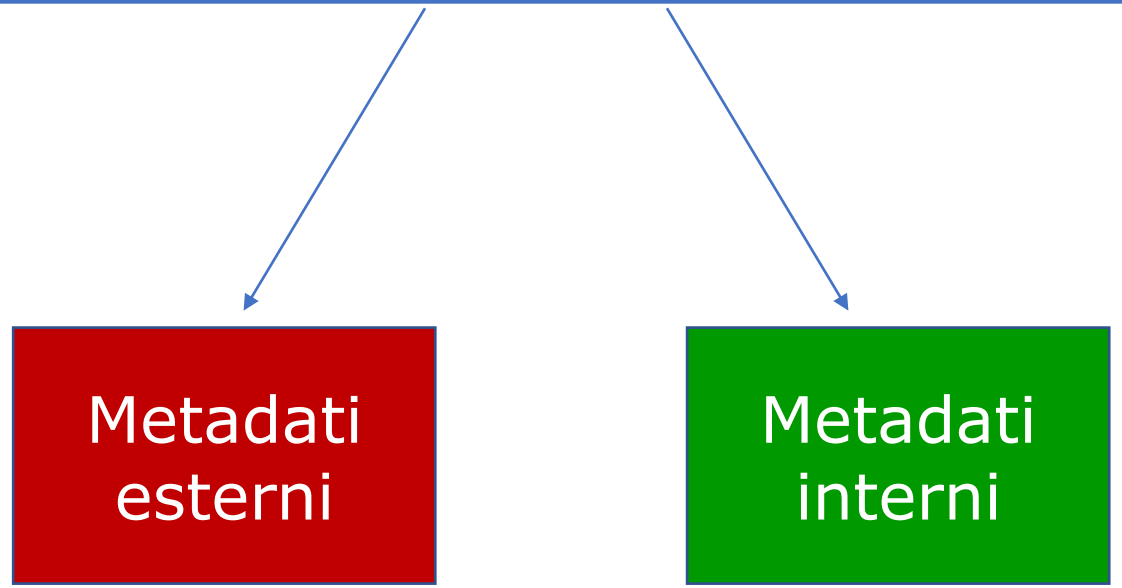
Acquisizione di un documento informatico per via telematica o su supporto informatico

Memorizzazione su supporto informatico di informazioni digitali

Generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni

I metadati

La rilevanza dei metadati



Principali metadati

Per il documento informatico generico, i metadati sono i seguenti:
Identificativo: un ID univoco composto da caratteri alfanumerici associato permanentemente a un documento.
Modalità di formazione: informazioni sui software e le modalità adottate per creare/acquisire un dato documento.
Tipologia documentale: se si tratta, ad esempio, di fatture, delibere, determine.
Dati di registrazione: tipologia di flusso, tipo di registro, data di registrazione, numero documento e codice identificativo del registro.
Chiave descrittiva: metadato che riassume o chiarisce la natura del contenuto del documento.
Soggetti: informazioni identificative di tutti i soggetti coinvolti e competenti sul documento in questione.
Allegati: eventuali allegati aggiunti al documento.
Classificazione: classificazione del documento in base al Piano di classificazione (obbligatorio nelle PA e consigliato in ambito privato).
Riservato: livello di sicurezza di un documento.
Identificativo del formato: questo metadato indica sia il formato del documento sia la versione del software utilizzato per crearlo.
Verifica: dichiara la presenza o meno di una delle modalità di convalida previste nelle Linee Guida (firma elettronica, sigillo, marcatura temporale, conformità copie immagine).
Identificativo del documento principale: codice identificativo univoco e persistente del documento principale.
Versione del documento: numero della versione del documento in questione.
Tracciature modifiche documento: metadato che tiene traccia di tutte le modifiche apportate al documento.
Tempo di conservazione: indicazione del tempo di conservazione minimo del documento in questione.

Nella pubblica amministrazione, quando si parla di formazione di un documento amministrativo informatico, ai metadati già indicati nel paragrafo precedente bisogna aggiungere:
Identificativo dell'aggregazione: identificativo del fascicolo o della serie a cui il documento è assegnato.

I metadati da associare a un'aggregazione documentale sono:
Identificativo dell'aggregazione: una sequenza di caratteri alfanumerici associata permanentemente a un'aggregazione documentale.
Tipologia di fascicolo: i fascicoli possono essere organizzati per affare, persona, attività e procedimento amministrativo. Questo ovviamente è un metadato valido solo se l'aggregazione è un fascicolo.
Soggetti e assegnazione: informazioni identificative di tutti i soggetti coinvolti e competenti sull'aggregazione documentale.
Data apertura: data di apertura dell'aggregazione documentale.
Classificazione: classificazione dell'aggregazione.
Progressivo: progressivo numerico associato all'aggregazione.
Chiave descrittiva: metadato che riassume o chiarisce la natura dell'aggregazione.
Data chiusura: data di chiusura dell'aggregazione documentale.
Procedimento amministrativo: indicazione del procedimento a cui il fascicolo afferisce. Questo ovviamente è un metadato valido solo se l'aggregazione è un fascicolo.
Indice documenti: elenco degli identificativi che rimandano a tutti i documenti presenti nell'aggregazione.
Posizione fisica: posizione fisica dell'aggregazione documentale in caso essa faccia parte di un archivio ibrido tra cartaceo e digitale.
Identificativo dell'aggregazione principale: codice identificativo univoco e persistente dell'aggregazione principale.
Tempo di conservazione: indicazione del tempo di conservazione minimo dell'aggregazione in questione e dei documenti presenti al suo interno.

Le diverse tipologie di documenti informatici

Come è facile intuire, l'evolversi della tecnologia ha portato alla proliferazione di software e tipologie di file che possono essere usati per la creazione di un documento informatico.

Documenti impaginati	PDF, Microsoft® OOXML (.docx) e Word (.doc), OpenDocument Text (.odt), Rich-Text Format (.rtf), EPUB, PostScript™ (.ps), Adobe® InDesign® Markup Language (.idml).
Ipertesti	XML, dialetti e schemi XML (.xsd, .xsl), HTML (.html, .htm), fogli di stile per XML/HTML (.xsl, .xslt, .css), Markdown (.md).
Dati strutturati	SQL, CSV, Microsoft® OOXML (.accdb) e Access (.mdb), OpenDocument Database (.odb), JSON, Linked OpenData (.json-ld), JWT.
Posta elettronica	.eml, .mbox.
Fogli di calcolo	Microsoft® OOXML (.xlsx) e Excel (.xls), OpenDocument Spreadsheet (.ods).
Presentazioni multimediali	Microsoft® OOXML (.pptx) e PowerPoint (.ppt), OpenDocument Presentation (.odp).
Immagini raster	JPEG (.jpg, .jpeg), TIFF (.tif, .tiff), PNG, GIF, OpenEXR (.exr), JPEG2000 (.jp2k, .jp2c, .jp2), DICOM, Adobe® DNG, Adobe® Photoshop® (.psd), DPX, ARRIRAW (.ari).
Immagini vettoriali e modellazione digitale	SVG, Adobe® Illustrator® (.ai), Encapsulated PostScript™ (.eps).
Modelli digitali	StereoLithography (.stl); Autodesk® DWG™, DXF™, DWF™, FBX™.
Caratteri tipografici	OpenType (.otf), TrueType (.ttf), Web Open Font (.woff, .woff2).
Suono	Waveform RIFF / Broadcast Wave (.wav, .bwf), MP3, audio RAW (.pcm, .raw, .snd), AIFF (.aiff, .aifc, .aif), FLAC, MusicXML™ (.music.xml), MIDI (.mid); molteplici codec audio.
Video	formati video delle famiglie MPEG2 e MPEG4; molteplici codec video.
Sottotitoli	TTML/IMSC/EBU-TT (.ttml, .dfxp, .xml), EBU STL.
Contenitori multimediali	MP4, MXF, MPEG2 Transport/Program Stream (.vob, .ts, .ps), AVI RIFF (.avi), Matroska (.mkv), QuickTime (.mov, .qt), WebM.
Pacchetti multimediali	pacchetto di master interoperabile (IMF, IMP); pacchetto per il cinema digitale (DCP); master per la distribuzione cinematografica (DCDM); pacchetti Digital Intermediate basati su sequenze di fotogrammi (.exr/.dpx; .wav), ACES metadata file (.amf); pacchetto XDCAM.
Archivi compressi	TAR, ZIP, GZIP, 7-Zip (.7z), RAR, TAR compresso (.tgz, .t7z, …), ISO9660 (.iso), VMware® Disk (.vmdk), Apple Disk Image (.dmg).
Documenti amministrativi	fattura elettronica, fascicolo sanitario elettronico, response SAML SPID, segnatura di protocollo.
Applicazioni e codice sorgente	eseguibili Microsoft® (.exe, .com), applet Java (.jar); pacchetti applicativi Windows® (.msi), Android (.apk), macOS® (.pkg), iOS® (.ipa); librerie statiche (.a, .lib) e dinamiche (.so, .dll, .dylib); script interpretabili (.sh, .?sh, .bat, .cmd, .py, .perl, .js, .go, .r, …); codice sorgente in vari linguaggi di programmazione (.c, .cpp, .h, .java, .asm, …).
Applicazioni crittografiche	certificati elettronici (.cer, .crt, .pem), chiavi crittografiche (.pkix, .pem), marcature temporali elettroniche (.tsr, .tsd, .tst), impronte crittografiche (.sha1, .sha2, .md5, …); per le firme e i sigilli elettronici avanzati: buste crittografiche XAdES (.xml), CAdES (.p7m, .p7s), PAdES (.pdf), contenitori ASiC (.zip); KDM (.kdm.xml).

La gestione elettronica documentale

Lo sviluppo di strumenti quali la firma elettronica ed il protocollo informatico uniti all'espansione dell'uso della posta elettronica, rende possibile la realizzazione di una gestione completamente automatizzata dei flussi documentali e la conseguente attuazione di profonde innovazioni nelle modalità di lavoro delle unità organizzative.

La gestione documentale è la gestione informatica dei documenti in modalità avanzata. È stata così denominata perché si tratta di una soluzione che privilegia ed esalta essenzialmente le potenzialità legate alla gestione informatizzata dei documenti e degli archivi.

La gestione documentale consiste in realtà in una macro-categoria, che comprende attività assai eterogenee, che variano a seconda del grado di funzionalità che si desideri attuare, ma che trovano una logica ben precisa per il loro accorpamento: ovvero il loro comune presupposto fondamentale, che è quello della dematerializzazione dei documenti cartacei e quindi della disponibilità degli stessi a livello informatico.

Le fasi del documento informatico

FORMAZIONE

(originale informatico, copia per immagine, copia informatica, duplicato)

Integrità, immodificabilità, autenticità

Le Regole Tecniche

GESTIONE DOCUMENTALE

(protocollo - registrazione e segnatura di protocollo, classificazione, organizzazione e fascicolazione, assegnazione, reperimento)

Contestualizzazione, archiviazione, ricercabilità

CONSERVAZIONE

(verifica, consolidamento, mantenimento leggibilità nel tempo, sicurezza)

La dematerializzazione dei documenti cartacei prevede le seguenti attività:

- registrazione con trattamento delle immagini (scannerizzazione dei documenti cartacei);
- assegnazione per via telematica al destinatario;
- gestione avanzata della classificazione dei documenti (utilizzo di *thesauri* e vocabolari controllati ecc.);
- collegamento dei documenti alla gestione dei procedimenti.

E’ indispensabile, inoltre, ai fini di una valida ed efficace informatizzazione delle attività di un ufficio, la cd. reingegnerizzazione dei processi interessati (in altri termini adeguare le procedure amministrative alle esigenze dell’informatizzazione).

Appare, quindi, chiaro che la vera dematerializzazione in realtà non può ridursi ai processi di digitalizzazione dei documenti, bensì consiste nel faticoso e complesso intervento di semplificazione dei processi e di diminuzione delle fasi e dei passaggi del processo decisionale, come del resto indicato negli obiettivi della legge 241 del 1990 da ormai 20 anni.

Bisogna, però, chiarire che la dematerializzazione o meglio il processo di informatizzazione della memoria documentaria, deve includere inoltre, per produrre risultati di qualche efficacia, il controllo sulla corretta formazione del documento e il governo del ciclo del documento in tutte le sue fasi incluso quello della conservazione: nessun processo di trasformazione può avere successo se non prevede la definizione di procedure e il controllo gestionale pianificato di tutte le fasi.

La conservazione sostitutiva

Riguardo la conservazione sostitutiva dei documenti informatici, l'art. 43 del CAD sancisce che gli obblighi di conservazione e di esibizione di documenti si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le relative procedure sono effettuate in modo tale da garantire la conformità ai documenti originali e sono conformi alle linee guida.

Inoltre, se il documento informatico è conservato per legge cessa l'obbligo di conservazione a carico dei cittadini e delle imprese che possono in ogni momento richiedere accesso al documento stesso ai medesimi soggetti pubblici che lo conservano. Le amministrazioni rendono disponibili a cittadini ed imprese i predetti documenti attraverso servizi on-line accessibili previa identificazione con l'identità digitale di cui all'articolo 64 ed integrati con i servizi di cui agli articoli 40-ter e 64-bis.

L'art. 44 del CAD nella sua nuova formulazione fissa i requisiti per la gestione e conservazione dei documenti informatici che deve assicurare l'indicizzazione e la ricerca dei documenti e fascicoli informatici attraverso il sistema di cui all'articolo 40-ter nel rispetto delle Linee guida.

In sintesi il sistema di conservazione dei documenti informatici deve assicurare, per quanto in esso conservato, caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, secondo le modalità indicate nelle Linee guida.

Al comma 1-bis dell'art. 44 del CAD si introduce la figura del responsabile della gestione dei documenti informatici che deve operare d'intesa con il responsabile della transizione al digitale, il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196 (ora superato), ove nominato, e con il responsabile del sistema della conservazione dei documenti informatici delle pubbliche amministrazioni, nella definizione e gestione delle attività di rispettiva competenza.

Al comma 1-quater dell'art. 44 del CAD si prevede la possibilità per il responsabile della conservazione, che opera a sua volta d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, di chiedere la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche e di protezione dei dati personali.

Questi principi sono stati approfonditi da tre decreti della Presidenza del Consiglio dei Ministri adottati in attuazione di alcune disposizioni del Codice dell'amministrazione digitale, che dettano le regole tecniche in materia di protocollazione formazione, conservazione e trasmissione dei documenti informatici.

Si fa riferimento in particolare al DPCM del 3 dicembre 2013 che detta le "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005" , al DPCM sempre del 3 dicembre 2013 che detta le "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005" ed al DPCM del 13 novembre 2014 che detta le regole tecniche per i documenti informatici previste dall'art. 20, commi 3 e 4, dall'art. 22, commi 2 e 3, dall'art. 23, e dall'art. 23-bis, commi 1 e 2 e dall'art. 23-ter del Codice dell'Amministrazione Digitale (d.lgs. n. 82/2005).

In particolare il decreto sulla conservazione sostitutiva apportando modifiche alla deliberazione CNIPA n. 11/2004 ha introdotto il concetto di "sistema di conservazione", che assicura la conservazione a norma dei documenti elettronici e la disponibilità dei fascicoli informatici, stabilendo le regole, le procedure, le tecnologie e i modelli organizzativi da adottare per la gestione di tali processi.

Viene, inoltre, disciplinata in modo più accurato la figura del responsabile della conservazione sostitutiva che definisce ed attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia in relazione al modello organizzativo di conservazione adottato.

Ogni pubblica amministrazione dovrebbe adottare anche un manuale di conservazione che dovrà illustrare dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate ed ogni altra informazione utile alla gestione ed alla verifica del funzionamento del sistema di conservazione.

In particolare è necessario indicare:
- i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
- la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
- la descrizione delle tipologie degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
- la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
- la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
- la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;

- la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
- la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
- la descrizione delle procedure per la produzione di duplicati o copie;
- i tempi entro i quali le diverse tipologie di documenti devono essere scartate ovvero trasferite in conservazione, ove, nel caso delle pubbliche amministrazioni, non già presenti nel manuale di gestione;
- le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
- le normative in vigore nei luoghi dove sono conservati i documenti.

In realtà ormai questi decreti come già si è avuto modo di vedere sono stati sostituiti dalle "Linee guida sulla formazione, gestione e conservazione dei documenti informatici" dell'AgID.

La marca temporale

Da tenere ben distinta dalla firma digitale è la marca temporale che viene apposta al fine di sottoporre a validazione temporale un'evidenza informatica.

Ricordiamo che la validazione temporale è il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

Una marca temporale contiene almeno le seguenti informazioni:

a) identificativo dell'emittente;
b) numero di serie della marca temporale;
c) algoritmo di sottoscrizione della marca temporale;
d) certificato relativo alla chiave utilizzata per la verifica della marca temporale;
e) riferimento temporale della generazione della marca temporale;
f) identificativo della funzione di hash utilizzata per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale;
g) valore dell'impronta dell'evidenza informatica.

La posta elettronica certificata

1. Quali norme la disciplinano?
2. Come funziona?
3. Quali sono le sue caratteristiche?
4. Perché è importante?

Norma fondamentale di riferimento è il D.P.R. n° 68 emanato in data 11.2.2005 con questo titolo: "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 l. 16.1.2003 n° 3".

Il Codice dell'Amministrazione Digitale (d.lgs. n. 82/2005) fa esplicito riferimento alla posta elettronica certificata all'art. 48 con rinvio al D.P.R. 68/2005 per la disciplina specifica, anche se il Consiglio di Stato avrebbe gradito (v. parere n° 11995 dell'Adunanza del 7.2. 2005) l'assorbimento dell'intero Decreto nell'ambito del CAD così come è avvenuto con il Sistema Pubblico di Connettività.

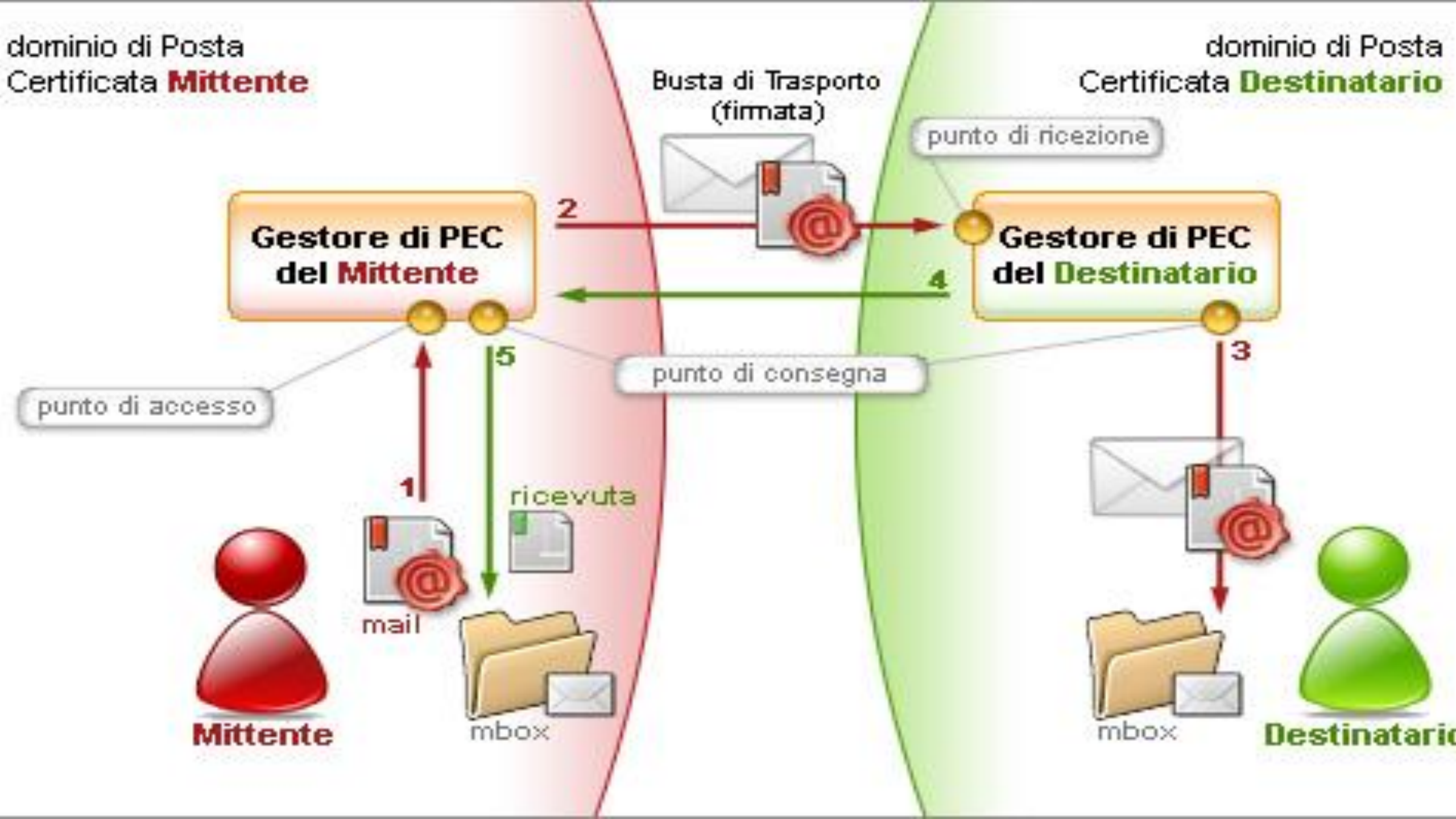
L’art. 48 prevede al primo comma che la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o mediante altre soluzioni tecnologiche individuate con le linee guida.

Al secondo comma viene sancito che 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.

Al terzo comma si precisa che 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.

Che significa certificare invio e ricezione nella PEC?

"Certificare" l'invio e la ricezione - i due momenti fondamentali nella trasmissione dei documenti informatici – significa fornire al mittente, dal proprio gestore di posta, una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale allegata documentazione. Allo stesso modo, quando il messaggio perviene al destinatario, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna con precisa indicazione temporale.


dominio di Posta
Certificata Mittente
Busta di Trasporto
(firmata)
dominio di Posta
Certificata Destinatario
punto di ricezione
Gestore di PEC
del Mittente
2
Gestore di PEC
del Destinatario
4
5
punto di consegna
3
punto di accesso
1
ricevuta
mail
mbox
Mittente
mbox
Destinatario

	PEC	E mail	Fax	Raccomandata A/R
Valore legale	SI	NO	SI	SI
Ricevuta di consegna avvenuta	SI	NO	SI	SI
Non ripudiabilità del messaggio consegnato	SI	NO	SI	SI
Inalterabilità del contenuto	SI	NO	SI	SI
Identità del mittente e del destinatario	SI	NO	NO	NO
Consegna immediata	SI	SI	SI	NO
Certezza del contenuto	SI	NO	NO	NO
Invio gratuito	SI	SI	NO	NO

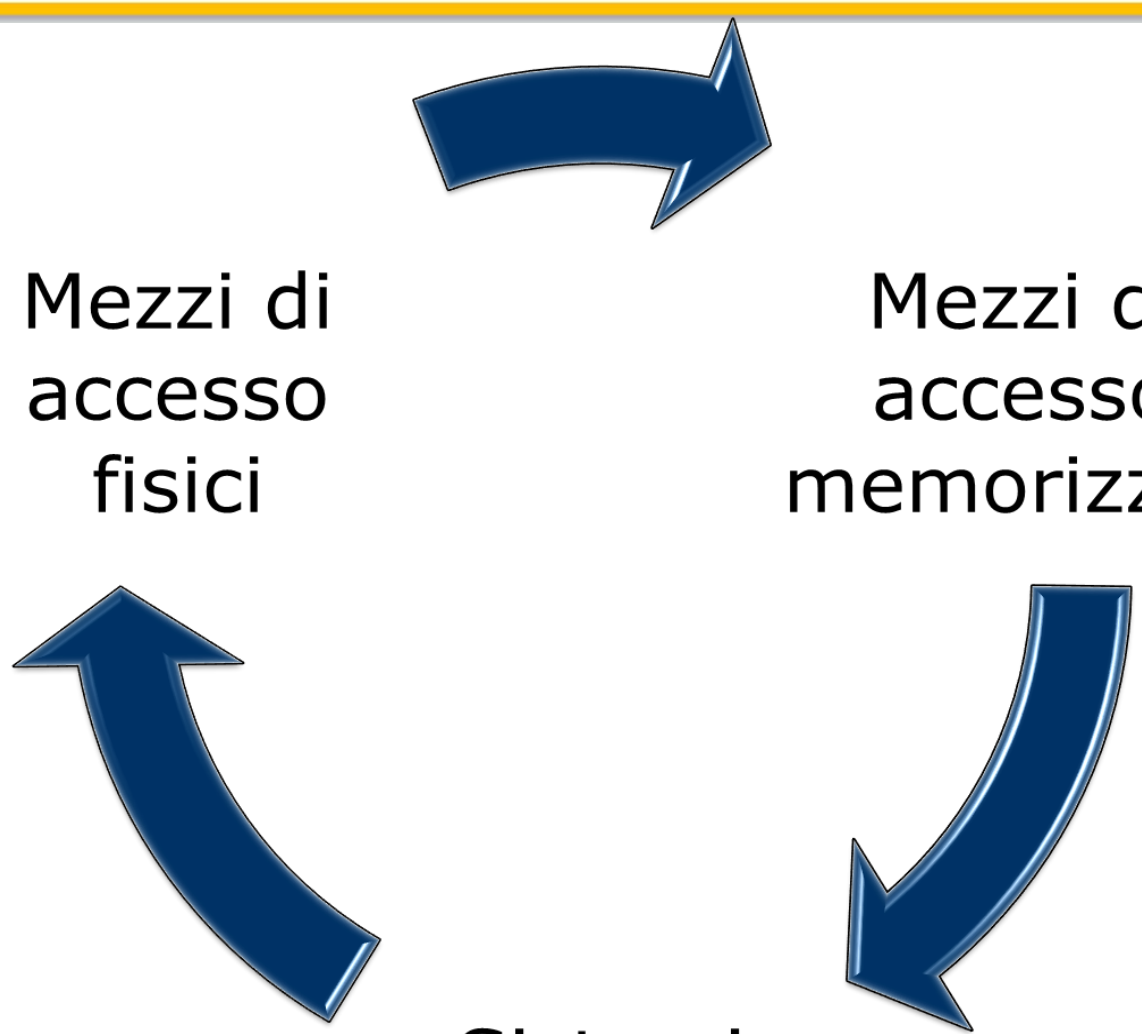
Gestione e sicurezza delle informazioni

La sicurezza nell'informatica equivale ad attuare tutte le misure e tutte le tecniche necessarie per proteggere l'hardware, il software ed i dati dagli accessi non autorizzati (intenzionali o meno), per garantirne la riservatezza, nonché eventuali usi illeciti, dalla divulgazione, modifica e distruzione.
Si include, quindi, la sicurezza del cuore del sistema informativo, cioè il centro elettronico dell'elaboratore stesso, dei programmi, dei dati e degli archivi.

Questi problemi di sicurezza sono stati presenti sin dall'inizio della storia dell'informatica, ma hanno assunto dimensione e complessità crescenti in relazione alla diffusione e agli sviluppi tecnici più recenti dell'elaborazione dati; in particolare per quanto riguarda i data base, la trasmissione dati e la elaborazione a distanza (informatica distribuita).

Riguardo l'aspetto "sicurezza" connesso alla rete telematica essa può essere considerata una disciplina mediante la quale ogni organizzazione che possiede un insieme di beni, cerca di proteggerne il valore adottando misure che contrastino il verificarsi di eventi accidentali o intenzionali che possano produrre un danneggiamento parziale o totale dei beni stessi o una violazione dei diritti ad essi associati.

Come può essere garantita la sicurezza?


Mezzi di accesso fisici
Mezzi di accesso memorizzati
Sistemi biometrici

La sicurezza nel GDPR

Non poteva, ovviamente, mancare nel Regolamento un chiaro riferimento alle misure di sicurezza che già vengono menzionate nell'art. 24 quando si chiarisce che il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento (principio di accountability).

Più nello specifico, l'art. 32 del Regolamento ne parla a proposito della sicurezza del trattamento.
Tenuto conto, quindi, dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Tali misure comprendono:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
d) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel recente passato si è assistito ad una rapida evoluzione della minaccia cibernetica ed in particolare per quella incombente sulla pubblica amministrazione, che è divenuta un bersaglio specifico per alcune tipologie di attaccanti particolarmente pericolosi.

I servizi digitali e le Piattaforme Nazionali

Lo sforzo di trasformazione sugli elementi “di base” dell’architettura digitale della PA, come infrastrutture (cloud) e interoperabilità dei dati è accompagnato da investimenti mirati a migliorare i servizi digitali offerti ai cittadini.

Soluzioni per erogare servizi di qualità

- Software as a service
- Riuso
- Modelli e strumenti validati
- Monitoraggio dei servizi on line
- Accessibilità

Strumenti disponibili

- Linee guida
- Designers Italia
- Developers Italia
- Forum Italia

Pago PA

PagoPA è la piattaforma nazionale che ti permette di scegliere, secondo le tue abitudini e preferenze, come pagare tributi, imposte o rette verso la Pubblica Amministrazione e altri soggetti aderenti che forniscono servizi al cittadino.

In particolare pagoPA permette di pagare tributi, tasse, utenze, rette, quote associative, bolli, multe, ammende, sanzioni, canoni e qualsiasi altro tipo di pagamento verso le Pubbliche Amministrazioni centrali e locali, comprese le scuole, le università, le ASL, ma anche verso altri soggetti, come le aziende a partecipazione pubblica e i gestori di pubblici servizi.

SIOPE +

SIOPE+ è l'evoluzione del Sistema Informativo sulle Operazioni degli Enti Pubblici (SIOPE) per la rilevazione ed il monitoraggio di incassi e pagamenti ordinati dalle pubbliche amministrazioni ai propri tesorieri/cassieri attraverso Ordinativi Informatici di pagamento ed incasso (OPI) emessi in conformità allo Standard OPI emanato da AgID.

Il progetto SIOPE+, disciplinato dall'art. 1, comma 533, della legge 11 dicembre 2016 (legge di bilancio 2017), impegna, con la gradualità definita da appositi Decreti MEF, tutte le Amministrazioni Pubbliche a:

1. ordinare incassi e pagamenti al proprio tesoriere o cassiere utilizzando esclusivamente ordinativi informatici emessi secondo lo Standard OPI definito dall'AgID;
2. trasmettere gli ordinativi informatici al tesoriere/cassiere solo ed esclusivamente per il tramite dell'infrastruttura SIOPE+, gestita dalla Banca d'Italia.

SPID

Come già si è avuto modo di vedere lo SPID è il Sistema Pubblico di Identità Digitale che garantisce a tutti i cittadini e le imprese un accesso unico, sicuro e protetto ai servizi digitali della Pubblica Amministrazione e dei soggetti privati aderenti.

SPID consente anche l'accesso ai servizi pubblici degli stati membri dell'Unione Europea e di imprese o commercianti che l'hanno scelto come strumento di identificazione.

Con il sistema di accesso su cui si basa SPID, la Pubblica Amministrazione è ancora più vicina ai cittadini. Garantendo a tutti una modalità di accesso ai servizi online, che è sempre uguale ed intuitiva, SPID facilita la fruizione dei servizi online e semplifica il rapporto dei cittadini con gli uffici pubblici.

L'identità SPID è rilasciata dai Gestori di Identità Digitale (Identity Provider - IdP), soggetti privati accreditati da AgID che, nel rispetto delle regole emesse dall'Agenzia, forniscono le identità digitali e gestiscono l'autenticazione degli utenti. E' possibile richiedere l'identità SPID al gestore che si preferisce e che più si adatta alle proprie esigenze. Il gestore, dopo aver verificato i dati, emette l'identità digitale, rilasciando le credenziali.

L'identità SPID è costituita, quindi, da credenziali erogate dagli identity provider o gestori di identità digitale, aziende che rispondono alle caratteristiche definite dai regolamenti tecnici e che possono fare richiesta di accreditamento all'Agenzia per l'Italia Digitale. Cittadini e imprese saranno liberi di scegliere il gestore di identità che preferiscono poiché tutti applicheranno le regole di gestione definite da AgID.

In base alle proprie esigenze, si può scegliere tra diverse modalità di riconoscimento e tre diversi livelli di sicurezza per accedere ai servizi online:

- livello 1, permette l'accesso con nome utente e password;
- livello 2, permette l'accesso con le credenziali SPID di livello 1 e la generazione di un codice temporaneo di accesso OTP (one time password) o l'uso di un'APP fruibile da smartphone o tablet;
- livello 3, permette l'accesso con le credenziali SPID e l'utilizzo di ulteriori soluzioni di sicurezza e di eventuali dispositivi fisici (es. smart card) che vengono erogati dal gestore dell'identità.

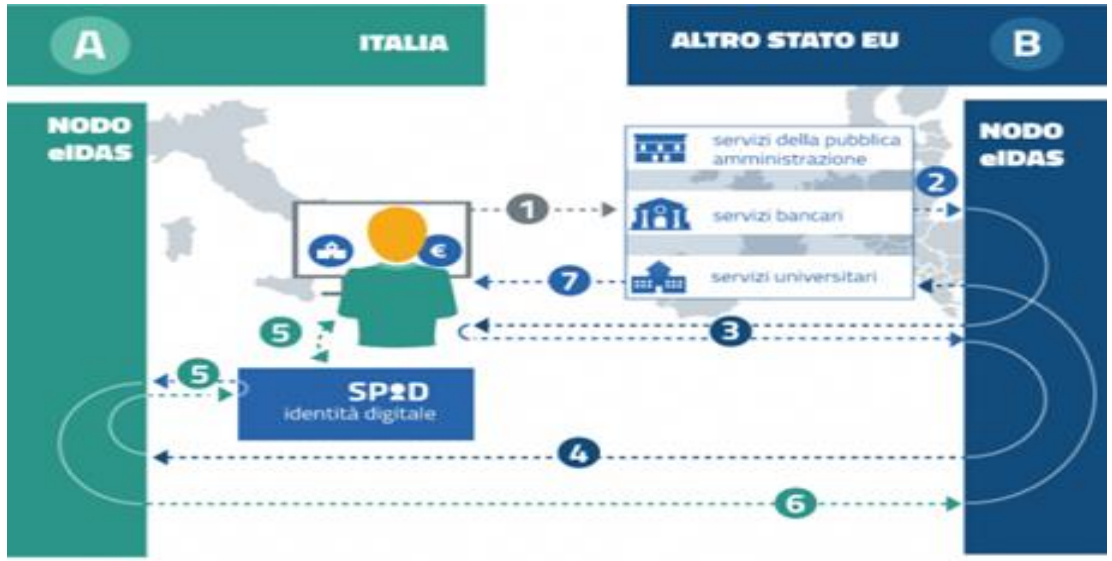
Nodo eIDAS italiano

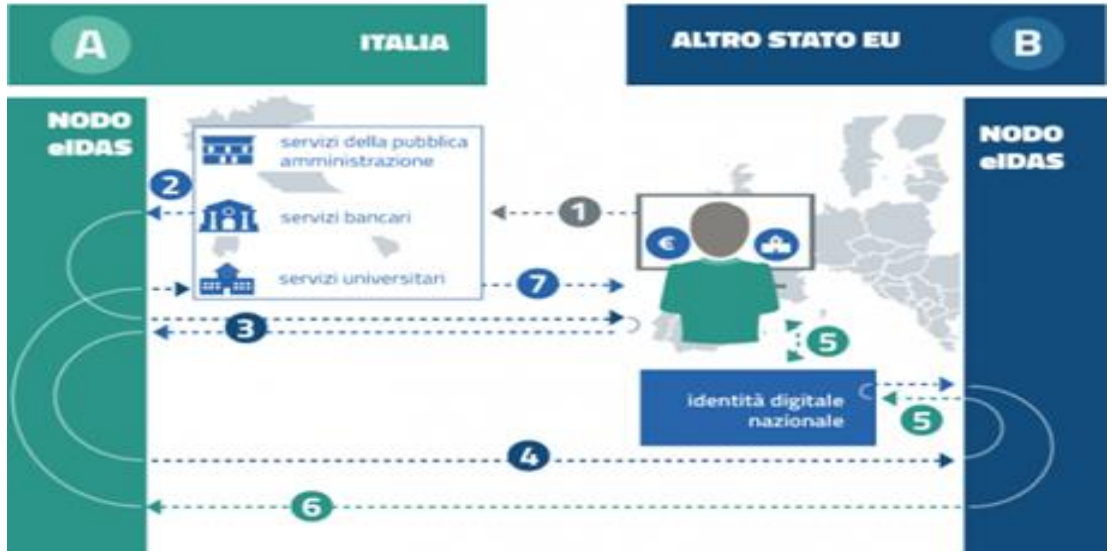
Come si è visto Il Regolamento eIDAS (electronic IDentification Authentication and Signature) - Regolamento UE n° 910/2014 sull'identità digitale - ha l'obiettivo di fornire una base normativa a livello comunitario per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri.

Il regolamento eIDAS fornisce una base normativa comune per interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni e incrementa la sicurezza e l'efficacia dei servizi elettronici e delle transazioni di e-business e commercio elettronico nell'Unione Europea.

Di seguito la descrizione del modello di funzionamento del nodo eIDAS, nel caso in cui un utente italiano richieda di fruire il servizio online di un altro stato membro della UE (e viceversa di un cittadino straniero che chiede di accedere a fornitori di servizi italiani – pubblici o privati):

1. L'utente italiano richiede l'accesso al servizio di uno stato membro UE
2. Il service provider dello stato membro invia una richiesta al proprio nodo eIDAS
3. Il nodo eIDAS dello stato membro chiede all'utente italiano il suo paese di provenienza
4. Nel momento in cui l'utente seleziona il proprio paese di provenienza, Il nodo eIDAS dello stato membro inoltra una richiesta al nodo eIDAS italiano
5. Il nodo eIDAS italiano risponde alla richiesta del nodo eIDAS dello stato membro interpellando l'identity provider del richiedente, per l'autenticazione
6. Una volta che l'autenticazione è andata a buon fine, il nodo eIDAS italiano invia una conferma al nodo eIDAS dello stato membro, che a sua volta inoltra la conferma al service provider
7. Il service provider permette all'utente italiano l'accesso al servizio richiesto.


A
ITALIA
ALTRO STATO EU
B
NODO eIDAS
NODO eIDAS
servizi della pubblica amministrazione
servizi bancari
servizi universitari
SPID
identità digitale
1
2
3
4
5
6
7


A
ITALIA
ALTRO STATO EU
B
NODO eIDAS
NODO eIDAS
servizi della pubblica amministrazione
servizi bancari
servizi universitari
identità digitale nazionale
1
2
3
4
5
6
7

E-procurement

L'e-procurement promuove la domanda pubblica di innovazione mirando alla semplificazione, digitalizzazione e trasparenza delle procedure di aggiudicazione e gestione dei contratti pubblici.

L'e-procurement rappresenta una fondamentale leva per la crescita dell'economia, per la modernizzazione ed una maggiore efficienza dei processi amministrativi, per il controllo e la riduzione della spesa pubblica.

La digitalizzazione dei processi di approvvigionamento di beni e servizi delle pubbliche amministrazioni (electronic public procurement) è uno dei principali driver delle politiche della Commissione Europea; l'obiettivo, nel medio periodo, è quello di digitalizzare l'intero processo di approvvigionamento delle pubbliche amministrazioni nelle due fasi di pre e post aggiudicazione, ovvero dalla pubblicazione dei bandi fino al pagamento (appalti elettronici end-to-end).

Fatturazione elettronica

Tutte le Pubbliche Amministrazioni hanno l'obbligo di emettere, trasmettere, gestire e conservare le fatture esclusivamente in formato elettronico.

La fattura elettronica è un documento in formato digitale la cui autenticità e integrità sono garantite da:

1. la presenza della firma elettronica di chi emette la fattura;
2. la trasmissione della fattura ad uno specifico Sistema di Interscambio (SDI).

Anagrafe Nazionale Popolazione Residente (ANPR)

L'Anagrafe Nazionale della Popolazione Residente (ANPR), è la banca dati nazionale nella quale sono confluite le anagrafi comunali.
ANPR è un sistema integrato che consente ai Comuni di svolgere i servizi anagrafici e di consultare o estrarre dati, monitorare le attività, effettuare statistiche: è il punto di riferimento per l'intera Pubblica amministrazione e per tutti coloro che sono interessati ai dati anagrafici, in particolare i gestori di pubblici servizi.

L'ANPR è istituita presso il Ministero dell'Interno ai sensi dell'articolo 62 del Dlgs n. 82/2005 (Codice dell'Amministrazione Digitale).
Non è solo una banca dati ma un sistema integrato che consente ai Comuni di svolgere i servizi anagrafici ma anche di consultare o estrarre dati, monitorare le attività, effettuare statistiche.

Carta d'Identità Elettronica

La **Carta di Identità Elettronica** (**CIE**) è il documento d'identità dei cittadini italiani emesso dal Ministero dell'Interno e prodotto dal Poligrafico e Zecca dello Stato che, grazie a sofisticati elementi di sicurezza e anticontraffazione, permette l'accertamento dell'identità del possessore e l'accesso ai servizi online delle Pubbliche Amministrazioni sia in Italia che nei Paesi dell'Unione Europea.

Oltre ad accertare l'identità del titolare, la CIE è dotata anche di una componente elettronica che – grazie all'adozione delle più avanzate tecnologie disponibili e in conformità alla normativa europea – rappresenta l'identità digitale del cittadino.

I cittadini possono accedere ai servizi online aderenti con le credenziali CIE in maniera semplice e veloce; in funzione del servizio richiesto dal cittadino, l'autenticazione può avvenire attraverso 3 livelli di autenticazione a sicurezza crescente:
livello 1: accesso mediante una coppia di credenziali (username e password),
livello 2: l'accesso prevede, in aggiunta alle credenziali di livello 1, l'impiego di un secondo fattore o meccanismo di autenticazione che certifichi il possesso di un dispositivo (es. codice temporaneo OTP, scansione QR code),
livello 3: è richiesto l'utilizzo di lettore o uno smartphone dotato di tecnologia NFC per la lettura della CIE.

Il progetto della CIE ha due obiettivi: accrescere gli elementi di sicurezza del documento di identità attraverso avanzate soluzioni tecnologiche e garantire l'emissione della Carta di Identità Elettronica per tutti i cittadini italiani residenti in Italia e per i cittadini italiani residenti all'estero iscritti all'AIRE (Anagrafe Italiani Residenti all'Estero).

A livello di sicurezza il progetto CIE può contare sulla personalizzazione centralizzata del supporto, prodotto in esclusiva dall'Istituto Poligrafico e Zecca dello Stato, e sull'aderenza ai più innovativi standard internazionali in materia di documenti elettronici.

La nuova CIE è molto più che un documento d'identità: grazie al microprocessore RF può essere letta da dispositivi NFC (es. smartphone) e usata per accedere ai varchi o per creare connessioni sicure (TLS) verso i servizi in rete.

La CIE contiene le seguenti informazioni, che sono accessibili secondo diverse modalità e livelli di protezione:

- Dati accessibili liberamente: Numero Unico Servizi (NIS)
- Dati accessibili con scansione MRZ o digitazione CAN: nome, cognome, data e luogo di nascita, sesso, cittadinanza, validità per l'espatrio, fotografia, genitori (nel caso di minorenni), indirizzo di residenza (al momento del rilascio), codice fiscale, numero di serie
- Dati accessibili con PIN: certificato client
- Dati accessibili solo a forze dell'ordine: impronte digitali


REPUBBLICA ITALIANA
MINISTERO DELL'INTERNO
CARTA DI IDENTITÀ / IDENTITY CARD
CA00000AA
COMUNE DI / MUNICIPALITY
SERENELLA MARITTIMA
COGNOME / SURNAME
ROSSI
NOME / NAME
BIANCA
LUOGO E DATA DI NASCITA
PLACE AND DATE OF BIRTH
PINO SULLA SPONDA DEL LAGO MAGGIORE (VA) 30.12.1964
SESSO
SEX
F
STATURA
HEIGHT
180
CITTADINANZA
NATIONALITY
ITA
EMISSIONE / ISSUING
30.05.2012
SCADENZA / EXPIRY
30.12.2
FIRMA DEL TITOLARE
HOLDER'S SIGNATURE
CAN
123456
COGNOME E NOME DEI GENITORI O DI CHI NE FA LE VECI
PARENTS' - TUTOR'S NAME
ROSSI MARIA
CODICE FISCALE
FISCAL CODE
RSSBNC64T70G677R
ESTREMI ATTO DI NASCITA
00000.0.A00
INDIRIZZO DI RESIDENZA / RESIDENCE
VIA SALARIA, 712
Codice fiscale
C<ITACA00000AA4<<<<<<<
6412308F2212304ITA<<<<
ROSSI<<BIANCA<<<<<<<<<<<<<<
MRZ

La CIE è quindi l'evoluzione della carta di identità in versione cartacea. Ha le dimensioni standard di una carta di pagamento (85,60 millimetri di larghezza per 53,98 millimetri di altezza) ed è realizzata con un materiale plastico in policarbonato su cui sono stampati a laser la foto e i dati del cittadino, protetti con elementi e tecniche di anticontraffazione, come ologrammi e inchiostri speciali.

La CIE è dotata di un microchip contactless che contiene:

- i dati personali, la foto e le impronte del titolare, protetti da meccanismi che ne prevengono la contraffazione e la lettura impropria;
- le informazioni per consentire l'autenticazione in rete da parte del cittadino a servizi online erogati da pubbliche amministrazioni e imprese;
- ulteriori dati per servizi a valore aggiunto, in Italia e in Europa.

Il fronte delle nuove carte di identità prodotte dalla fine del mese di settembre 2022 è arricchito dall'inserimento della bandiera dell'Unione europea e da un elemento di sicurezza contenente la sigla nazione IT.

Le carte di identità rilasciate precedentemente continuano ad essere valide fino alla naturale scadenza.

Simbolo ICAO[1]

Numero di serie del documento

Bandiera EU con sigla dello stato emittente

Dati anagrafici del titolare

Eventuale non validità per l'espatrio

Codice nazione

Data di scadenza

Card Access Number[2]

Codice fiscale in formato alfanumerico

Codice fiscale in formato barcode[4]

MRZ – Codice a lettura ottica[3]

PNRR e digitalizzazione

il Piano Nazionale di Ripresa e Resilienza (PNRR), è stato approvato nell'ambito del programma Next Generation EU e si sostanzia in un pacchetto da 750 miliardi di euro concordato dall'Unione Europea per sostenere la ripresa economica dopo la crisi causata dalla pandemia.

Il Piano è composto da un corposo pacchetto di investimenti e riforme, con l'obiettivo, tra gli altri, di accelerare la transizione ecologica e digitale, modernizzare la Pubblica Amministrazione, rafforzare il sistema produttivo, raggiungere una maggiore equità di genere, generazionale e territoriale.

La Missione 1 del Piano Nazionale di Ripresa e Resilienza si pone l'obiettivo di dare un impulso decisivo al rilancio della competitività e della produttività del Sistema Paese. Per una sfida di questa entità è necessario un intervento profondo, che agisca su più elementi chiave del nostro sistema economico: la connettività per cittadini, imprese e pubbliche amministrazioni, una PA moderna e alleata dei cittadini e del sistema produttivo e la valorizzazione del patrimonio culturale e turistico, anche in funzione di promozione dell'immagine e del *brand* del Paese.

Lo sforzo di digitalizzazione e innovazione è centrale in questa Missione, ma riguarda trasversalmente anche tutte le altre. La digitalizzazione è infatti una necessità trasversale, in quanto riguarda il continuo e necessario aggiornamento tecnologico nei processi produttivi.

La realizzazione degli obiettivi di crescita digitale e di modernizzazione della PA costituisce una priorità per il rilancio del sistema paese. Questa componente si sostanzia in:

- Un programma di digitalizzazione della Pubblica Amministrazione che include ogni tassello/abilitatore tecnologico necessario ad offrire a cittadini e imprese servizi efficaci, in sicurezza e pienamente accessibili: infrastrutture, interoperabilità, piattaforme e servizi, e *cybersecurity*
- Misure propedeutiche alla piena realizzazione delle riforme chiave delle Amministrazioni Centrali, quali lo sviluppo e l'acquisizione di (nuove) competenze per il personale della PA (anche con il miglioramento dei processi di *upskilling* e di aggiornamento delle competenze stesse) e una semplificazione/sburocratizzazione delle procedure chiave, incluso un intervento dedicato al Ministero della Giustizia per lo smaltimento dell'arretrato di pratiche.