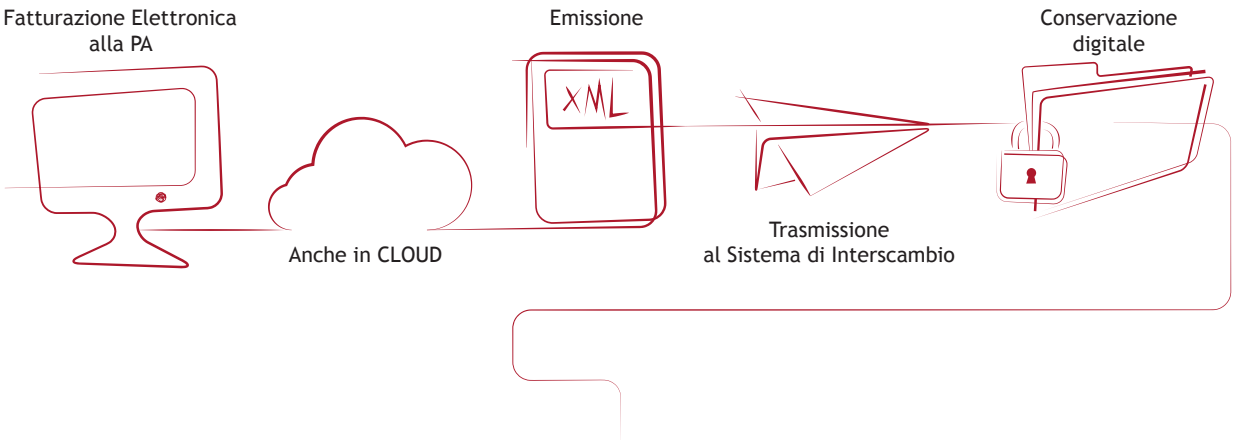
sistemiamo l'Italia

La digitalizzazione dei documenti nelle aziende e negli studi professionali

Vol. I - Conservazione digitale

Aggiornato al provvedimento del Direttore dell'Agenzia delle Entrate n.102807 del 30 giugno 2016

Progetto realizzato da Sistemi S.p.A.
in collaborazione con il Dott. Umberto Zanini.



sistemi®
Professione Informatica

La digitalizzazione dei documenti nelle aziende e negli studi professionali.

Vol. I - Conservazione digitale

Aggiornato al provvedimento del Direttore dell'Agenzia delle Entrate n.102807 del 30 giugno 2016

Progetto realizzato da Sistemi S.p.A.
in collaborazione con il Dott. Umberto Zanini.

sistemi®
Professione Informatica

Prefazione

Fare “digitalizzazione” dei documenti in Italia è possibile da ormai più di 12 anni, da quando con un insieme di regole tecniche e previsioni normative sono stati definiti il concetto di documento informatico e le relative modalità di conservazione.

Che la digitalizzazione dei documenti rappresenti una forte innovazione nei processi amministrativi è stato subito chiaro agli operatori del settore, così come i notevoli benefici economici ad essa collegati, in termini di risparmi di costi e maggiore efficienza.

Tuttavia, come spesso avviene per le innovazioni che determinano un cambiamento organizzativo, perché le aziende e gli studi professionali intraprendano in massa la nuova strada è necessario l’obbligo normativo: così è stato con l’introduzione della fatturazione elettronica verso la Pubblica Amministrazione, che dopo alcuni anni di gestazione ha finalmente visto la luce.

Sistemi ha lavorato da subito per fornire ai suoi Utenti strumenti specifici per la digitalizzazione dei documenti, supportandoli con la competenza sviluppata: oggi può quindi offrire soluzioni avanzate per la gestione della fattura elettronica e degli altri documenti, nella convinzione che i benefici più consistenti si ottengono estendendo le innovazioni a tutto il processo documentale.

La presente pubblicazione, suddivisa in due volumi, è la sintesi delle nostre conoscenze in materia, ed è stata scritta in collaborazione con il Dott. Umberto Zanini, da anni a fianco di Sistemi S.p.A. con utili indicazioni e suggerimenti oltre che con una costante attività formativa svolta a commercialisti ed aziende in ambito digitalizzazione dei documenti.

Enrica Eandi

Amministratore Delegato Sistemi S.p.A.

Sommario

Premessa

L'introduzione dell'obbligo della fatturazione elettronica alla PA, data l'innovativa soluzione adottata, pone l'Italia in posizione di avanguardia nel contesto Europeo e non solo e questo certamente stimolerà le imprese ed i professionisti ad adottare simili soluzioni.
Il 6 giugno 2014, data di entrata in vigore dell'obbligo, è stato senz'altro un passo epocale per l'intero sistema Italia ed è stato certamente un successo per il Ministero dell'Economia e delle Finanze, per l'Agenzia delle Entrate, per la Ragioneria Generale dello Stato, per Sogei Spa e per l'Agenzia per l'Italia Digitale.
Ma è stato un chiaro successo anche per tutti coloro che sin dall'inizio hanno creduto in questa iniziativa ed hanno lavorato incessantemente affinché diventasse realtà, come l'Osservatorio fatturazione elettronica e dematerializzazione della School of Management del Politecnico di Milano e la Sistemi Spa che sin dall'inizio ne supporta l'attività di studio e di ricerca.

Gli ultimi interventi normativi poi, vanno tutti verso un'unica direzione: semplificare i processi di conservazione digitale e di fatturazione elettronica per consentire un'adozione di massa di queste soluzioni da parte di imprese, studi professionali e pubblica amministrazione, perché solo in questo modo sarà possibile semplificare la burocrazia amministrativa e consentire di dedicare più tempo ad attività a più alto valore aggiunto.

Non percepire i cambiamenti in atto è dimostrazione di non essere più in sintonia con il mondo che sta cambiando, ma non basta rendersene conto, è necessario avere a disposizione utili e validi strumenti di supporto. È necessario infatti capire cosa prevede l'obbligo di fatturazione elettronica alla PA, come si svolge la conservazione digitale dei documenti tributari secondo le ultime disposizioni normative, quali sono gli adempimenti da eseguire, quali sono le criticità da evitare oltre che capire quali opportunità si celano dietro queste importanti innovazioni.

Obiettivo di questo documento, redatto con un linguaggio semplice e per quanto possibile non tecnico, è quello di dare alle imprese ed agli studi professionali un utile strumento al fine di poter affrontare in modo lineare ed organico tematiche che potrebbero sembrare ostiche, ma che in realtà non lo sono, consentendo di implementare processi di digitalizzazione senza timore di incorrere in errori o fuorvianti interpretazioni oltre che di poter meglio valutare software e soluzioni.

Con l'intento altresì di condividere i cambiamenti in essere, ulteriore obiettivo del documento è quello di spingere i lettori a riflettere su come si evolveranno nei prossimi anni i processi amministrativi e considerare la conservazione digitale e la fattura elettronica, non un semplice traguardo da raggiungere, ma l'inizio di un nuovo modo di concepire i processi amministrativi, logistici e finanziari, in grado di creare soluzioni win-win tra i vari stakeholder: soluzioni di "supply chain collaboration" tra i fornitori ed i clienti, soluzioni in grado di ridurre i costi amministrativi per le imprese ed al contempo velocizzare l'attività di verifica da parte dell'Agenzia delle Entrate, soluzioni in grado di permettere ai Commercialisti di svolgere attività a più alto valore aggiunto e di consentire agli istituti finanziari di offrire nuovi servizi di Supply Chain Finance.

Il volume è suddiviso in sette capitoli: nel primo capitolo viene analizzata la conservazione digitale dei documenti tributari e gli strumenti necessari ad implementarla, nel secondo il regolamento eIDAS e lo SPID, nel terzo la digitalizzazione dei DDT nelle imprese e nella PA con esempi di processi che possono essere adottati, nel quarto la PEC e la firma grafometrica, nel quinto sono proposte le procedure di digitalizzazione di Sistemi Spa sia per imprese che per commercialisti, gli ultimi capitoli sono dedicati ad una serie di FAQ utili a chiarire eventuali dubbi ed ai principali riferimenti normativi.

CAPITOLO 1

La conservazione digitale dei documenti fiscali

1.1 - La conservazione digitale

La fonte normativa che consente di conservare in solo formato digitale i documenti, le scritture contabili, la corrispondenza ed ogni altro atto, dato o documento, è contenuta nel decreto legislativo 7 marzo 2005 n.82 (Codice dell'Amministrazione Digitale-CAD), ove all'art.39 riporta che *"I libri, i repertori e le scritture, ivi compresi quelli previsti dalla legge sull'ordinamento del notariato e degli archivi notarili, di cui sia obbligatoria la tenuta possono essere formati e conservati su supporti informatici in conformità alle disposizioni del presente codice e secondo le regole tecniche stabilite ai sensi dell'articolo 71"*, mentre all'art.43 primo comma riporta che *"I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione e la conservazione nel tempo sono effettuate in modo da garantire la conformità dei documenti agli originali, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71"*.

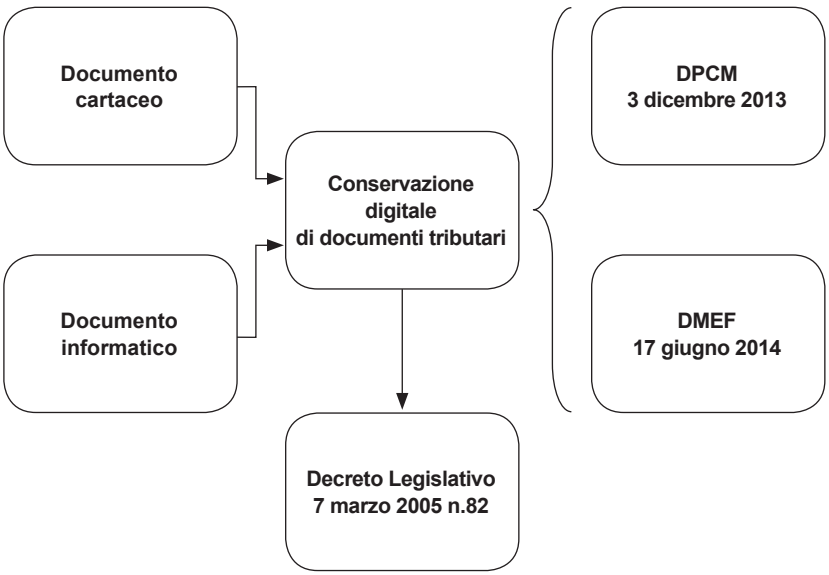
Lo stesso Codice civile contempla la possibilità di conservare documenti e scritture contabili in solo formato digitale, ed infatti l'art. 2220 terzo comma del Codice civile, introdotto dall'art.7/bis quarto comma del decreto legge n.357 del 10 giugno 1994, riporta che *"Le scritture e i documenti di cui al presente articolo possono essere conservati sotto forma di registrazioni su supporti di immagini, sempre che le registrazioni corrispondano ai documenti e possano in ogni momento essere rese leggibili con i mezzi messi a disposizione dal soggetto che utilizza detti supporti".* Va aggiunto altresì, che lo stesso art.7/bis nono comma del decreto legge n.357 del 10 giugno 1994, con riferimento all'art.2220 terzo comma del Codice civile, prevedeva che *"Con decreto del Ministro delle finanze sono determinate le modalità per la conservazione su supporti di immagini delle scritture e dei documenti di cui al presente comma"*.

L'iter normativo è concluso nei primi mesi del 2004 con la pubblicazione del DMEF 23 gennaio 2004 e della deliberazione CNIPA n.11 del 19 febbraio 2004, e quindi dal 2004 è possibile in ambito Italiano conservare in solo formato digitale, sia ai fini civili che fiscali, documenti e scritture contabili, siano essi originali cartacei, siano essi prodotti già come documenti informatici.
Decorsi 10 anni dalla loro pubblicazione, era però necessario un intervento normativo in grado sia di semplificare la tempistica che le formalità, sia di adeguare le procedure di

conservazione a standard internazionali, e nel corso del 2014 è stato pubblicato il DPCM 3 dicembre 2013 (che sostituì la deliberazione CNIPA n.11 del 19 febbraio 2004) ed il DMEF 17 giugno 2014 (che sostituì il DMEF 23 gennaio 2004).

La conservazione digitale dei documenti fiscali, si svolge quindi seguendo sia le disposizioni normative di cui al DMEF 17 giugno 2014 (entrato in vigore il 27 giugno 2014) sia le regole tecniche sui sistemi di conservazione di cui al DPCM 3 dicembre 2013 (entrato in vigore 11 aprile 2014), rilevando che per i soggetti che alla data di entrata in vigore di quest'ultimo decreto avevano già in essere dei sistemi di conservazione, è stato concesso una proroga di 36 mesi di tempo per adeguarsi.
Da rilevare poi che vi sono ulteriori disposizioni normative da considerare, come il DPCM 13 novembre 2014 (regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici), oppure il DPCM 22 febbraio 2013 (regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali).

Figura 1. ***Conservazione digitale dei documenti tributari***



È necessario poi, al fine di evitare fuorvianti interpretazioni, un breve cenno sulla corretta terminologia da adottare, dato che il processo di conservazione digitale di documenti viene definito in tanti modi: conservazione sostitutiva, conservazione ottica sostitutiva, conservazione a norma, conservazione legale, conservazione CNIPA, conservazione digitale, conservazione elettronica, conservazione informatica, etc. Sebbene la deliberazione CNIPA 11/2004 impiegasse il termine "conservazione sostitutiva" per definire il suddetto processo (anche se impropriamente dato che il termine "sostitutiva" presupponeva la presenza di un documento cartaceo da "sostituire" con un documento informatico), sia il DPCM 3 dicembre 2013 che il DMEF 17 giugno 2014 non impiegano alcun termine se non "sistema di conservazione".
Considerato che l'aggettivo "digitale" viene impiegato quando dati o documenti informatici vengono trasformati a seguito di un processo di cifratura (e.g. firma digitale), e che i suddetti sistemi di conservazione si basano sull'impiego massiccio della firma digitale (in fase di generazione delle copie per immagine su supporto informatico di documenti analogici, in fase di chiusura del processo di conservazione, in fase di esibizione dei pacchetti di distribuzione, etc), si ritiene corretto impiegare unicamente il termine "conservazione digitale".
Con il termine "conservazione digitale" quindi, si intende quel processo che applicando pedissequamente le regole di cui al DPCM 3 dicembre 2013 e DMEF 17 giugno 2014, consente di conservare in sola modalità digitale, sia ai fini civili che fiscali, documenti, scritture contabili, corrispondenza e qualsiasi altro atto o dato, sia nel caso in cui il documento sia in origine cartaceo (che per semplicità espositiva chiameremo "conservazione digitale di documento analogico") sia nel caso in cui il documento sia prodotto già come documento informatico (che per semplicità espositiva chiameremo "conservazione digitale di documento informatico").

Come avremo modo di osservare, nelle imprese, negli studi professionali ed in qualsiasi organizzazione, la conservazione digitale dei documenti impiegando le regole sui sistemi di conservazione, consente di creare una vera e propria "cassaforte digitale" il cui unico obiettivo è quello di preservare per gli anni richiesti dalla normativa di riferimento, documenti, scritture contabili, corrispondenza, libri sociali obbligatori, e qualsiasi altro documento che si intende conservare. Non quindi l'obiettivo di ricercare o consultare quotidianamente i documenti, ma di preservarli negli anni, dato che la ricerca e la consultazione, così come l'approvazione (e.g. ordine di acquisto, pagamento di una fattura, etc), lo stato del processo

(e.g. offerta economica inoltrata al cliente, etc) oppure altre attività, vengono svolte da altre procedure comunemente denominate gestione elettronica documentale (GED).
Anche se in molte aziende e studi professionali la consultazione elettronica dei documenti si svolge ancora tramite l'ausilio di cartelle (directory) di file system nominate per cliente, per tipologia documentale o per attività svolta, le soluzioni di gestione elettronica documentale (GED) stanno avendo un notevole riscontro per gli enormi vantaggi in termine di tempo risparmiato nella ricerca e nella consultazione dei documenti archiviati.

Nelle aziende quindi, mentre i sistemi di conservazione digitale, avendo l'obiettivo di preservare i documenti negli anni richiesti dalla normativa di riferimento, consentono l'accesso al sistema di conservazione a pochi soggetti (e.g. responsabile della conservazione), i sistemi di gestione elettronica documentale (GED), avendo l'obiettivo di velocizzare la ricerca e la consultazione dei documenti oltre che di gestire il passaggio dalla carta al digitale, consentono l'accesso ad una più ampia platea di utenti e tipicamente sono interfacciati con i sistemi ERP[1] oppure in alcuni casi integrati in essi.
Negli studi professionali invece, considerata la necessità di far colloquiare i sistemi informativi dello studio con quelli presenti presso i clienti al fine di velocizzare lo scambio e la consultazione dei documenti, si tende a preferire l'impiego di piattaforme di "gestione elettronica documentale" accessibili via web consentendo al cliente un accesso da remoto previa autenticazione.
Le recenti disposizioni normative, quale per esempio l'obbligo di fatturazione elettronica alla PA, indurranno sempre più gli studi professionali a dotarsi di piattaforme web di condivisione dei documenti con i propri clienti, data appunto la necessità di dover scambiare in modo semplice e veloce documenti informatici che non possono più essere consegnati o spediti su carta come appunto le fatture elettroniche in formato XML da trasmettere alla PA.

È altresì evidente la necessità per gli studi professionali, di orientarsi verso piattaforme web di condivisione documentale integrate con i sistemi informativi dello studio che siano affidabili in termini di generazione dei log utili a tracciare le attività svolte dai soggetti autorizzati ad accedervi.

1 Enterprise Resource Planning

1.2 - I benefici conseguibili

1.2.1 - I benefici per le aziende

I benefici ed i vantaggi che le aziende possono conseguire adottando processi di digitalizzazione dei documenti, sono stati da tempo documentati dall'*Osservatorio fatturazione elettronica e dematerializzazione* della School of Management del Politecnico di Milano, e li possiamo sintetizzare nei seguenti valori:

- conservazione digitale delle fatture di vendita, risparmi compresi tra 1-2 € per singola fattura;
- conservazione digitale delle fatture di acquisto, risparmi compresi tra 0,5-1,2 € per singola fattura (al netto della scansione);
- fatturazione elettronica non strutturata (e.g. PDF), risparmi compresi tra 0,6-4 € per singola fattura (per la coppia cliente-fornitore);
- fatturazione elettronica strutturata (e.g. XML), risparmi compresi tra 5,5-8,5 € per singola fattura (per la coppia cliente-fornitore);
- completa integrazione ordine-pagamento, risparmi compresi tra 25-65 € per ciclo (per la coppia cliente-fornitore).

1.2.2 - I benefici per gli studi professionali

Negli studi professionali i vantaggi ed i benefici conseguibili dall'implementare processi di digitalizzazione, derivano essenzialmente da una riduzione dei tempi di ricerca dei documenti, da una riduzione degli spazi dedicata agli archivi e da una riduzione dei costi per la stampa dei documenti.

Da una ricerca condotta dall'Osservatorio ICT & Commercialisti della School of Management del Politecnico di Milano, possiamo sintetizzare i benefici economici per i Commercialisti nei seguenti valori:

- conservazione digitale dei registri e delle scritture contabili, risparmi compresi tra 0,5-1 € per pagina;
- conservazione digitale delle fatture di vendita, risparmi compresi tra 1-3 € per singola fattura;
- conservazione digitale delle fatture di acquisto, risparmi compresi tra 1-2 € per singola fattura;
- registrazione automatica delle fatture di acquisto, risparmi compresi tra 1-2 € per singola fattura.

1.3 - Gli strumenti

1.3.1 - La firma digitale

Introdotta nell'ordinamento giuridico Italiano con il decreto legislativo del 23 gennaio 2002 n.10 che ha recepito la *Direttiva 1999/93/CE del Parlamento Europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche*, la firma digitale è uno strumento semplice da usare ed estremamente affidabile che consente di garantire l'autenticità del firmatario e l'integrità del documento informatico su cui è apposta.

Così come definita all'art.1 primo comma lettera s) dal CAD, 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 o di un insieme di documenti informatici".*

Data la sua estrema semplicità d'uso ed affidabilità in termini di sicurezza crittografica, la firma digitale viene impiegata in molti contesti, come per esempio firmare dei contratti redatti in modalità informatica, garantire l'autenticità e l'integrità delle fatture elettroniche, ultimare il processo di conservazione digitale con apposizione all'indice del pacchetto di archiviazione (SInCRO[2]) della firma digitale del responsabile della conservazione congiuntamente alla marca temporale, garantire l'integrità dei dati trasmessi tramite canale EDI[3], etc.

La firma digitale quindi, oltre che essere impiegata in contesti il cui utilizzo ha l'obiettivo di esprimere la volontà del firmatario come per esempio sottoscrivere un contratto o approvare una delibera, ed in questi casi è chiaro che dovrà essere applicato il principio WYSIWYS[4]

2 UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

3 Electronic Data Interchange

4 Il principio del WYSIWYS (What You See Is What You Sign), significa che la procedura di firma deve consentire al firmatario di firmare solo il documento che in quel momento sta visualizzando sullo screen, e quindi il firmatario avvia la procedura di firma del singolo documento dopo una sua attenta lettura. E' quanto in effetti è riportato all'art. 35 secondo comma del CAD: "*I documenti informatici devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma secondo quanto previsto dalle regole tecniche di cui all'articolo 71.*"

può anche essere impiegata come strumento di data authentication[5] per provare l'autenticità e l'integrità dei documenti informatici generati da un particolare processo, come per esempio firmare le fatture elettroniche emesse dall'impresa, ed in questi casi potrà applicarsi il diverso principio del WYDSIWYS[6].

Il rilascio dei dispositivi sicuri di firma digitale, come per esempio la smart-card, USB token, oppure dispositivi di firma massiva HSM (Hardware Security Module), viene svolto ad opera di uno dei 16 certificatori accreditati attualmente presenti nell'elenco consultabile sul sito dell'Agenzia per l'Italia Digitale (www.agid.gov.it).
È utile poi ricordare alcuni rilevanti aspetti che spesso vengono trascurati:

► Il certificato qualificato può contenere qualifiche o limitazioni d'uso
Il certificato qualificato del firmatario può contenere, oltre a specifiche qualifiche del titolare come l'appartenenza ad ordini professionali o l'iscrizione ad albi, anche eventuali limitazioni d'uso del certificato oppure limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato.

► La custodia del solo dispositivo di firma può essere affidata ad un terzo soggetto
Con riferimento alla custodia e all'utilizzo del dispositivo sicuro per la generazione della firma digitale (smart-card o USB token), vanno rilevati almeno due aspetti:

- l'art.32 primo comma del CAD riporta che: "*Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma.*";
- l'art. 11 secondo comma del DPCM 22 febbraio 2013 riporta che: "*Il dispositivo sicuro per la generazione della firma elettronica qualificata o della firma digitale deve poter essere attivato esclusivamente dal titolare mediante sistemi di autenticazione ritenuti adeguati, secondo le rispettive competenze, dall'OCSI e dall'Agenzia, prima di procedere alla generazione della firma.";*

5 Secondo il Modinis Study on Identity Management in eGovernment - Common terminological framework for interoperable electronic identity management, v2.01, November 23, 2005, "Data authentication is the corroboration that the origin and integrity of data is as claimed".

6 What You Don't See Is What You Sign

Premesso quindi che l'utilizzo e l'attivazione del dispositivo sicuro per la generazione della firma devono essere svolti personalmente dal titolare del certificato qualificato, va rilevato che l'eventuale custodia del solo dispositivo sicuro per la generazione della firma (e non quindi dei codici di attivazione che dovranno essere conservati solo dal titolare) potrebbe eventualmente essere affidata a terzi soggetti, come per esempio gli studi professionali, purchè dimostrino di aver adottato le misure organizzative e tecniche necessarie ad una sicura custodia e venga redatto un apposito incarico di custodia.

► È necessario garantire il valore nel tempo della firma digitale

Un ulteriore aspetto da tener presente al fine di evitare eventuali criticità nell'impiego della firma digitale, è dovuto al fatto che i certificati qualificati hanno un periodo di validità limitato che dipende dalla robustezza crittografica delle chiavi impiegate (solitamente durano almeno 3 anni), e così come stabilito dall'art. 62 del DPCM 22 febbraio 2013, le firme digitali il cui certificato qualificato è scaduto (revocato o sospeso) "*sono valide se alle stesse è associabile un riferimento temporale opponibile ai terzi che collochi la generazione di dette firme rispettivamente in un momento precedente alla scadenza, revoca o sospensione del suddetto certificato".*

Diventa quindi rilevante associare alla firma digitale un riferimento temporale opponibile ai terzi (e.g. marca temporale) necessario a consentire una validità nel tempo della firma digitale anche se il certificato qualificato è scaduto.

Il che significa in sostanza che è opportuno per qualsiasi documento informatico a cui è associata una firma digitale, conservarlo in modalità digitale secondo le regole previste per i documenti tributari, che prevedono appunto una firma digitale del responsabile della conservazione ed una marca temporale apposta all'indice del pacchetto di archiviazione (SInCRO).

Figura 2. ***Elenco dei certificatori accreditati***

Ragione sociale	Indirizzo della sede legale	Rappresentante legale	Man. oper. certificatore	Data iscrizione	Man. oper. sottoscritto AgID
ACTALIS S.p.A.	Via S. Clemente, 53 – 24036 Ponte San Pietro (BG) , IT	Simone Braccagni, Amministratore delegato	Link	28/03/2002	Manuale
Aruba Posta Elettronica Certificata S.p.A.	Via Sergio Ramelli, 8 – 52100 Arezzo, IT	Simone Braccagni, Amministratore unico	Link	06/12/2007	Manuale
Banca d'Italia	Via Nazionale, 91 - 00184 Roma, IT	il Governatore pro tempore	Link	23/01/2008	Manuale
Cedacri S.p.A. (già Cedacrinord S.p.A.)	via del Conventino, 1 - 43044 Collecchio (PR), IT	Sergio Capatti, Presidente	Link	15/11/2001	Manuale
Comando C4 Difesa - Stato Maggiore della Difesa	Via Stresa, 31/B - 00135 Roma, IT	Generale B.Calogero Massara, Comandante C4 Difesa	Link	20/09/2006	Manuale
Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili	Piazza della Repubblica, 59 - 00185 Roma, IT	Il Presidente pro tempore	Link	10/07/2008	Manuale
Consiglio Nazionale del Notariato	via Flaminia, 160 - 00196 Roma, IT	Il Presidente pro tempore	Link	12/09/2002	Manuale
ICBPI - Istituto Centrale delle Banche Popolari Italiane S.p.A.	Corso Europa, 18 - 20122 Milano, IT	De Censi Giovanni (Presidente)	Link	17/12/2012	Manuale
In.Te.S.A. S.p.A.	Strada Pianezza, 289 - 10151 Torino IT	Luca Altieri, Amministratore Delegato	Link	22/03/2001	Manuale
Infocert S.p.A.	Piazza Sallustio, 9 - 00187 Roma, IT	Daniele Vaccarino, Presidente CdA	Link	19/07/2007	Manuale
Intesa Sanpaolo S.p.A. (già Sanpaolo IMI S.p.A. e Banca Intesa S.p.A.)	P.za San Carlo, 156 - 10126 Torino, IT	Messina Carlo, Consigliere delegato e CEO	Link	07/04/2004	Manuale
Lombardia Informatica S.p.A.	via Don Minzoni,24 - 20158 Milano, IT	Davide Rovera, Presidente	Link	16/12/2010	Manuale
Namirial S.p.A.	Via Caduti sul Lavoro, 4 - 60019 Senigallia (AN), IT	Paolo Giacometti, Amministratore Unico	Link	03/11/2010	Manuale
Postecom S.p.A.	Viale Europa, 175 - 00144 Roma IT	Giuseppe Dallona, Amministratore Delegato	Link	20/04/2000	Manuale
Telecom Italia Trust Technologies S.r.l.	S.S. 148 Pontina - Km 29,100 - 00040 Pomezia (RM), IT	Leopoldo Genovesi, Amministratore Delegato	Link	01/01/2014	Manuale
Zucchetti S.p.A.	Via Solferino, 1 - 26900 Lodi	Alessandro Zucchetti, Amministratore delegato	Link	22/10/2015	Manuale

Funzione di hash ed impronta

Prima di trattare della firma digitale e della marca temporale, è necessario soffermarsi su due importanti argomenti che sono alla base di entrambi i suddetti strumenti oltre che dei sistemi di conservazione, e che sono la funzione di hash[7] e l'impronta (*hash value o hash code o message digest*).

A norma dell'art.1 del DPCM 22 febbraio 2013:
g) funzione di hash: una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti;

h) impronta di una sequenza di simboli binari (bit): la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash;

La funzione di hash, ed in particolare gli *one-way hash function,* sono delle funzioni aventi la caratteristica, indipendentemente dalla dimensione dell'input (file, immagine, testo, etc), di produrre un output (impronta) con una lunghezza fissa prestabilita (160 bit, 256 bit, 384 bit, 512 bit, etc).

Oltre alla suddetta caratteristica, gli *one-way hash function* hanno le seguenti 3 proprietà:

- *Pre-image resistance*: dato una impronta (output), è impossibile trovare l'input che l'ha generata ;
- *Second pre-image resistance*: dato una impronta (output) di un conosciuto input, è impossibile trovare un diverso input avente la stessa impronta (output);
- *Collision resistance*: due input diversi non possono avere una identica impronta (output).

7 Viene usato il temine hash, che in inglese significa "triturare e mescolare", perché è sostanzialmente quello che viene svolto dalla funzione che tritura il file dato in input, mescola i pezzi prodotti e poi rilascia l'output cioè l'impronta.

Proviamo a fare un semplice esempio con l'incantevole poesia *L'infinito* di Giacomo Leopardi:

Sempre caro mi fu quest'ermo colle,
e questa siepe, che da tanta parte
dell'ultimo orizzonte il guardo esclude.
Ma sedendo e mirando, interminati
spazi di là da quella, e sovrumani
silenzi, e profondissima quiete
io nel pensier mi fingo, ove per poco
il cor non si spaura. E come il vento
odo stormir tra queste piante, io quello
infinito silenzio a questa voce
vo comparando: e mi sovvien l'eterno,
e le morte stagioni, e la presente
e viva, e il suon di lei. Così tra questa
immensità s'annega il pensier mio:
e il naufragar m'è dolce in questo mare

- L'impronta calcolata sull'intero testo della poesia tramite l'algoritmo SHA-256[8] (256 bit) ed espresso in base 16 è rappresentata in questo modo: 05be86c0ab1a60e457261334705dcb99da5b8aedf18ef41bae8345d72a7e93b9

In particolare poi:

- Partendo dall'impronta è impossibile trovare l'input che l'ha generata, cioè la poesia (*pre-image resistance*);
- Partendo dall'impronta è impossibile trovare un diverso input (testo, file, etc) avente la stessa impronta (*second pre-image resistance);*
- È impossibile trovare un altro input (testo, file, etc) avente un'identica impronta (*collision resistance*).

8 Secure Hash Algorithm 256 (SHA-256)

L'impronta calcolata sull'intero testo della poesia escludendo l'ultimo carattere "e" tramite l'algoritmo SHA-256 (256 bit) ed espresso in base 16 è rappresentata in questo modo: 7afec9b2115aa12f8b20bde05bf384b3ba8adc681d3aabf78b10e0b385ee6d08

La generazione della firma digitale

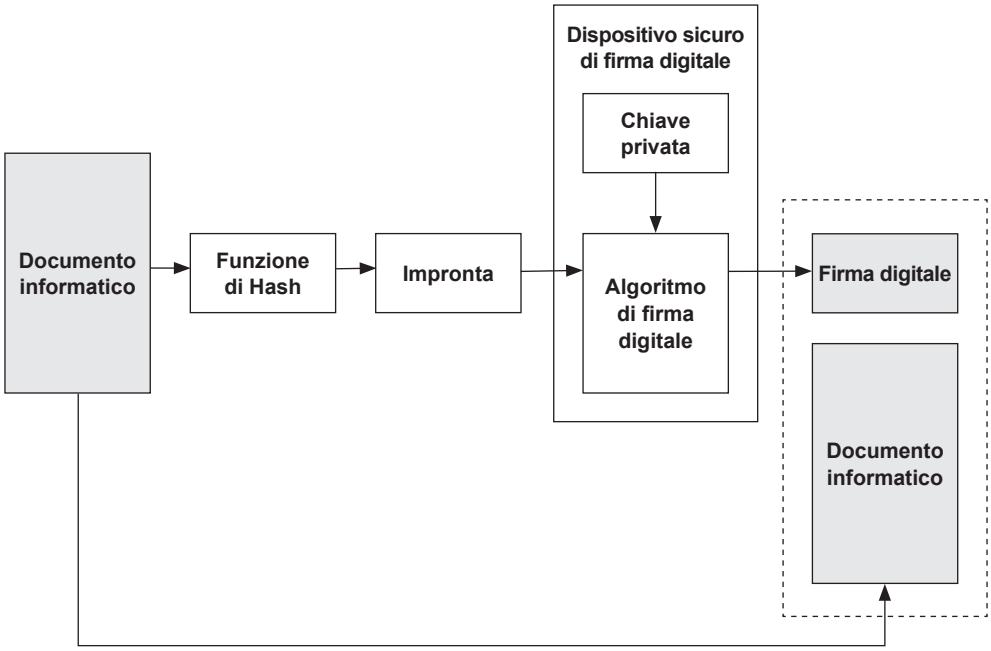
La procedura di generazione della firma digitale, che come è risaputo si svolge all'interno del dispositivo sicuro per la generazione della firma digitale (smart-card o USB token), è un processo estremamente semplice, che senza entrare nei dettagli tecnici avviene secondo i seguenti principali passaggi:

1. Tramite l'ausilio di un apposito software[9] necessario a generare la firma digitale, viene calcolata l'impronta (tramite algoritmo SHA-256) del documento informatico che si intende firmare digitalmente;
2. All'interno del dispositivo sicuro per la generazione della firma digitale (smart-card o USB token) l'impronta viene cifrata con la chiave privata del firmatario tramite algoritmo RSA[10] e generando in questo modo la firma digitale;
3. La firma digitale viene associata al documento informatico.

9 I software che ad oggi si possono impiegare per generare e verificare la firma digitale, e le cui caratteristiche tecniche sono reperibili sul sito dell'Agenzia per l'Italia Digitale (www.agid.gov.it), sono: Digital Signature Service, Digital Sign, Firma OK!gold, PkNet, Dike, Firma Certa, DSTK, View2Sign, MnlSignVerifier.

10 RSA è un algoritmo di cifratura asimmetrica a chiave privata e pubblica, che prende il nome dai tre ricercatori del MIT che nel 1978 ne hanno brevettato il funzionamento : Ronald Rivest, Adi Shamir, Leonard Adleman.

Figura 3. ***Processo di generazione della firma digitale***



La firma digitale è quindi un file, denominato busta crittografica, che contiene una serie di dati, tra cui il certificato qualificato del firmatario (il quale contiene a sua volta la chiave pubblica che consente di decifrare la firma digitale), il certificato qualificato della CA che ha emesso il certificato qualificato del firmatario, l'evidenza informatica della firma digitale vera e propria (cioè l'impronta del documento cifrata con la chiave privata del firmatario) e se lo standard di firma utilizzato lo prevede anche il documento informatico in chiaro (e.g. CAdES).

La rappresentazione visiva di una firma digitale espressa in base 16 appare in questo modo:

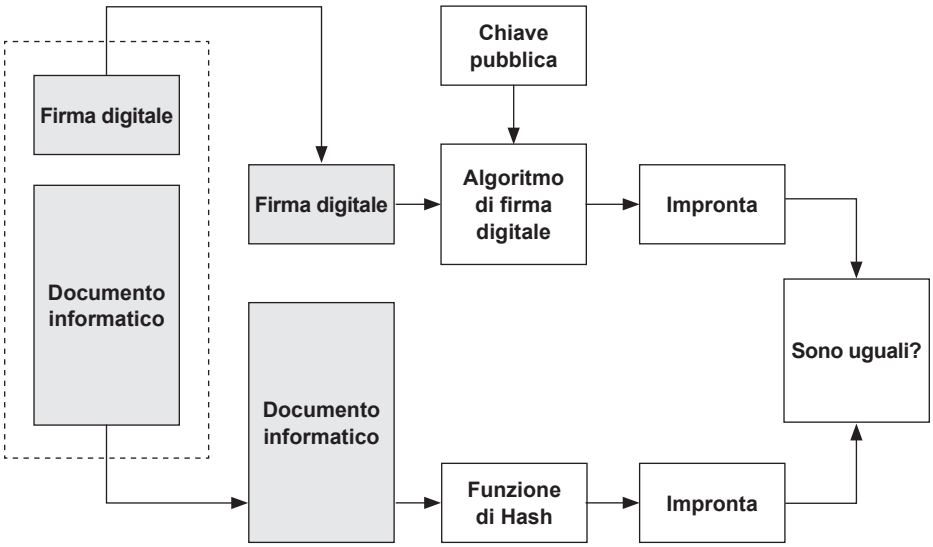
```
0A60 E8F6 C799 6317 3677 C3A6 5606 2263 9717 38D7 AE8D 5F8A FA72 87F1 C235
4C7D B36A 7157 1611 6C19 1353 FE3B 8190 C046 8556 C5A9 5238 D5EA ECFC 5810
A3CF C904 47C1 E6D3 C4FE 618F 2594 513A 4EE8 05C8 0506 B53F AFCF 45C0 3726
```

La verifica della firma digitale

Anche la procedura di verifica della firma digitale è estremamente semplice ed avviene secondo i seguenti principali passaggi:

1. Tramite l'ausilio di un apposito software (il medesimo impiegato per generarla o altri software reperibili su www.agid.gov.it), viene verificata l'autenticità del certificato qualificato dopodichè la firma digitale viene sottoposta ad un processo di controllo che impiega i medesimi due algoritmi utilizzati per generarla, la funzione di hash SHA-256 e l'algoritmo RSA. Tramite l'algoritmo RSA e con l'ausilio della chiave pubblica contenuta nel certificato qualificato del firmatario, viene decifrata la firma digitale ritornando in questo modo all'originaria impronta;
2. Viene nuovamente calcolata l'impronta del documento informatico tramite algoritmo SHA-256;
3. Si confrontano le due impronte: quella ottenuta dalla decifratura della firma digitale e quella calcolata sul documento informatico. Se le due impronte sono identiche significa che la verifica della firma digitale ha dato esito positivo, quindi il firmatario riportato nel certificato qualificato ha realmente firmato digitalmente il documento informatico a cui è associata la firma digitale.

Figura 4. ***Processo di verifica della firma digitale***



Standard di firma

Il documento informatico, dopo che è stato firmato digitalmente, può assumere diversi formati; come stabilito dalla decisione di esecuzione (UE) 2015/1506[11], e per tutti gli Stati membri i formati di riferimento delle firme elettroniche sono tre:

► **CAdES**, come indicato nelle specifiche ETSI TS 103 173 v2.2.1.
Il formato CAdES (*Cryptographic Message Syntax Advanced Electronic Signature*) è certamente il formato più diffuso e lo si riconosce subito perché quando il documento è firmato digitalmente assume l'estensione *.p7m*
La principale caratteristica di questo formato è che il documento in chiaro è contenuto nella *busta crittografica* ed è necessario avere un software che lo estragga e ne consenta la visualizzazione.

► **PAdES**, come indicato nelle specifiche ETSI TS 103 172 v2.2.2.
Il formato PAdES (*PDF Advanced Electronic Signature*) è un formato definito dallo standard ISO 32000-1 ed è utilizzabile solo per documenti in formato PDF. Le principali caratteristiche sono legate al fatto che la firma digitale è inglobata nel PDF (l'estensione rimane *.pdf*) ed è visualizzabile con i più comuni *reader* di PDF. È altresì possibile stabilire l'esatta posizione in cui apporre la firma digitale all'interno dell'intero documento (molto utile nei contratti), e decidere come verrà visualizzata la firma (e.g. Dott. Paolo Rossi, Rossi Paolo, etc).

► **XAdES**, come indicato nelle specifiche ETSI TS 103 171 v2.1.1.
Il formato XAdES (*XML Advanced Electronic Signature*) è un formato che sta avendo una notevole diffusione in quanto è quello utilizzato per firmare le notifiche/ricevute trasmesse dal SDI nell'ambito dell'obbligo della fattura elettronica alla PA.

11 *Decisione di esecuzione (UE) 2015/1506 della Commissione dell' 8 settembre 2015 che stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere, di cui all'art.27, paragrafo 5, e all' art.37, paragrafo 5, del regolamento (UE) n.910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.*

Le firme multiple

La sottoscrizione da parte di più firmatari del medesimo documento informatico è una situazione riscontrabile in diversi contesti (e.g. contratti, ordine di acquisto, etc) e spesso può essere utile avere una loro sequenzialità.
Può essere rilevante quindi avere prova che la Dott.ssa Paola Neri ha firmato digitalmente dopo il Dott. Luca Bianchi e che il Dott. Marco Rossi ha firmato digitalmente per ultimo.

Mentre in un ambiente cartaceo questa esigenza potrebbe essere in realtà non semplice da ottenere, in un ambiente digitale è possibile grazie alle diverse tecnologie impiegate nell'ambito delle "firme multiple".
Con il termine "firme multiple" si intende quindi l'apposizione al medesimo documento informatico della firma digitale da parte di più firmatari; mentre per il formato PAdES può eseguirsi aggiungendo all'interno del PDF le diverse firme digitali generate, in caso di impiego del formato CAdES oppure XAdES può eseguirsi secondo due diverse modalità:

- **Firma multipla "controfirma"**, impiegata quando è rilevante dimostrare l'ordine dei firmatari, tecnicamente si svolge firmando digitalmente una precedente firma digitale apposta dal precedente firmatario e creando in questo modo una vera e propria sequenza dei diversi firmatari;
- **Firma multipla "parallela"**, impiegata quando non è rilevante dimostrare l'ordine dei firmatari, tecnicamente si svolge firmando digitalmente i dati contenuti nella busta crittografica.

Figura 5. ***Firma multipla "controfirma"***

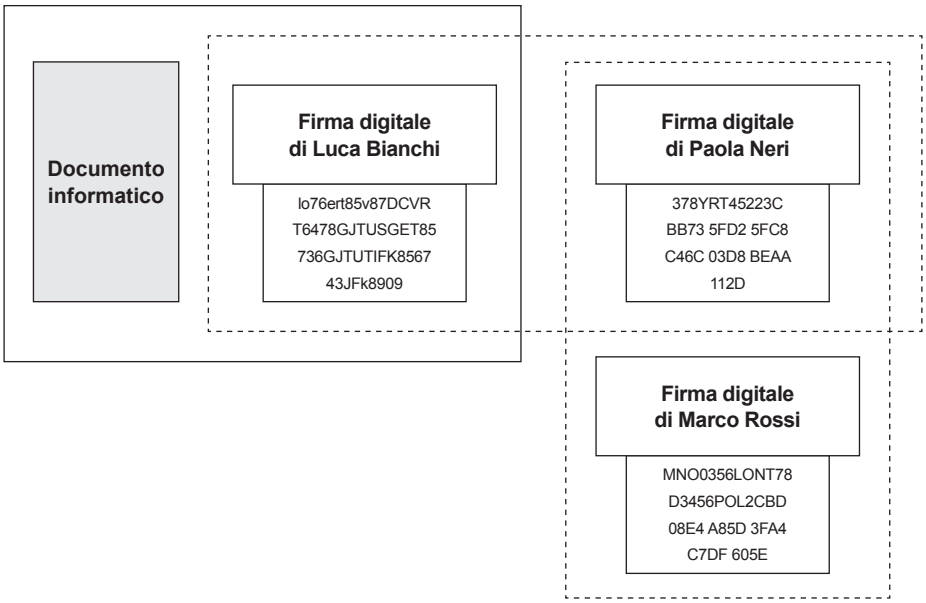
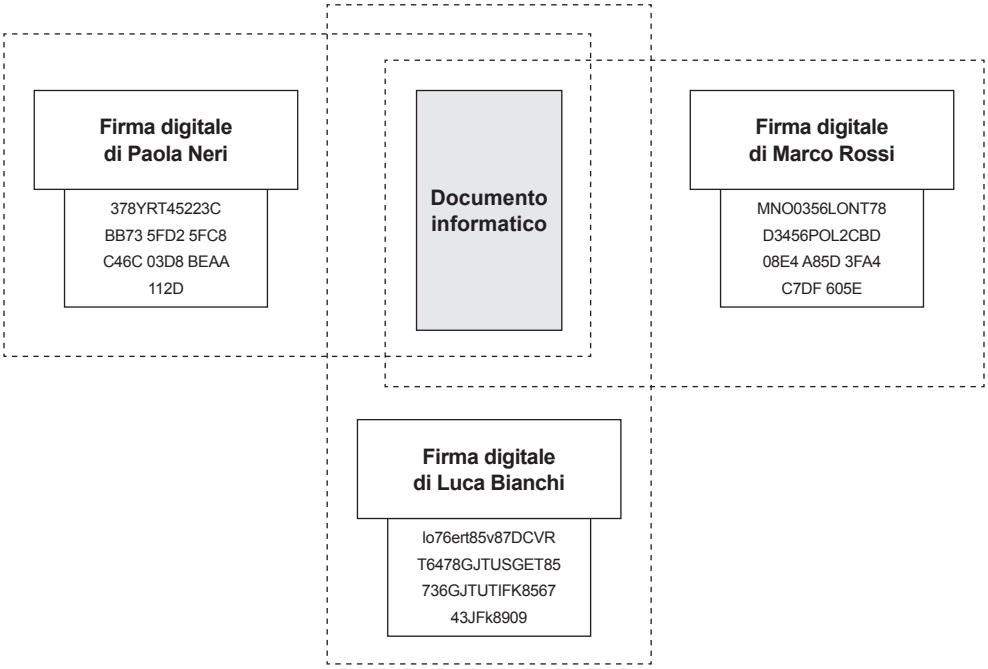


Figura 6. ***Firma multipla "parallela"***



1.3.2 - Il riferimento temporale

In un ambiente digitale così come in un ambiente cartaceo è estremamente importante stabilire con certezza il momento temporale (anno, mese, giorno ed ora) in cui si è svolto un determinato fatto, evento o attività, come per esempio quando il documento viene prodotto, quando il documento viene sottoscritto, quando una particolare attività viene svolta (integrazione o rettifica al documento).

La collocazione temporale di un determinato fatto, evento o attività che viene svolta su un documento cartaceo, viene eseguita aggiungendo allo stesso la data (anno, mese, giorno), come per esempio quando si sottoscrive una scrittura privata che oltre alla sottoscrizione si aggiunge la data ed eventualmente il luogo.

Nei casi in cui il documento cartaceo è stato redatto oppure sottoscritto senza inserire alcuna data, è eventualmente possibile stabilire in modo approssimativo il periodo in cui il documento è stato prodotto o sottoscritto, analizzando con particolari tecniche e procedure chimiche il supporto cartaceo oppure l'inchiostro utilizzato.

Quanto detto per i documenti cartacei vale naturalmente anche per i documenti digitali, dove la collocazione temporale di un determinato fatto, evento o attività è certamente più difficile (spesso impossibile), se al documento digitale non vengono associati dei dati in grado di stabilirne l'esatto momento temporale in cui l'evento si è svolto.
Le procedure informatiche previste dal legislatore Italiano in grado di associare ad un documento informatico l'esatta collocazione temporale (anno, mese, giorno, ora, minuto), le possiamo schematizzare nelle seguenti tre tipologie:

► **riferimento temporale**: "*evidenza informatica, contenente la data e l'ora, che viene associata ad uno o più documenti informatici"* (art.1 lettera m) del DPCM 22 febbraio 2013);

► **validazione temporale:** "*il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi*" (art.1 lettera bb) del CAD).

Costituiscono validazione temporale:

- Il riferimento temporale ottenuto attraverso l'utilizzo della PEC;
- Il riferimento temporale contenuto nella segnatura di protocollo di cui all'art.9 delle regole tecniche per il protocollo informatico (DPCM 3 dicembre 2013);
- Il riferimento temporale ottenuto attraverso la marcatura postale elettronica (DPR 12 gennaio 2007 n.18).

► **marca temporale**: "*il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo"* (art.1 lettera i) del DPCM 22 febbraio 2013).

Oltre alla esigenza di stabilire quando un determinato fatto, evento o attività è stata eseguita su un determinato documento informatico, oppure provare che un particolare documento informatico esisteva ad una certa data, è altresì utile accertare quando la firma digitale è stata generata.
In caso di impiego della firma digitale infatti, è necessario certificare il momento in cui la firma digitale è stata generata (oppure quello immediatamente successivo), dato che la verifica di validità del certificato qualificato va eseguita con riferimento al momento in cui la firma digitale era stata generata e non al momento in cui si svolge la verifica: *"Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso."* (art.24 terzo comma del CAD).

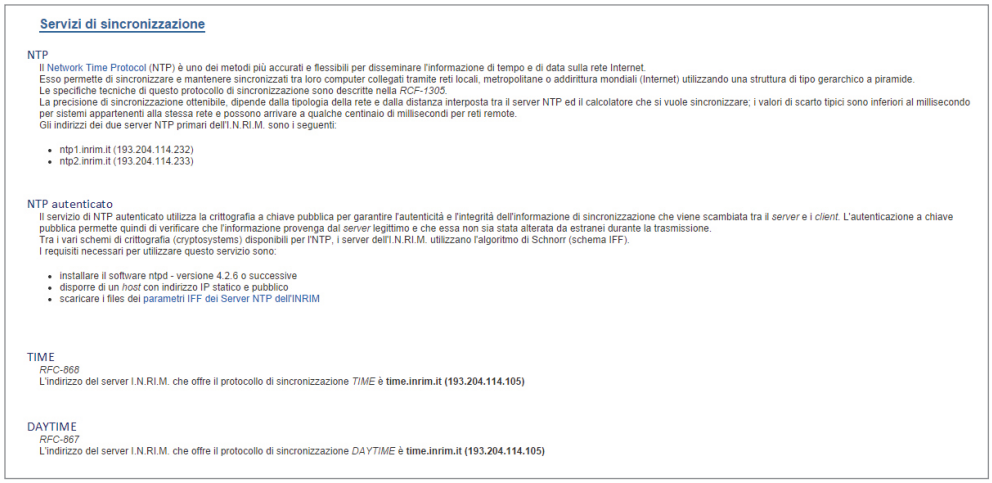
È necessario quindi associare al documento informatico firmato digitalmente (oppure anche a più documenti informatici) una informazione contenente data ed ora in grado di dimostrare il momento esatto in cui la firma digitale è stata generata, e a seconda delle diverse esigenze si potrà utilizzare un semplice ed economico *riferimento temporale,* oppure una più sicura ed inconfutabile *marca temporale*.

Nell'ambito dei processi di conservazione digitale dei documenti fiscali, la procedura informatica che solitamente viene associata alla firma digitale per provare il momento della sua generazione è il *riferimento temporale,* mentre la *marca temporale* viene utilizzata

solo a chiusura del processo di conservazione digitale congiuntamente alla firma digitale del responsabile della conservazione da apporre all'indice del pacchetto di archiviazione (SInCRO).

Il *riferimento temporale* viene generalmente prodotto dall'orologio interno del computer impiegato per generare la firma digitale, dopo che si è provveduto ad implementare una valida procedura di sincronizzazione via Internet con riconosciuti istituti di misurazione del tempo.
La sincronizzazione dell'orologio del computer via Internet, che da diversi anni ormai viene attivata automaticamente dagli stessi computer, viene eseguita tramite scambio di dati secondo un prestabilito protocollo, il Network Time Protocol (NTP).
In Italia è possibile per esempio sincronizzare l'orologio dei sistemi informativi, dei computer, dei server, dei PC, dei tablet, degli smartphone, etc tramite l'utilizzo di uno dei due server NTP primari che l'Istituto Nazionale di Ricerca Metrologica[12] mette gratuitamente a disposizione per tutti gli utenti collegati ad Internet.

Figura 7. ***Sincronizzazione tramite l'INRiM***



Servizi di sincronizzazione

NTP

Il Network Time Protocol (NTP) è uno dei metodi più accurati e flessibili per disseminare l'informazione di tempo e di data sulla rete Internet.
Esso permette di sincronizzare e mantenere sincronizzati tra loro computer collegati tramite reti locali, metropolitane o addirittura mondiali (Internet) utilizzando una struttura di tipo gerarchico a piramide.
Le specifiche tecniche di questo protocollo di sincronizzazione sono descritte nella *RCF-1305*.
La precisione di sincronizzazione ottenibile, dipende dalla tipologia della rete e dalla distanza interposta tra il server NTP ed il calcolatore che si vuole sincronizzare; i valori di scarto tipici sono inferiori al millisecondo per sistemi appartenenti alla stessa rete e possono arrivare a qualche centinaio di millisecondi per reti remote.
Gli indirizzi dei due server NTP primari dell'I.N.RI.M. sono i seguenti:

- ntp1.inrim.it (193.204.114.232)
- ntp2.inrim.it (193.204.114.233)

NTP autenticato

Il servizio di NTP autenticato utilizza la crittografia a chiave pubblica per garantire l'autenticità e l'integrità dell'informazione di sincronizzazione che viene scambiata tra il *server* e i *client*. L'autenticazione a chiave pubblica permette quindi di verificare che l'informazione provenga dal *server* legittimo e che essa non sia stata alterata da estranei durante la trasmissione.
Tra i vari schemi di crittografia (cryptosystems) disponibili per l'NTP, i server dell'I.N.RI.M. utilizzano l'algoritmo di Schnorr (schema IFF).
I requisiti necessari per utilizzare questo servizio sono:

- installare il software ntpd - versione 4.2.6 o successive
- disporre di un *host* con indirizzo IP statico e pubblico
- scaricare i files dei parametri IFF dei Server NTP dell'INRIM

TIME

RFC-868
L'indirizzo del server I.N.RI.M. che offre il protocollo di sincronizzazione *TIME* è **time.inrim.it (193.204.114.105)**

DAYTIME

RFC-867
L'indirizzo del server I.N.RI.M. che offre il protocollo di sincronizzazione *DAYTIME* è **time.inrim.it (193.204.114.105)**

12 www.inrim.it

1.3.3 - La marca temporale

A norma dell'art. 1 lettera i) del DPCM 22 febbraio 213, la marca temporale è un *"riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo".*

Diversamente dalla firma digitale, la cui generazione avviene all'interno del dispositivo sicuro per la generazione della firma digitale e quindi non vi è necessità di essere collegati ad Internet, per la generazione della marca temporale è necessario essere collegati ad Internet, dato che viene generata dal sistema di validazione temporale del certificatore accreditato.

Nel momento di generazione della marca temporale, il certificatore accreditato non include nella marca temporale alcuna informazione in grado di identificare il richiedente e quindi la marca temporale, pur garantendo l'integrità del documento informatico a cui è associata (la marca temporale è infatti una firma digitale apposta dal certificatore accreditato), non garantisce l'identificazione del richiedente la marca temporale.

Va ricordato altresì che a norma dell'art. 53 del DPCM 22 febbraio 2013, "*Tutte le marche temporali emesse da un sistema di validazione sono conservate in un apposito archivio digitale non modificabile per un periodo non inferiore a venti anni ovvero, su richiesta dell'interessato, per un periodo maggiore, alle condizioni previste dal certificatore".*
Considerato quindi che le marche temporali sono firme digitali i cui certificati qualificati sono anch'essi soggetti a scadenza, la conservazione per almeno 20 anni delle informazioni in esse contenute consente di preservare la validità delle marche temporali nel tempo senza necessità di adottare particolari procedure.

Con riferimento quindi alla conservazione digitale dei documenti fiscali ad opera di aziende o studi professionali, dopo che il processo di conservazione digitale sarà ultimato non vi è alcuna necessità di eseguire procedure al fine di rinnovare periodicamente la validità delle marche temporali.

Diversamente dalle altre validazioni temporali (e.g. PEC, segnatura di protocollo, etc), la marca temporale genera una serie di informazioni che la rendono insostituibile in molti

contesti (e.g. conservazione digitale di documenti tributari), dato che a norma dell'art. 48 primo comma DPCM 22 febbraio 2013 contiene:

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".*

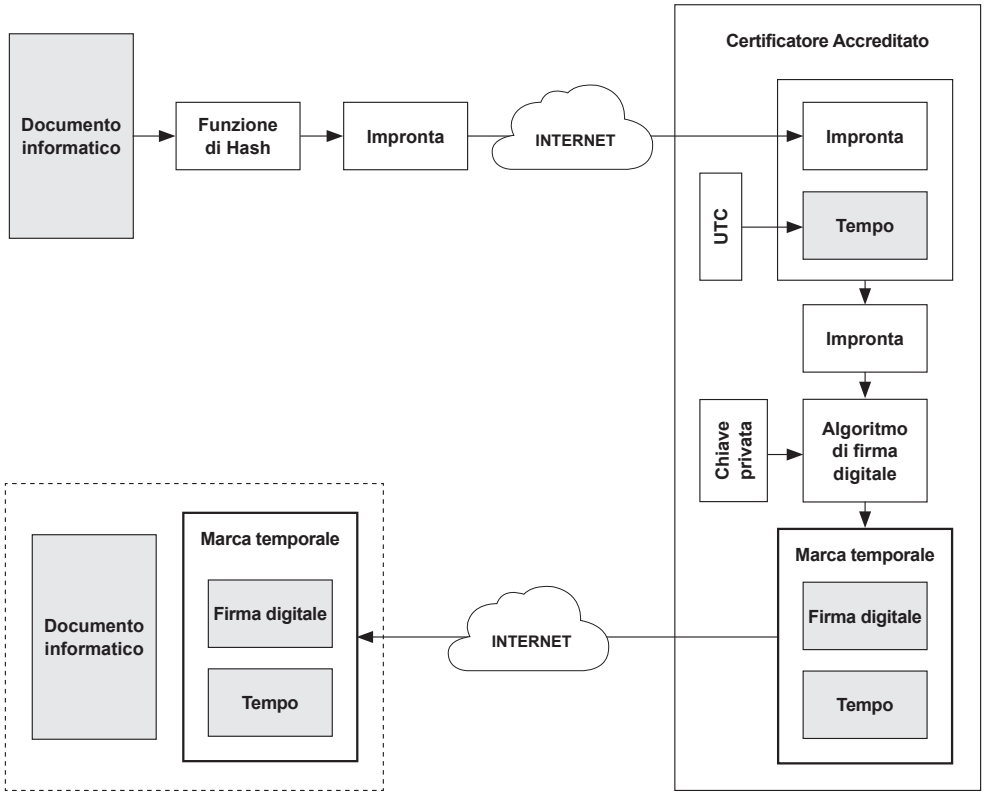
La generazione della marca temporale

La generazione della marca temporale avviene secondo i seguenti principali passaggi:

1. Il richiedente la marca temporale tramite l'ausilio di un apposito software (un elenco è reperibile su www.agid.gov.it) genera l'impronta del documento informatico a cui intende associare la marca temporale e la trasmette automaticamente via Internet al sistema di validazione temporale del certificatore accreditato (al certificatore accreditato viene trasmessa solo l'impronta del documento informatico, e non l'intero documento);
2. Il sistema di validazione temporale del certificatore accreditato riceve l'impronta del documento informatico, associa i dati inerenti il tempo UTC[13] (YYYYMMDDhhmmss), ed appone una firma digitale, creando in questo modo la marca temporale;
3. Il sistema di validazione temporale del certificatore accreditato trasmette al richiedente entro pochi secondi la marca temporale (la firma digitale ed i dati inerente il tempo UTC). Il tempo di risposta nella generazione delle marche temporali, inteso come differenza tra il momento della ricezione della richiesta e l'ora riportata nella marca temporale, non può essere superiore ad un minuto primo.

13 Il Coordinated Universal Time (UTC) è uno standard internazionale del tempo.

Figura 8. ***Processo di generazione della marca temporale***

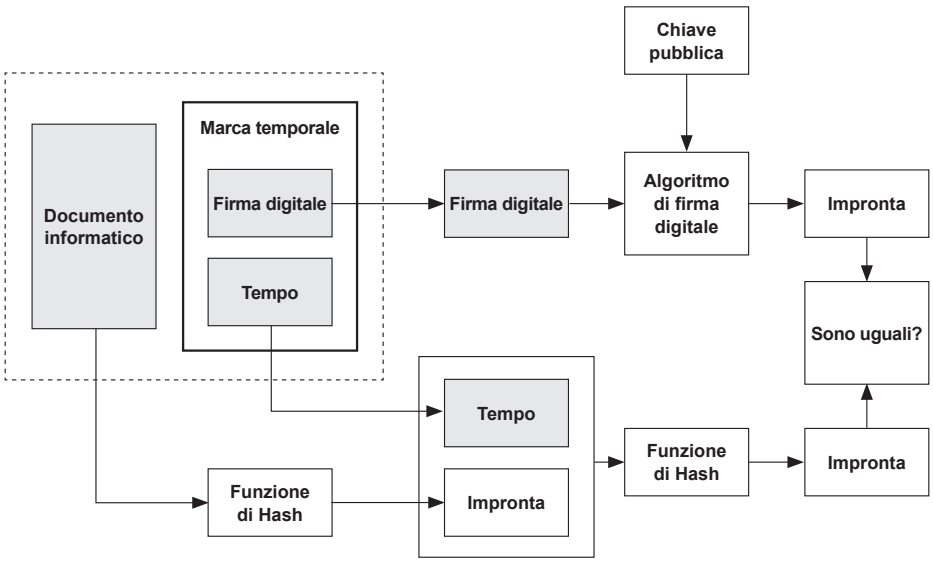


La verifica della marca temporale

La verifica della marca temporale avviene secondo i seguenti principali passaggi:

1. Tramite l'ausilio di un apposito software (il medesimo impiegato per generarla o altri software reperibili su www.agid.gov.it), con la chiave pubblica contenuta nel certificato qualificato della marca temporale, viene decifrata la firma digitale generata dal sistema di validazione temporale del certificatore accreditato, ritornando in questo modo all'originaria impronta;
2. Si calcola l'impronta del documento informatico, si associano i dati inerenti il tempo UTC (YYYYMMDDhhmmss) e si calcola nuovamente l'impronta;
3. Si confrontano le due impronte e, se identiche, significa che la verifica della marca temporale ha dato esito positivo, quindi la data e l'ora della marca temporale è stata realmente associata al documento informatico e generata dal sistema di validazione temporale del certificatore accreditato a cui è associato il certificato qualificato.

Figura 9. ***Processo di verifica della marca temporale***



1.4 - Quali documenti si possono conservare in solo formato digitale

La conservazione digitale dei documenti tributari può riguardare sia documenti cartacei (e.g. documenti di anni pregressi conservati su carta) ed in questo caso si adotterà una conservazione digitale di documenti analogici, sia documenti prodotti dai sistemi informativi già come documenti informatici e, in questi casi, si adotterà una conservazione digitale di documenti informatici.
Sebbene i suddetti processi di conservazione digitale siano i medesimi, in caso di conservazione digitale di documenti analogici vi è la necessità di produrre una *"copia per immagine su supporto informatico di documento analogico*" tramite l'ausilio di un processo di scansione.

La conservazione in solo formato digitale di documenti tributari, può essere svolta, ad esclusione di qualche eccezione, con riguardo a tutti i documenti, scritture contabili e libri sociali; ed a mero titolo esemplificativo, ma non certo esaustivo, si riporta un elenco dei suddetti documenti così come contenuto nell'allegato al provvedimento del Direttore dell'Agenzia delle Entrate del 25 ottobre 2010[14].

14 *Provvedimento attuativo della comunicazione dell'impronta relativa ai documenti informatici rilevanti ai fini tributari, ai sensi dell'articolo 5 del decreto 23 gennaio 2004*

Figura 10. ***Documenti che si possono conservare in formato digitale***

FattureEmesse
FattureRicevute
NotaVariazioneAumento
NotaVariazioneDiminuzione
DocumTrasporto
Scontrino
Ricevuta
Bolla
LibroGiornale
LibroInventari
LibroMastro
RegistroCronologico
LibroCespiti
RegistroIrpef
RegistroFattureAcquisto
RegistroAcquistiAgenzieViaggio
RegistroFattureEmesse
RegistroFattureInSospeso
RegistroCorrispettivi
GiornaleFondo
RegistroCorrispettiviAgenzieViaggio
RegistroEmergenzaIva
Bollettario
RegistroPrimaNota
RegistroUnicoIva
RegistroRiepilogativoIva
RegistroSezionaleIvaAcquisitiIntraUe
RegistroAcquistiIntraUeNonComm
RegistroTrasferimentiIntraUe
RegistroDichIntentiEmesse
RegistroDichIntentiRicevute
RegistroOmaggi
RegistroMemoriaProdContrassegno
RegistroLavorazioneProdContrassegno
RegistroCaricoProdContrassegno
RegistroScaricoProdContrassegno
RegistroBeniInDeposito
RegistroBeniInContoLavorazione
RegistroBeniComodato
RegistroBeniProva
RegistroSezionaleIvaInterno
RegistroCaricoStampatiFiscali
RegistroSocControllantiControllate
RegistroCaricoScaricoRegimeMargineMetodoAnalitico
RegistroAcquistiRegimeMargineMetodoGlobale
RegistroVenditeRegimeMargineMetodoGlobale
RegistroCaricoCentriElabDati
RegistroScaricoCentriElabDati
RegistroSommeRicevuteDeposito
RegistroEditori
LibroSoci
LibroObbligazioni
LibroAdunanzeDelibAssemblee
LibroAdunanzeDelibConsiglioAmministrazione
LibroAdunanzeDelibCollegioSindacale
LibroAdunanzeDelibComitatoEsecutivo
LibroAdunanzeDelibAssembleeAzionisti
AltriRegistri
UnicoPersoneFisiche
UnicoSocietaPersone
UnicoSocietaCapitale
UnicoEntiNonCommerciali
IrapPersoneFisiche
IrapSocietaPersone
IrapSocietaCapitale
IrapEntiNonCommercialiEdEquiparati
IrapAmministrazioniEdEntiPubblici
Modello730
ModelloConsolidatoNazionaleEMondiale
ModelloIva
ModelloIvaVrRichiestaRimborsoCreditoIva
ModelloIva26Lp2006ProspettoLiquidazioniPeriodiche
ModelloIva74Bis
ComunicazioneAnnualeDatiIva
ModelloRichiestaRimborsoCreditoIvaTrimestrale
ModelloDatiContenutiDichiarazioneIntentoRicevute
Modello770Semplificato
Modello770Ordinario
ModelloCertificazioneCud
ModelloF23
ModelloF24
ModelliAllegatiDichiarazioneRedditiModelloUnico
ModelliAnnotazioneSeparata
RicevutaPresentazioneModelliDichiarazione
AltriDocumenti

1.5 - Il DPCM 3 dicembre 2013

Con la pubblicazione del DPCM 3 dicembre 2013, che con effetto dall'11 di aprile 2014 ha sostituito la deliberazione CNIPA n. 11 del 19 febbraio 2004, il legislatore ha inteso dare un nuovo corso alle procedure di conservazione, introducendo nell'ordinamento giuridico regole e tecniche di conservazione coerenti con rilevanti standard internazionali, come per esempio lo standard ISO 14721:2012 OAIS[15]. Le regole tecniche sui sistemi di conservazione di cui al DPCM 3 dicembre 2013, che si applicano anche alla conservazione digitale dei documenti fiscali, sono caratterizzate dai seguenti principali aspetti:

► Sistema di conservazione

Il termine "*sistema di conservazione*" non va inteso come una semplice procedura informatica in grado di conservare in digitale i documenti, quanto piuttosto ad un "complesso organizzato di elementi" che nel loro insieme costituiscono appunto un "sistema" e che sono per esempio le persone che partecipano al processo di conservazione, le regole che ne governano lo svolgimento, le procedure e le tecnologie impiegate, il know-how e l'esperienza maturata negli anni, la struttura organizzativa adottata, i sistemi di storage e di backup impiegati, etc.

► Garanzia di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Il sistema di conservazione deve essere in grado di assicurare l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità degli documenti informatici conservati compresi i corrispondenti metadati ad essi associati, dove in particolare:

- **autenticità**: "*caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico*";
- **integrità**: "*insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato*";
- **leggibilità**: "*insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti*".

15 *ISO 14721:2012 Space data and information transfer systems - Open archival information system (OAIS)*

► Gestione degli oggetti da conservare tramite pacchetti informativi

Il sistema di conservazione deve essere in grado di gestire gli oggetti da conservare (i documenti informatici ed i corrispondenti metadati), tramite l'ausilio di pacchetti informativi, cioè contenitori che racchiudono gli oggetti da conservare.

I pacchetti informativi possono essere di tre diverse tipologie:

- ***Pacchetto di versamento***, il pacchetto informativo inviato dal produttore al sistema di conservazione;
- ***Pacchetti di archiviazione***, il pacchetto informativo che sarà oggetto di conservazione;
- ***Pacchetto di distribuzione***, il pacchetto informativo inviato dal sistema di conservazione all'utente che ne ha fatto richiesta.

► Individuazione dei ruoli: produttore, responsabile della conservazione, utente

È necessario individuare almeno i seguenti tre ruoli:

- ***Produttore***, che è colui che produce il pacchetto di versamento e lo invia al sistema di conservazione;
- ***Responsabile della conservazione***, che è colui che sovraintende il sistema di conservazione e che svolge le attività riportate all'art.7 del DPCM 3 dicembre 2013;
- ***Utente***, che è colui che può accedere al sistema di conservazione ed estrarne eventuali informazioni.

► Usare solo certi formati

Il formato da impiegare nella conservazione digitale, va scelto nell'ambito dei formati indicati dalle regole tecniche, ricordando di riportare nel manuale della conservazione il motivo della scelta. È comunque ammissibile impiegare anche formati diversi, purchè nel manuale della conservazione se ne riportano le motivazioni.

Figura 11. ***Formati ammessi dalle regole tecniche***

Formato	Nome completo	Società che lo ha sviluppato	Estensione	Formato aperto
PDF	Portable Document Format	Adobe Systems	.pdf	Si
PDF/A	Portable Document Format for Long-term Preservation	Adobe Systems	.pdf	Si
TIFF	Tagged Image File Format	Aldus e Microsoft, ma le specifiche erano di proprietà di Aldus (oggi Adobe Corporation).	.tif	No
JPEG	JPEG Image Encoding Family	Joint Photographic Experts Group	.jpg .jpeg	Si
OOXML	Office Open XML	Microsoft	.docx .xlsx .pptx	Si
ODF	Open Document Format for office applications	OASIS	.ods .odp .odg .odb	Si
XML	Extensible Markup Language	W3C	.xml	Si
TXT	Formato non binario leggibile			
e-mail	Messaggi email secondo le specifiche RFC 2822/MIME			

► Metadatazione dei documenti informatici

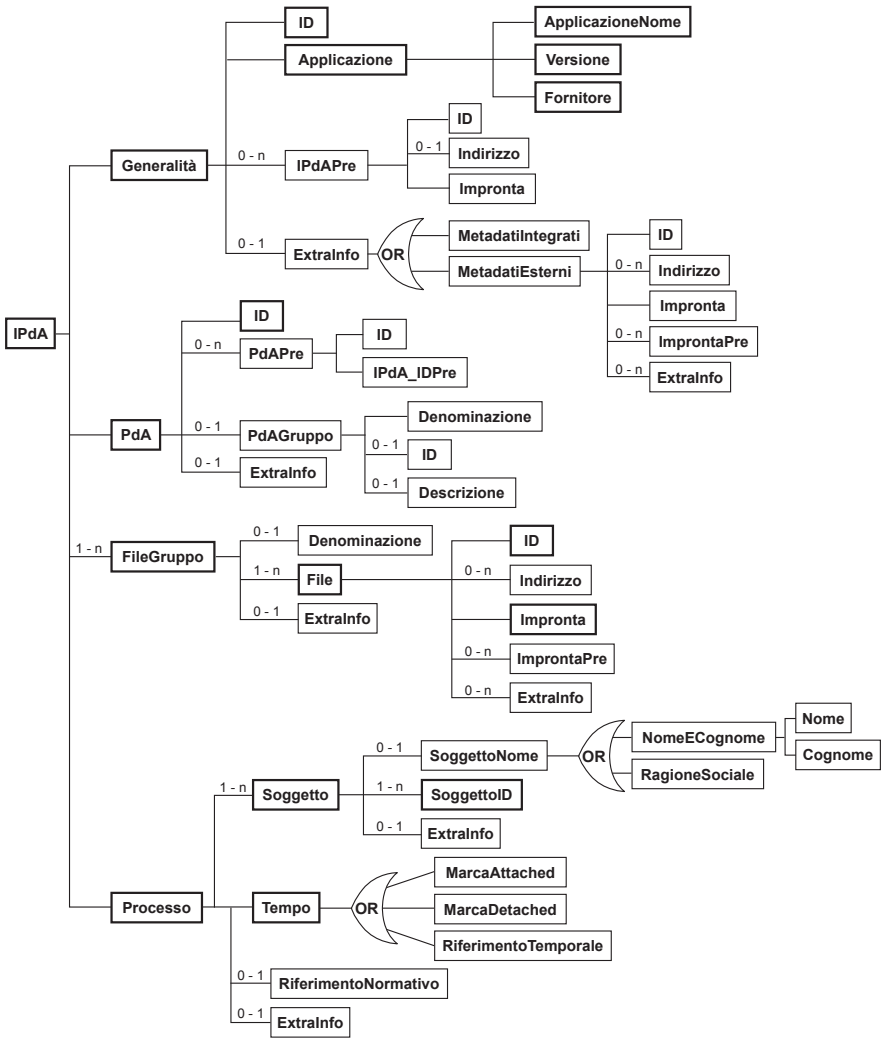
Congiuntamente ai documenti informatici è necessario conservare anche i "metadati" ad essi associati, cioè quell'insieme di dati ed informazioni che consentono di identificare e descrivere il contesto, il contenuto e la struttura del documento informatico conservato. I metadati minimi che è necessario associare ai documenti informatici oggetto di conservazione digitale sono:

- ***Identificativo,*** sequenza di caratteri alfanumerici che ne consentono l'identificazione;
- ***Data di chiusura,*** momento nel quale il documento informatico è reso immodificabile;
- ***Oggetto,*** consente di definire la natura del documento informatico (e.g. fattura di vendita, fattura di acquisto, libro giornale, etc);
- ***Soggetto produttore,*** il soggetto incaricato a produrre il documento informatico;
- ***Destinatario,*** il soggetto incaricato a ricevere il documento informatico.

► Indice del pacchetto di archiviazione secondo lo standard SInCRO

Il processo di conservazione dei documenti tributari termina con la firma digitale del responsabile della conservazione e la marca temporale sull'indice del pacchetto di archiviazione (IPdA), che dovrà essere costruito secondo lo standard SInCRO[16].

Figura 12. ***IPdA secondo lo standard SInCRO***



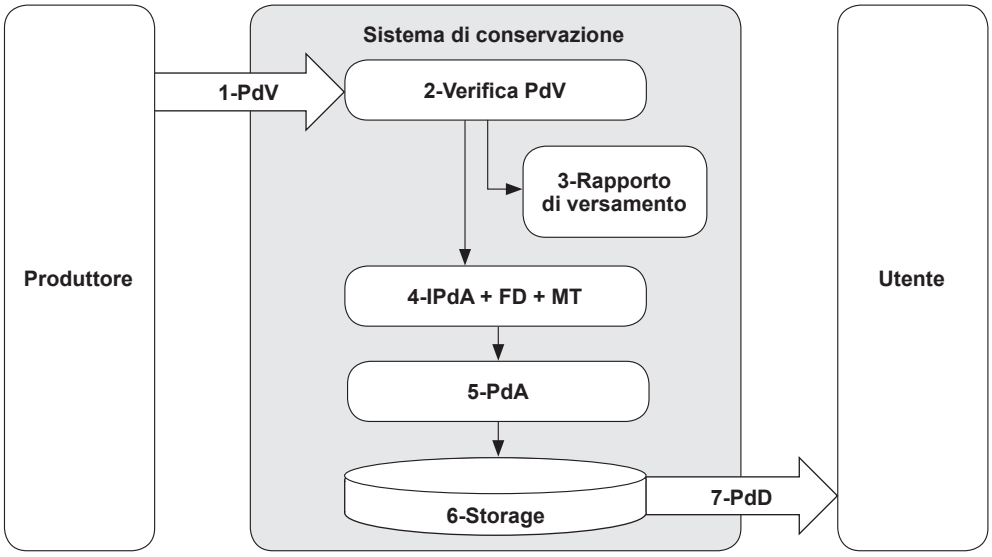
16 *UNI 11386:2010 Standard SInCRO – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.*

► Processo di conservazione seguendo precisi passaggi

Il processo di conservazione digitale dei documenti tributari si svolge secondo i seguenti passaggi:

1. Il produttore trasferisce nel sistema di conservazione i pacchetti di versamento (PdV);
2. Il sistema di conservazione verifica il contenuto dei pacchetti di versamento e se coerente con quanto previsto nel manuale della conservazione lo prende in carico, diversamente viene rifiutato;
3. Generazione del rapporto di versamento con eventuale apposizione di firma digitale;
4. Produzione dell'indice del pacchetto di archiviazione (IPdA) secondo lo standard SInCRO con apposizione della firma digitale (FD) del responsabile della conservazione e della marca temporale (MT);
5. Produzione del pacchetto di archiviazione (PdA) contenente gli oggetti da conservare compreso l'IPdA;
6. Conservazione dei documenti digitali su appositi sistemi di memorizzazione per gli anni richiesti dalla normativa di riferimento;
7. In caso di esibizione, accesso dell'utente al sistema di conservazione con produzione ed estrazione del pacchetto di distribuzione (PdD).

Figura 13. ***Processo di conservazione***



► Obbligo di istituire il manuale della conservazione

È necessario istituire e conservare in solo formato digitale il manuale della conservazione, il quale dovrà contenere le informazioni richieste dall'art.8 del DPCM 3 dicembre 2013:

"Il manuale di conservazione è un documento informatico che riporta, almeno:

a. *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;*
b. *la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;*
c. *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;*
d. *la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;*
e. *la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;*
f. *la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;*
g. *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;*
h. *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;*
i. *la descrizione delle procedure per la produzione di duplicati o copie;*
j. *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;*
k. *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;*
l. *le normative in vigore nei luoghi dove sono conservati i documenti."*

1.6 - Il DMEF 17 giugno 2014

Il DMEF 17 giugno 2014, pubblicato in GU il 26 giugno 2014, dal 27 giugno 2014 sostituisce il precedente DMEF 23 Gennaio 2004 in tema di conservazione digitale di documenti e scritture rilevanti ai fini fiscali.

Le aziende e gli studi professionali che quindi intendono conservare documenti fiscali in solo formato digitale, oltre ad avere un sistema di conservazione conforme alle regole tecniche di cui al DPCM 3 dicembre 2013, dovranno seguire le disposizioni normative riportate nel DMEF 17 giugno 2014.
I principali aspetti contenuti nel DMEF 17 giugno 2014, possono essere sintetizzati nei seguenti punti:

► **Garanzia di immodificabilità, integrità, autenticità e leggibilità.**
Il documento informatico deve avere la caratteristica dell'immodificabilità (statico e non modificabile nella forma e nel contenuto), dell'integrità (intatto ed inalterato), dell'autenticità (è ciò che dichiara di essere e che non ha subito alterazioni) e della leggibilità (leggibile all'occhio umano).

► **Conformità al Codice civile, al CAD, alle regole tecniche, ed alle disposizioni tributarie**
I documenti informatici devono essere conservati in modo che siano rispettate le disposizioni normative del Codice civile, del CAD, delle regole tecniche e delle altre disposizioni tributarie riguardanti la corretta tenuta della contabilità.

Esempio: Ordinata contabilità
L'art.2219 del Codice civile, riporta testualmente che *"Tutte le scritture devono essere tenute secondo le norme di un'ordinata contabilità, senza spazi in bianco, senza interlinee e senza trasporti in margine. Non vi si possono fare abrasioni e, se è necessaria qualche cancellazione, questa deve eseguirsi in modo che le parole cancellate siano leggibili."*
In caso di conservazione digitale, la locuzione "***secondo le norme di un'ordinata contabilità***" significa anche conservare secondo il principio di "omogeneità di conservazione per tipologia documentale e per periodo d'imposta" e quindi nel corso di un medesimo periodo d'imposta la medesima tipologia documentale (e.g. fatture di vendita, fatture di acquisto, etc) dovrà essere conservata tutta in formato digitale oppure tutta su carta, casomai impiegando diversi sezionali.

Se per esempio la società Alfa Srl ha un solo sezionale delle fatture di vendita (un'unica serie di numerazione) che conserva su carta ed in data 1 settembre 2014 emette una fattura elettronica in formato XML alla PA che dovrà essere conservata in solo formato digitale, Alfa Srl ha due strade percorribili:

- istituire dal mese di settembre un nuovo sezionale nell'ambito della tipologia documentale fatture di vendita (il nuovo sezionale potrà essere contraddistinto dalla lettera "D", cioè digitale ed avrà una propria numerazione: n.1/D, n.2/D, etc) e quindi impiegare il sezionale "D" per le fatture di vendita emesse alla PA nel corso del 2014 e che saranno conservate in digitale, ed impiegare il sezionale "C" (cioè cartaceo) per le fatture di vendita emesse sempre nel 2014 ai restanti clienti con una propria numerazione (n.1/C, n.2/C, etc) e che saranno conservate in formato cartaceo;
- continuare ad avere un solo sezionale (cioè un'unica numerazione), ma conservare tutte le fatture di vendita dell'anno 2014 in solo formato digitale. Non è in sostanza ammissibile avere un unico sezionale con riguardo alle fatture di vendita, ove alcune fatture sono conservate su carta ed altre conservate in digitale.

► Funzioni di ricerca e grafica vettoriale

Il sistema di conservazione deve essere in grado di poter estrarre i documenti conservati per i seguenti campi di ricerca: cognome, nome, ragione sociale, codice fiscale, partita IVA e data. In caso di conservazione di registri cronologici o scritture contabili (non quindi fatture, documenti di trasporto, etc) è necessario conservarli impiegando una grafica vettoriale e non raster[17], al fine di consentirne la ricerca anche all'interno del documento informatico tramite la funzione "*ricerca*", oppure "*trova*", oppure "*search*".

► Chiusura del processo di conservazione

Il processo di conservazione dei documenti fiscali termina con l'apposizione sull'indice del pacchetto di archiviazione (SInCRO) della firma digitale del responsabile della conservazione (aspetto non riportato nel DMEF 17 giugno 2014 perché già contemplato nel DPCM 3 dicembre 2013) e di un riferimento temporale opponibile a terzi, cioè una marca temporale;

17 Mentre infatti la grafica vettoriale essendo basata su delle primitive geometriche quali punti, linee, curve e forme consente una ricerca all'interno del documento (e.g. PDF del libro giornale prodotto direttamente dal sistema informativo), la grafica raster (o grafica bitmap) essendo basata sui pixel non consente una simile ricerca (e.g. TIFF del libro giornale prodotto da scansione). La differenza è evidente quando lo zoom dell'ingrandimento è al massimo, e mentre nella grafica vettoriale le linee e le immagini continuano ad essere nitide, nella grafica raster sono sgranate e poco chiare.

► Tempistica di conservazione

Il processo di conservazione dei documenti fiscali, comprese anche le fatture elettroniche emesse e ricevute, va effettuato entro il termine previsto dall'art. 7, comma 4-ter, del decreto-legge 10 giugno 1994 n. 357[18], cioè nei tre mesi successivi dal termine ultimo di presentazione delle dichiarazioni annuali.

Esempio: termine ultimo di conservazione delle fatture di vendita 2014

La società Ferrari Srl è una piccola impresa che ha iniziato l'attività il 10 luglio 2014 ed il legale rappresentante ha deciso di conservare tutti i documenti dell'aziende in solo formato digitale. Con riguardo alle fatture di vendita si è adottato la seguente procedura:

- produzione dal sistema ERP delle fatture di vendita in formato PDF (XML se il cliente è una PA);
- apposizione su ciascuna fattura PDF (oppure XML) della firma digitale del legale rappresentante congiuntamente al riferimento temporale[19], senza alcuna stampa cartacea delle fatture di vendita;
- trasmissione ai clienti tramite e-mail delle fatture in formato PDF (XML se è una PA);
- chiusura del processo di conservazione digitale di tutte le fatture emesse nell'anno 2014 con apposizione all'indice del pacchetto di archiviazione (SInCRO) della firma digitale del responsabile della conservazione (legale rappresentante) e della marca temporale entro il 30 dicembre 2015[20].

---

18 Si riporta l'art.7 comma 4/ter del decreto legge del 10/06/1994 n. 357 *"4-ter. A tutti gli effetti di legge, la tenuta di qualsiasi registro contabile con sistemi meccanografici è considerata regolare in difetto di trascrizione su supporti cartacei, nei termini di legge, dei dati relativi all'esercizio per il quale i termini di presentazione delle relative dichiarazioni annuali non siano scaduti da oltre tre mesi, allorquando anche in sede di controlli ed ispezioni gli stessi risultino aggiornati sugli appositi supporti magnetici e vengano stampati contestualmente alla richiesta avanzata dagli organi competenti ed in loro presenza".*

19 Anche se l'art.21 del DPR 633/72 non richiede più il riferimento temporale, è consigliabile certificare il momento in cui la fattura è stata firmata digitalmente, dato che la verifica di validità del certificato qualificato va eseguita con riferimento al momento in cui la firma digitale era stata generata.

20 A norma dell'art. 66 del DPR 600/73, *"Per il computo dei termini si applicano le disposizioni dell'art. 2963 del codice civile"*, mentre l'art. 2963 del Codice civile riporta che: *"I termini di prescrizione contemplati dal presente codice e dalle altre leggi si computano secondo il calendario comune. Non si computa il giorno nel corso del quale cade il momento iniziale del termine e la prescrizione si verifica con lo spirare dell'ultimo istante del giorno finale. Se il termine scade in giorno festivo, è prorogato di diritto al giorno seguente non festivo. La prescrizione a mesi si verifica nel mese di scadenza e nel giorno di questo corrispondente al giorno del mese iniziale. Se nel mese di scadenza manca tale giorno, il termine si compie con l'ultimo giorno dello stesso mese".*

► Conservazione di documenti analogici

La conservazione dei documenti analogici (cartacei) in solo formato digitale prevede due distinte fasi:

- **procedimento di generazione** delle "*copie informatiche e delle copie per immagine su supporto informatico di documenti e scritture analogici*", che termina con l'apposizione sul documento informatico della firma digitale. Va rilevato che la produzione delle "*copie informatiche e delle copie per immagine su supporto informatico di documenti e scritture analogici*", potrà essere svolta oltre che tramite l'impiego di scanner, anche tramite l'acquisizione dell'immagine digitale, purchè "*il procedimento di acquisizione garantisca che l'immagine rispecchi in maniera fedele, corretta e veritiera i dati, i fatti e gli atti che il documento rappresenta*[21]*";*
- **procedimento di conservazione digitale,** che termina con l'apposizione sull'indice del pacchetto di archiviazione (SInCRO) della firma digitale del responsabile della conservazione e della marca temporale. In caso di documenti analogici originali unici (e.g. scheda carburante) è necessario che l'immagine digitale venga autenticata da un notaio o altro pubblico ufficiale, oppure è sempre possibile istituire due sezionali (due distinte serie di numerazione) lato fatture di acquisto.

► Comunicazione in dichiarazione redditi di conservazione digitale

Il contribuente che adotta una conservazione digitale dei documenti rilevanti ai fini tributari, lo dovrà comunicare nella dichiarazione dei redditi relativa al periodo di imposta di riferimento e con riguardo al modello Unico 2016:

- Unico 2016-SC (Società di Capitali), si dovrà indicare il codice 1 nel rigo RS104;
- Unico 2016-SP (Società di Persone), si dovrà indicare il codice 1 nel rigo RS40;
- Unico 2016-ENC (Enti non Commerciali ed equiparati), si dovrà indicare il codice 1 nel rigo RS83;
- Unico 2016-PF (Persone Fisiche), si dovrà indicare il codice 1 nel rigo RS140.

21 Risoluzione 158/E del 15 giugno 2009

► Esibizione in caso di verifiche, controlli o ispezioni

In caso di verifiche, controlli o ispezioni, è necessario che il documento informatico conservato:

- sia "*reso leggibile*", quindi in caso di conservazione di documenti fiscali in formato XML (per esempio fattura elettronica alla PA) è necessario avere delle procedure o dei software (installati in house oppure fruibili via Internet), che consentono di visualizzare sullo screen i suddetti file in un formato leggibile all'occhio umano;
- sia "*disponibile su supporto cartaceo o informatico*" presso la sede del contribuente ovvero presso il luogo di conservazione delle scritture dichiarato ai sensi dell'art. 35 del DPR 633/72.

► Imposta di bollo assolta entro 120 giorni dalla chiusura dell'esercizio

L'imposta di bollo sui documenti informatici rilevanti ai fini fiscali, quali le fatture elettroniche, le scritture contabili ed altri atti, documenti o registri, viene assolta tramite versamento con F24 da eseguirsi entro 120 giorni dalla chiusura dell'esercizio. Con riguardo poi alle scritture contabili, quali il libro giornale o il libro inventari, tenute in modalità meccanografica e conservate unicamente in digitale, l'imposta di bollo è dovuta ogni 2.500 registrazioni o frazioni di esse.

Esempio: assolvimento imposta di bollo

La società Ferrari Srl nel corso del 2015 emette 10 fatture elettroniche alla PA, di cui 3 con imposta di bollo, e quindi:

- nel formato XML della fattura elettronica PA, nel campo <*BolloVirtuale*> dovrà essere riportato "*SI*", e nel campo <*ImportoBollo*> dovrà essere inserito <*2.00*>
- entro il 30 aprile 2016 dovrà essere versata l'imposta di bollo pari ad € 6.00 tramite F24 impiegando il codice tributo 2501.

1.7 - La conservazione digitale dei documenti nelle aziende

1.7.1 - Esempio 1 - Fatture di vendita

Beta Srl svolge un'attività di commercio all'ingrosso di prodotti nel settore meccanico, emette annualmente circa 15.000 fatture di vendita (fatture differite a fine mese), ha un unico sezionale ed ha deciso di adottare dal 1 settembre 2014 una conservazione digitale delle sole fatture di vendita tramite l'impiego di una soluzione di conservazione digitale in house. L'azienda ha nominato quale responsabile della conservazione il direttore amministrativo Dott.ssa Paola Bianchi, e la conservazione dal 1 settembre 2014 viene svolta secondo i seguenti principali passaggi:

1. produzione alla fine di ciascun mese delle fatture differite in formato PDF inerenti le consegne eseguite nel corso del mese;
2. apposizione su ciascuna fattura in formato PDF, della firma digitale della Dott.ssa Paola Bianchi e del riferimento temporale attestante il momento della firma;
3. emissione delle fatture ai clienti sia tramite spedizione postale previa loro stampa ed imbustamento, sia tramite trasmissione e-mail per i clienti che hanno acconsentito a ricevere le fatture in questa modalità;
4. nessuna stampa delle fatture di vendita da parte dell'azienda ed, entro il 30 dicembre 2015, conservazione digitale di documento informatico di tutte le fatture emesse dal 1 settembre 2014 al 31 dicembre 2014, tramite apposizione all'indice del pacchetto di archiviazione (SInCRO) della firma digitale della Dott.ssa Paola Bianchi congiuntamente ad una marca temporale;
5. avendo un solo sezionale con riguardo alle fatture di vendita, l'azienda dovrà conservare in digitale tutte le fatture emesse nel corso del 2014 (non è ammissibile che alcune fatture di vendita siano conservate su carta ed altre in digitale) ed è quindi necessario adottare una conservazione digitale di documento analogico delle fatture emesse nel periodo 1 gennaio 2014 - 31 agosto 2014, e quindi:
    a. procedimento di generazione delle *copie per immagine su supporto informatico di documento analogico*, previa acquisizione dell'immagine digitale già prodotta (non è necessario scansionare le fatture);
    b. apposizione sul singolo documento informatico della firma digitale della Dott.ssa Paola Bianchi congiuntamente ad un riferimento temporale;
    c. conservazione digitale di documento analogico di tutte le fatture emesse dal 1 gennaio 2014 al 31 agosto 2014, tramite apposizione all'indice del pacchetto

di archiviazione (SInCRO) della firma digitale della Dott.ssa Paola Bianchi congiuntamente ad una marca temporale;

d. distruzione delle fatture cartacee conservate del periodo 1 gennaio 2014 - 31 agosto 2014, tramite l'ausilio di una società specializzata;

6. conservazione dei file su dedicati server localizzati nella sede dell'azienda e sottoposti ad opportune procedure di salvataggio dei dati in grado di ridurre al minimo il rischio di distruzione, perdita o danneggiamento.

1.7.2 - Esempio 2 - Fatture di acquisto

Gamma Srl svolge un'attività di produzione e commercio nel settore abbigliamento, riceve annualmente circa 12.000 fatture di acquisto, ha un unico sezionale, ed ha deciso di conservare dal 2014 le fatture di acquisto in solo formato digitale tramite l'impiego di una soluzione di conservazione digitale fruibile in modalità SaaS[22].

L'azienda ha nominato, quale responsabile della conservazione, il direttore dei sistemi informativi Dott. Franco Rossi e la conservazione viene svolta secondo i seguenti principali passaggi:

1. ricezione delle fatture di acquisto tramite posta ordinaria oppure e-mail, ed in quest'ultimo caso le fatture vengono stampate su carta. L'azienda utilizza anche le schede carburanti (circa 50 ad anno), e per questo motivo si è deciso di istituire un nuovo sezionale denominato "C" (carta) in cui confluiranno le fatture di acquisto conservate su supporto cartaceo (schede carburante), mentre nell'altro sezionale denominato "D" (digitale) confluiranno tutte le restanti fatture conservate in solo formato digitale;
2. registrazione delle fattura in contabilità, e tramite l'impiego di una piccola stampante di etichette adesive in uso a ciascun operatore e collegata con il sistema aziendale GED interfacciato con il sistema ERP, dopo aver ultimato la registrazione della singola fattura viene stampata una etichetta adesiva riportante in chiaro il protocollo IVA (Art. 25 del DPR 633/72), la data della registrazione ed il barcode;

22 Software as a service (SaaS), significa che l'utente utilizza il software della software house tramite rete Internet, senza quindi più necessità di dotarsi di costosi computer o dover affrontare oneri di manutenzione e di aggiornamento, ma è necessario però che vi sia una buona banda in termini di velocità trasmissione dati.

3. apposizione della etichetta adesiva in un'area libera della fattura cartacea, ed ultimate tutte le registrazioni della giornata (oppure della settimana), scansione massiva di tutte le fatture di acquisto registrate tramite l'impiego di qualsiasi tipologia di scanner, con automatica acquisizione delle immagini da parte del sistema GED e contestuale metadatazione grazie al riconoscimento del barcode apposto sulla singola fattura;
4. entro il mese successivo a ciascun trimestre (ma la tempistica può essere diversa), tramite l'ausilio di apposito software fruibile in modalità SaaS, apposizione sul singolo documento informatico della firma digitale del Dott. Franco Rossi congiuntamente ad un riferimento temporale e conservazione digitale di documento analogico di tutte le fatture di acquisto registrate nel trimestre, tramite apposizione all'indice del pacchetto di archiviazione (SInCRO) della firma digitale del Dott. Franco Rossi congiuntamente ad una marca temporale;
5. dopo aver ultimato la conservazione digitale del trimestre, distruzione delle fatture di acquisto tramite l'ausilio di una società specializzata;
6. conservazione dei file su server localizzato nella sede dell'azienda e sottoposto a costante procedura di backup dei dati.

1.8 - La conservazione digitale dei documenti negli studi professionali

1.8.1 - Esempio 1 - Dichiarazione dei redditi elaborate dallo studio

Lo *Studio Paolo Neri - Dottore Commercialista*, elabora circa 230 dichiarazioni dei redditi ed ha deciso di conservare in solo formato digitale la copia dell'intermediario ad iniziare dalle dichiarazioni dei redditi elaborate nel corso del 2014 (*Unico persone fisiche 2014-Periodo d'imposta 2013)*.

Il responsabile della conservazione è il Dott. Paolo Neri, e la conservazione digitale viene svolta secondo i seguenti principali passaggi:

1. elaborazione *Unico persone fisiche 2014* dei singoli clienti;
2. convocazione dei clienti per consegna modello di versamento F24, con richiesta di sottoscrizione del frontespizio riepilogativo della dichiarazione dei redditi elaborata per presa visione (il frontespizio riepilogativo riporta i dati del contribuente, il soggetto che elabora la dichiarazione, i quadri compilati con i rispettivi importi, le imposte calcolate, etc), oppure richiesta di apposizione di firma grafometrica direttamente sulla dichiarazione redditi tramite apposito tablet;
3. trasmissione delle dichiarazioni entro il 30 settembre 2014 all'Agenzia delle Entrate tramite procedura Entratel;
4. acquisizione dei numeri di protocollo emessi dall'Agenzia delle Entrate e loro associazione alle corrispondenti dichiarazioni dei redditi;
5. produzione del PDF delle singole dichiarazioni dei redditi su modello conforme a quello approvato con apposito provvedimento dall'Agenzia delle Entrate, stampa dell'originale cartaceo da consegnare al cliente previa sottoscrizione[23] dell'intermediario nell'apposito riquadro;

23 L'art.3 comma 9 del DPR 322/98 riporta che *"I contribuenti e i sostituti di imposta che presentano la dichiarazione in via telematica, direttamente o tramite i soggetti di cui ai commi 2-bis e 3, conservano, per il periodo previsto dall'articolo 43 del decreto del Presidente della Repubblica 29 settembre 1973, n. 600, la dichiarazione debitamente sottoscritta e redatta su modello conforme a quello approvato con il provvedimento di cui all'articolo 1, comma 1, nonchè i documenti rilasciati dal soggetto incaricato di predisporre la dichiarazione. L'Amministrazione finanziaria può chiedere l'esibizione della dichiarazione e dei suddetti documenti"*. Va rilevato altresì che con riguardo alla sottoscrizione dell'intermediario, non si ritiene corretta la procedura di firmare tramite l'adozione di sistemi di elaborazione automatica in grado di riportare sulla dichiarazione in modo massivo una scansione della firma oppure la dicitura "F.to + Nome e Cognome".

6. entro i 30 giorni successivi dal termine ultimo di presentazione della dichiarazione, così come previsto dall'art. 3 comma 6 del DPR 322/98, consegna al contribuente dei seguenti documenti:
    a. originale della dichiarazione dei redditi su modello cartaceo conforme a quello approvato dall'Agenzia delle Entrate e sottoscritta dall'intermediario;
    b. impegno alla trasmissione datato e sottoscritto dall'intermediario;
    c. copia della comunicazione dell'Agenzia delle Entrate attestante l'avvenuta ricezione della dichiarazione trasmessa;
7. conservazione da parte dell'intermediario delle copie delle dichiarazioni dei redditi, così come stabilito dall'art. 3 comma 9-bis del DPR 322/98[24], con apposizione su ciascun file PDF delle copie delle dichiarazioni dei redditi su modello conforme a quello approvato dall'Agenzia delle Entrate, della firma digitale del Dott. Paolo Neri congiuntamente ad un riferimento temporale, senza necessità che la copia dell'intermediario riporti la sottoscrizione del contribuente[25];
8. ultimazione della conservazione digitale di tutte le 230 copie delle dichiarazioni dei redditi, tramite apposizione all'indice del pacchetto di archiviazione (SInCRO) della firma digitale del Dott. Paolo Neri congiuntamente ad una marca temporale;
9. conservazione dei file su server localizzato nello studio e sottoposto a periodica procedura di backup dei dati.

24 L'art.3 comma 9-bis del DPR 322/1998 riporta che *"I soggetti incaricati della trasmissione delle dichiarazioni conservano ,anche su supporti informatici ,per il periodo previsto dall'art.43 del DPR 29 settembre 1973 n.600, copia delle dichiarazioni trasmesse, delle quali l'Amministrazione finanziaria può chiedere l'esibizione previa riproduzione su supporto conforme a quello approvato con il provvedimento di cui all'art.1. comma 1"*.

25 Risoluzione 354/E del 8 agosto 2008

1.8.2 - Esempio 2 - Scritture contabili dei clienti

Lo *Studio Rita Verdi - Dottore Commercialista*, elabora circa 160 contabilità ordinarie ed ha deciso di conservare in solo formato digitale dal periodo d'imposta 2013 le scritture contabili dei clienti che hanno aderito a questa nuova modalità di conservazione e che sono 140.

Le scritture contabili che lo studio conserverà in solo formato digitale sono:

- il registro IVA vendite;
- il registro IVA acquisti;
- il libro giornale;
- i mastri contabili.

Il responsabile della conservazione è la Dott.ssa Rita Verdi, la conservazione digitale delle scritture contabili del periodo di imposta 2013 viene svolta secondo i seguenti principali passaggi:

1. tenuta meccanografica delle scritture contabili, con produzione annuale entro il 30 dicembre 2014 di un file PDF per ciascuna scrittura contabile, con produzione di ben 560 file;
2. apposizione su ciascun file PDF della firma digitale della Dott.ssa Rita Verdi e della marca temporale, così come stabilito dall'art.2215/bis del Codice civile;
3. conservazione digitale entro il 30 dicembre 2014 con produzione di un indice del pacchetto di archiviazione (SInCRO) per ciascun cliente (in totale vengono prodotti 140 file SInCRO) ed apposizione della firma digitale della Dott.ssa Rita Verdi congiuntamente ad una marca temporale;
4. conservazione dei file su server localizzato nello studio con periodica procedura di backup dei dati.

CAPITOLO 2

Il regolamento eIDAS

2.1 - Introduzione

Per l'Europa la spinta verso un'economia digitale è da anni una priorità. Per questo motivo nel marzo del 2010 la Commissione europea diede inizio ad un importante piano d'azione di durata decennale *(Europa 2020)*[26] con il chiaro obiettivo di fare uscire dalla crisi un'Europa più forte e di trasformare l'economia europea in un'economia capace di una crescita intelligente (basata sulla conoscenza e sull'innovazione), sostenibile (più verde e più competitiva) ed inclusiva (creare maggiore coesione economica e sociale grazie all'aumento del tasso di occupazione).

A tal proposito venne redatto il documento ***Un'agenda digitale Europea***[27], ed una delle sette iniziative faro che furono individuate per raggiungere i suddetti obiettivi, fu proprio quella di attribuire alla *Information and Communication Technologies* (ICT) un ruolo chiave nel creare in Europa un "unico mercato digitale" per poter cogliere a pieno i tanti benefici che solo un'economica digitale è in grado di produrre. Per dare un'idea del divario che l'Europa aveva accumulato nel settore dell' ICT, la Commissione europea riportava due dati significativi:

- nella lista *Global 500* stilata annualmente dal *Financial Times*[28], delle 13 aziende presenti produttrici di software, solo una era europea;
- nelle liste dei web-site più visitati al mondo[29], nelle prime 50 posizioni era presente 1 solo web-site europeo.

Vi era quindi la necessità di creare un vero e proprio "unico mercato digitale" e questo necessitava di regolamentare nuovi servizi fiduciari per le transazioni elettroniche e fornire un framework per il reciproco riconoscimento giuridico, al fine appunto di:

- consentire alle oltre 21 milioni di imprese europee, di digitalizzare totalmente i processi amministrativi, finanziari, logistici e commerciali, assicurando loro la possibilità di scambiarsi e trasmettere alla pubblica amministrazione in solo formato elettronico documenti quali le fatture, gli ordini di acquisto, i documenti di trasporto, etc.

---

26 Comunicazione della Commissione del 3 marzo 2010, *Europa 2020-Una strategia per una crescita intelligente, sostenibile e inclusiva,* COM (2010) 2020 definitivo

27 Comunicazione della Commissione del 26 agosto 2010, *Un'agenda digitale Europea,* COM (2010) 245 definitivo/2

28 Nella *Global 500* stilata dal *Financial Times* e riferita all'anno 2012, delle 13 aziende presenti produttrici di *Software & computer services,* 7 hanno sede in USA, 3 in India, 1 in Europa, 1 in Giappone, ed 1 ad Hong Kong.

29 Alexa, Google

- consentire agli oltre 500 milioni di cittadini europei di accedere in modo sicuro all'acquisto on-line di beni e servizi (e-Banking, e-Insurance, etc), di accedere ai servizi pubblici in modo più semplice oltre che partecipare in modo più attivo alla vita politica (e-Health, e-Tax, e-Justice, e-Vote, etc), di scambiare in modo sicuro e nel pieno rispetto delle regole soldi ed idee (P2P lending, crowdfunding, file sharing, etc).

La direttiva 1999/93/ (CE) del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche, non era più in grado di svolgere un tale ruolo, era necessario: a) armonizzare a livello europeo l'identificazione elettronica oltre che il valore probatorio dei documenti elettronici firmati elettronicamente, b) introdurre e regolamentare nuovi servizi fiduciari per le transazioni elettroniche, come per esempio il sigillo elettronico, i servizi elettronici di recapito certificato e l'autenticazione dei siti web.

A tal fine, nella Gazzetta ufficiale dell'unione europea del 28 agosto 2014, fu pubblicato il *regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno*, abrogativo della direttiva 1999/93/CE e meglio conosciuto come regolamento eIDAS (**e**lectronic **ID**entification, **A**uthentication, **S**ignature).

2.2 - Il percorso che ha portato al regolamento eIDAS

Il percorso che ha portato la Commissione europea a stilare il regolamento eIDAS, è iniziato almeno 10 anni prima rispetto alla sua pubblicazione, e lo possiamo riassumere nei seguenti passaggi chiave:

OTTOBRE 2003	Redazione da parte di un team di esperti del documento *The legal and market aspects of electronic signatures*[30]. Lo studio, così come contemplato dall'articolo 12 della direttiva 1999/93/CE, doveva fornire un'analisi di come la suddetta direttiva era stata implementata nei vari Stati membri, oltre che fornire una fotografia degli aspetti giuridici inerenti le firme elettroniche nei diversi Stati membri, ed emersero chiaramente criticità e problemi inerenti sia un non perfetto ed omogeneo recepimento della direttiva 1999/93/CE da parte dei vari Stati membri, sia una scarsa interoperabilità delle firme elettroniche a livello nazionale e cross-border.
15 MARZO 2006	Pubblicazione della comunicazione della Commissione *Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures*[31]. Il report, in parte basato sui risultati emersi dallo studio *The legal and market aspects of electronic signatures*, per la prima volta riportava l'esistenza di problemi e lacune inerenti l'impiego in ambito europeo delle firme elettroniche, evidenziando come la scarsa adozione di queste soluzioni sia da attribuire sia ad "aspetti legali" che ad "aspetti tecnologici".
22 NOVEMBRE 2007	Pubblicazione del documento *Study on the standardisation aspects of Signature*[32]. Lo studio, richiesto dalla Commissione europea, doveva evidenziare le carenze e le criticità riguardanti i diversi standard usati nel campo delle firme elettroniche, e fornire possibili soluzioni ed interventi migliorativi in caso di revisioni normative, ed anche in questo studio emersero l'assenza di servizi fiduciari basati sull'impiego delle firme elettroniche.

30 *The legal and market aspects of electronic signatures*, October 2003

31 Commission Communication of 15 March 2006, *Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures*, COM (2006) 120 final.

32 *Study on the standardisation aspects of eSignature*, 2007

28 NOVEMBRE 2008	Redazione della comunicazione della Commissione *Piano d'azione in materia di firma e di identificazione elettroniche destinato ad agevolare la prestazione di servizi pubblici transfrontalieri nel mercato unico*[33], ove veniva evidenziata la presenza di problemi in grado di inibire la interoperabilità legale e tecnica, e venivano proposte delle azioni per migliorare la interoperabilità cross-border delle firme elettroniche e dell'identificazione elettronica.
22 DICEMBRE 2009	Redazione da parte della Commissione europea del *Mandate 460*[34], ove veniva dato mandato ai tre organismi europei di standardizzazione (CEN, ETSI, e CENELEC), il compito di stilare un documento avente lo scopo di creare le condizioni per raggiungere una piena interoperabilità delle firme elettroniche a livello europeo, definendo un framework di standardizzazione delle firme elettroniche.
3 MARZO 2010	Redazione della comunicazione della Commissione *Europa 2020*, ove veniva individuata una strategia che consentisse all'Europa di uscire dalla crisi economica e prepararla alle sfide derivanti dalla globalizzazione dei mercati oltre che dai cambiamenti sociali. Vengono individuate tre importanti priorità: - *Crescita intelligente*, cioè sviluppare una economia basata sulla conoscenza e sulla innovazione; - *Crescita sostenibile*, cioè promuovere una economia più verde e più competitiva: - *Crescita inclusiva*, cioè sviluppare una economia con alti tassi di occupazione. Al fine di raggiungere le suddette priorità, vengono definite 7 "iniziative faro": - *L'Unione dell'innovazione* - *Youth on the move* - *Un'agenda Europea del digitale* - *Un'Europa efficiente sotto il profilo delle risorse* - *Una politica industriale per l'era della globalizzazione* - *Un'agenda per nuove competenze e nuovi posti di lavoro* - *Piattaforma Europea contro la povertà.* Nell'iniziativa *Un'agenda Europea del digitale*, venivano poi individuati gli obiettivi da raggiungere e che porteranno ad avviare una proposta di revisione della directive 1999/93/EC.

33 Comunicazione della Commissione del 28 novembre 2008, *Piano d'azione in materia di firma e di identificazione elettroniche destinato ad agevolare la prestazione di servizi pubblici transfrontalieri nel mercato unico*, COM (2008) 798 definitivo

34 M460 of 22 December 2009, *Standardisation mandate to the European standardisation organisations CEN, CENELEC, and ETSI in the field of information and communication technologies applied to electronic signatures*.

31 LUGLIO 2010	Pubblicazione del documento *Study on Cross-Border interoperability of eSignatures (CROBIES)*[35], dove venivano riportati i problemi, le criticità e gli ostacoli sia legali che di standard, esistenti nell'uso delle firme elettroniche in un contesto cross-border.
26 AGOSTO 2010	Redazione della comunicazione della Commissione **Un'agenda digitale Europea** (una delle 7 iniziative faro contenute nella Europe 2020), e dove veniva testualmente riportato che *"Lo scopo generale dell'agenda digitale europea è ottenere vantaggi socioeconomici sostenibili grazie a un mercato digitale unico basato su Internet veloce e superveloce e su applicazioni interoperabili"*.
2 DICEMBRE 2010	Redazione della comunicazione della Commissione *Sfruttare i vantaggi della fatturazione elettronica in Europa*[36], dove venivano evidenziati i tanti vantaggi e benefici economici derivanti dall'uso della fattura elettronica, e dichiarato chiaramente che *"La Commissione desidera che entro il 2020 la fatturazione elettronica diventi il principale modo di fatturazione in Europa"* e per questo motivo veniva dichiarato che *"La Commissione proporrà nel 2011 una revisione della direttiva 1999/93/CE sulle firme elettroniche al fine di fornire un quadro giuridico per il riconoscimento transfrontaliero e l'interoperabilità dei sistemi di autenticazione elettronica"*.
18 FEBBRAIO 2011	Avvio della *Public consultation on electronic identification, authentication, and signatures in the European digital single market*, che durerà fino al 15 aprile 2011 e nel corso della quale vennero raccolti ben 434 contributi.

35 *Study on Cross-Border interoperability of eSignatures*, 31st July 2010

36 Comunicazione della Commissione del 2 dicembre 2010, *Sfruttare i vantaggi della fatturazione elettronica in Europa*, COM (2010) 712 definitivo

13 APRILE 2011	Redazione della comunicazione della Commissione *L'atto per il mercato unico*[37], ove la Commissione identificava 12 leve da attivare per stimolare la crescita e rafforzare la fiducia, ribadendo come azione chiave la necessità di avere una *"Legislazione che garantisca il mutuo riconoscimento dell'identificazione e autenticazione elettronica in tutta l'UE, nonché una revisione della direttiva sulla firma elettronica, per consentire che le imprese, i cittadini e le amministrazioni pubbliche interagiscano per via elettronica in maniera sicura e senza ostacoli, a vantaggio dell'efficacia dei servizi e degli appalti pubblici, della prestazione di servizi e del commercio elettronico, anche nella loro dimensione transfrontaliera".*
12 AGOSTO 2011	Pubblicazione del documento *Overview of responses* riguardante la *Public consultation on electronic identification, authentication, and signatures in the European digital single market*, e contenente i 434 contributi raccolti dal 18 febbraio 2011 al 15 aprile 2011.
12 OTTOBRE 2011	Redazione della comunicazione della Commissione *A roadmap to stability and growth*[38], ove la Commissione nel riaffermare l'importanza dell'Euro e la necessità da parte degli Stati membri di raggiungere una stabilità finanziaria, ribadiva la necessità di *"Providing a common legal base for mutual recognition of e-authentication and electronic signature across borders"*.
4 GIUGNO 2012	Redazione della proposta del regolamento ***eIDAS services*** e del relativo *Impact assessment*[39].
28 AGOSTO 2014	Pubblicazione nella Gazzetta ufficiale dell'Unione Europea del *regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE*.

37 Comunicazione della Commissione del 13 aprile 2011, *L'atto per il mercato unico - Dodici leve per stimolare la crescita e rafforzare la fiducia - "Insieme per una nuova crescita"*, COM (2011) 206 definitivo

38 Commission Communication of 12 October 2011, *A roadmap to stability and growth*, COM (2011) 669 final

39 4th June 2012, *Commission staff working paper impact assessment-Accompanying the proposal for a regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market*, SWD (2012) 135 final

2.3 - Regolamento, atti di esecuzione ed atti delegati

► Regolamento e non direttiva

Lo strumento legislativo scelto per intervenire a correggere la direttiva 1999/93/CE, non è stato quello di stilare una nuova direttiva che poi i diversi Stati membri avrebbero dovuto recepire, lasciando loro la libertà di scegliere in merito alla forma ed ai mezzi, così come stabilisce l'art. 288 terzo comma del *Trattato sul Funzionamento dell'Unione Europea* (TFUE). La modalità che si è invece preferito scegliere, è stata quella di stilare un regolamento, caratterizzato da una immediata applicazione in tutti gli Stati membri e quindi utile ad introdurre una maggiore armonizzazione tra gli stessi, così come stabilito dall'art. 288 secondo comma del TFUE, secondo comma, ove testualmente riporta che *"Il regolamento ha portata generale. Esso è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri".*

Si è in sostanza evitato il ripetersi del medesimo errore già fatto in passato con la direttiva 1999/93/CE, ove il demandare ai vari Stati membri il recepimento della direttiva, avrebbe potuto comportare il rischio di fraintendimenti nei vocaboli da impiegare oltre che possibili "personalizzazioni", e quindi il ripetersi di problemi e criticità nel conseguire un reciproco riconoscimento dei servizi fiduciari ed una interoperabilità cross-border.

Con riguardo poi alla collocazione del regolamento comunitario nel sistema delle fonti del diritto nazionale, con sentenza 5 giugno 1984 n.170 la Corte Costituzionale ha chiaramente stabilito che il legislatore nazionale non deve intervenire a disciplinare materie già trattate nel regolamento comunitario, ed in caso di conflitto sono i regolamenti a prevalere. Questo aspetto è certamente importante, perché, come vedremo, il regolamento eIDAS interviene a disciplinare materie che in passato sono già state regolamentate dal legislatore nazionale, e quindi in caso di conflitto sono sempre i regolamenti comunitari a prevalere.

► Atti di esecuzione

Il regolamento eIDAS contiene diversi rimandi alla successiva redazione degli atti di esecuzione, così come contemplato nel *Trattato di Lisbona*, e la cui procedura è contenuta nell'art. 291 del *Trattato sul Funzionamento dell'Unione Europea*.

Figura 14. ***Atti di esecuzione pubblicati in ambito eIDAS***

Ambito di applicazione	Contenuto	Riferimento	Data
Identificazione elettronica	Modalità procedurali per la cooperazione tra Stati membri in materia di identificazione elettronica	2015/296	24.02.2015
	Quadro di interoperabilità in materia di identificazione elettronica e servizi fiduciari	2015/1501	08.09.2015
	Definizione delle specifiche e procedure tecniche minime riguardanti i livelli di garanzia per i mezzi di identificazione elettronica	2015/1502	08.09.2015
	Formati e procedure della notifica in materia di identificazione elettronica e servizi fiduciari	2015/1984	03.11.2015
Servizi fiduciari	Specifiche relative alla forma del marchio di fiducia UE per i servizi fiduciari qualificati	2015/806	22.05.2015
	Specifiche tecniche e formati relativi agli elenchi di fiducia	2015/1505	08.09.2015
	Specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati	2015/1506	08.09.2015
	Norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificato	2016/650	25.04.2016

► Atti delegati

Il regolamento eIDAS contiene diversi rimandi alla successiva redazione degli atti delegati, anch'essi introdotti con il *Trattato di Lisbona*, e la cui procedura è contenuta nell'art. 290 del *Trattato sul Funzionamento dell'Unione Europea*, ed è caratterizzata dai seguenti aspetti:

- è necessario definire gli obiettivi, il contenuto, la portata e la durata degli atti delegati;
- il Parlamento europeo o il Consiglio possono decidere di revocare la delega;
- il Parlamento europeo o il Consiglio possono decidere di sollevare obiezioni.

2.4 - Ambito di applicazione e contenuti

Analizzando nei contenuti il regolamento eIDAS, vanno rilevati alcuni importanti aspetti, ed in particolare:

- Il regolamento eIDAS è direttamente applicabile in ciascuno degli Stati membri a decorrere dal 1° luglio 2016.
- Il regolamento eIDAS è ispirato ad un principio di "neutralità tecnologica", utile ad evitare continui aggiornamenti e difformità negli effetti giuridici in caso di impiego di servizi basati su nuove tecnologie ad oggi non ancora presenti sul mercato.
- Il regolamento eIDAS interviene a regolamentare nei diversi Stati membri l'identificazione elettronica, gli effetti giuridici dei documenti elettronici, oltre a disciplinare 5 servizi fiduciari: le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i servizi elettronici di recapito certificato e l'autenticazione dei siti web.
- E' compito degli Stati membri definire gli effetti giuridici delle firme elettroniche, fatto salvo però quanto contenuto nell'art. 25 secondo comma del regolamento eIDAS, secondo il quale *"Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa".*
- E' sempre possibile per gli Stati membri mantenere o introdurre disposizioni nazionali in materie di servizi fiduciari, nella misura però che i suddetti servizi non siano compiutamente armonizzati dal regolamento eIDAS.
- E' necessario che gli Stati membri armonizzino le disposizioni interne al regolamento eIDAS, e con riguardo all'Italia, così come previsto dall'art.1 della legge 7 agosto 2015 n.124, il Governo è delegato ad adottare uno o più decreti legislativi volti a modificare ed integrare il decreto legislativo 7 marzo 2005 n.82 (codice dell'amministrazione digitale – CAD) al fine di *"adeguare il testo delle disposizioni vigenti alle disposizioni adottate a livello europeo"*.

2.5 - Identificazione elettronica e SPID

La prima parte del regolamento eIDAS è incentrata a disciplinare l'**identificazione elettronica**, definita all'art.3 primo comma punto 1) 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"*.

Una volta che quindi gli Stati membri avranno notificato i propri regimi di identificazione elettronica, grazie al reciproco riconoscimento dei mezzi di identificazione elettronica, cioè dei dati in grado di stabilire l'identità di una persona fisica o giuridica, sarà possibile per esempio per un cittadino italiano accedere ai servizi online forniti dalla pubblica amministrazione di un diverso Stato membro.
Il regolamento eIDAS prevede 3 livelli di garanzia con riguardo ai regimi di identificazione elettronica, ed in particolare prevede un primo livello in grado di fornire un grado di sicurezza limitato, un secondo livello in grado di fornire un grado di sicurezza significativo, ed un terzo livello in grado di fornire un grado di sicurezza più elevato.

Così come previsto sia dal regolamento eIDAS che dall'art.64 del CAD, con il DPCM 24 ottobre 2014 pubblicato in GU il 9 dicembre 2014, veniva avviato in Italia il sistema pubblico per la gestione dell'identità digitale, meglio conosciuto come SPID, consentendo in questo modo ai cittadini ed alle imprese di poter accedere con un'unica identità digitale ai servizi online offerti dalla pubblica amministrazione oppure da tutte quelle organizzazioni che intendono gestire in modo semplice e veloce l'autenticazione elettronica dei propri utenti.

Ad oggi i gestori dell'identità digitale sono tre e sono InfoCert SpA, Poste Italiane SpA e Telecom Italia Trust Technologies Srl (da settembre 2016, come da comunicato stampa dell'AgID, saranno attivi anche Aruba PEC Spa e Sielte Spa), mentre le pubbliche amministrazioni a cui è possibile accedere tramite SPID sono circa 300 tra cui l'Agenzia delle Entrate, INPS, INAIL, Equitalia, Unioncamere, diverse Camere di Commercio, sei Regioni (Piemonte, Emilia Romagna, Friuli Venezia Giulia, Liguria, Toscana e Marche), diversi comuni (Arezzo, Venezia, Modena, Reggio Emilia, Pisa, Prato), ed altre PA tra cui Università di Torino, Università La Sapienza di Roma, AUSL di Piacenza, AUSL di Bologna, AUSL di Modena, AUSL di Reggio Emilia, AUSL di Parma, AUSL di Ferrara, AUSL di Rimini.

Con la pubblicazione da parte dell'Agenzia per l'Italia Digitale (AgID) del *regolamento recante le modalità attuative per la realizzazione dello SPID*, i livelli di sicurezza delle identità digitali previsti nel nostro paese sono tre, crescenti in termini di sicurezza informatica. In base alla tipologia di servizi a cui si intende accedere potrà essere richiesto un livello basso di autenticazione informatica (livello 1), un livello medio (livello 2), oppure un livello alto (livello 3).

- **SPID di livello 1**

Il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica ad un solo fattore, che solitamente viene effettuato richiedendo all'utente *"nome utente"* e *"password"*, e con riguardo a quest'ultima si richiede di adottare alcune regole, tra le quali:
- lunghezza minima di 8 caratteri
- uso dei caratteri maiuscolo e minuscolo
- inclusione di uno o più caratteri numerici
- validità massima non superiore a 180 giorni

- **SPID di livello 2**

Il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica a due fattori non necessariamente basati su certificati digitali, e solitamente viene effettuato richiedendo all'utente oltre il *"nome utente"* e *"password"* anche l'inserimento di un OTP (One Time Password) inviato via SMS;

- **SPID di livello 3**

Il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica a due fattori basati su certificati digitali custoditi su dispositivi sicuri di firma digitale.

Il rilascio e la gestione dell'identità digitale SPID eseguita dai gestori dell'identità digitale, si articola nei seguenti 5 principali passaggi:

1. **Richiesta dell'identità digitale**, ove il richiedente presenta apposita domanda congiuntamente ad una serie di informazioni a secondo se trattasi di persona fisica (e.g. nome, cognome, sesso, data e luogo di nascita, codice fiscale, estremi di un documento

di identità, etc) oppure persona giuridica (denominazione/ragione sociale, codice fiscale o partita IVA, sede legale, visura camerale, etc);

2. **Identificazione del richiedente**, ove il gestore dell'identità digitale, dopo aver ricevuto la richiesta, provvede all'identificazione del soggetto richiedente tramite i documenti dallo stesso forniti. L'identificazione del soggetto richiedente, potrà svolgersi "de visu" con il richiedente che si reca personalmente presso un luogo prestabilito, oppure "da remoto" tramite strumenti di registrazione audio/video, rilevando che le immagini video devono essere a colori, l'audio deve essere chiaramente udibile e non devono essere presenti elementi di disturbo. E' contemplata altresì una identificazione informatica tramite firma digitale, ed in questo caso il soggetto richiedente dovrà trasmettere la richiesta sottoscritta con firma digitale;
3. **Esame e verifica dell'identità del richiedente**, che consiste nel verificare l'attendibilità delle informazioni e dei documenti raccolti in fase di identificazione;
4. **Conservazione e registrazione dei documenti**, che consiste nel conservare i riscontri e le prove inerenti i processi di identificazione eseguiti sia tramite identificazione "de visu" che "da remoto";
5. **Emissione e consegna dell'identità digitale**, ove il gestore rilascia l'identità digitale al richiedente, ed a secondo del livello di SPID possono essere previste diverse modalità di rilascio, come l'impiego della PEC o della posta raccomandata nei casi di livelli di sicurezza bassi (e.g. 1° livello di SPID), oppure altre modalità nei casi di livelli di sicurezza alti (e.g. 3° livello di SPID).

Figura 15. ***Principali caratteristiche dei gestori SPID***

Gestore SPID	Fattori di autenticazione			Modalità di riconoscimento				Costo annuale
	SPID di livello 1	SPID di livello 2	SPID di livello 3	Di persona	Webcam	CIE CNS	Firma digitale	
InfoCert	Username e password	Username e password + OTP su SMS --- OTP su App iOS --- OTP su App Android	-	SI	SI	SI	SI	Gratuito sino al 31/12/2016 (durata 2 anni)
Poste Italiane	Username e password	Username e password + OTP su SMS --- App iOS --- App Android	-	SI	-	SI	SI	
Telecom Italia	Username e password	Username e password + OTP su SMS	-	-	-	SI	SI	

2.6 - I servizi fiduciari

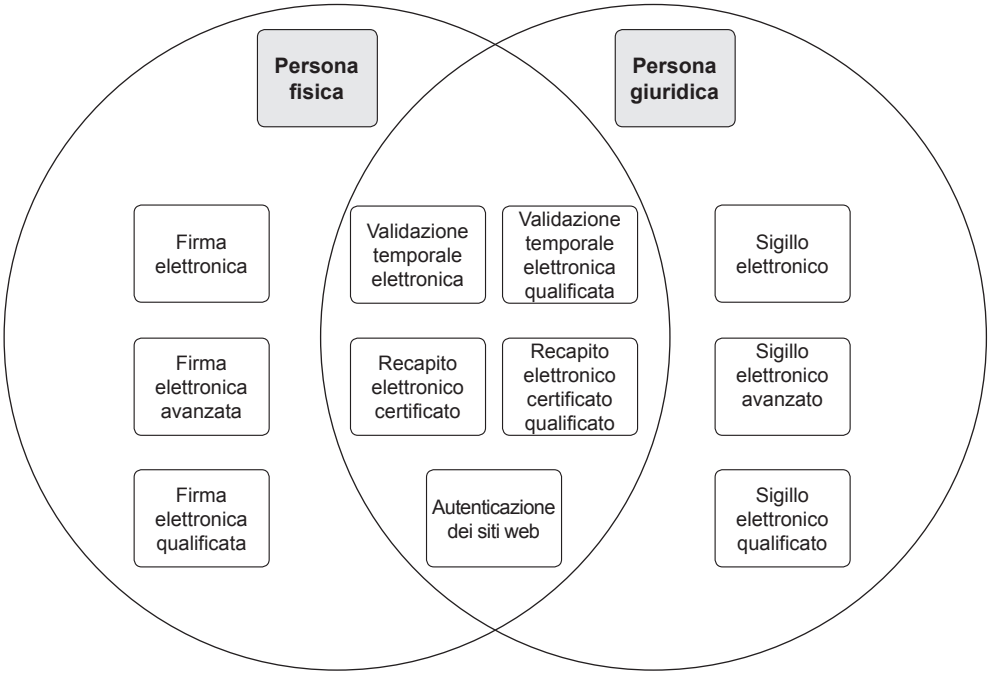
La seconda parte del regolamento eIDAS interviene a regolamentare 5 servizi fiduciari, ed in particolare le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i servizi elettronici di recapito certificato e l'autenticazione dei siti web.

I suddetti servizi fiduciari, alcuni dei quali erano già regolamentati in ambito italiano, potranno essere forniti da prestatori di servizi fiduciari qualificati, vigilati dall'Organismo di vigilanza dello Stato membro che per l'Italia è l'AgID, oppure da prestatori di servizi fiduciari non qualificati. La distinzione è certamente importante in termini di responsabilità ed onere della prova in caso di danni, dato che il dolo o la negligenza si presume in capo al prestatore di servizio fiduciario qualificato (salvo che questo dimostri che il danno si è verificato senza suo dolo o negligenza), mentre in caso di prestatore di servizio fiduciario non qualificato l'onere di dimostrare che il dolo o la negligenza è del prestatore ricade sulla persona fisica o giuridica che ha subito il danno.
Diventare prestatori di servizi fiduciari qualificati comporta una serie di adempimenti ed

oneri, non ultimo sottoporsi a proprie spese almeno ogni 24 mesi ad una verifica da parte di un organismo di valutazione della conformità, al fine di verificare la bontà dei servizi fiduciari prestati.

I servizi fiduciari disciplinati dal regolamento eIDAS, alcuni dei quali, lo ricordo nuovamente, erano già disciplinati nell'ordinamento giuridico Italiano, possono essere suddivisi in servizi fiduciari fruibili da parte delle sole persone fisiche (firme elettroniche), fruibili da parte delle sole persone giuridiche (sigilli elettronici), fruibili da parte di entrambi (le validazioni temporali elettroniche, i servizi elettronici di recapito certificato e l'autenticazione dei siti web).

Figura 16. ***Servizi fiduciari per tipologia di utilizzatori***



Va altresì rilevato che i prestatori di servizi fiduciari qualificati possono utilizzare il marchio di fiducia UE per presentare in modo riconoscibile e chiaro i servizi fiduciari qualificati da essi prestati.

Figura 17. ***Marchio di fiducia UE***

► Firme elettroniche

L'art.3 primo comma punto 9) del regolamento eIDAS, definisce "firmatario", una *"persona fisica che crea una firma elettronica"*, mentre al successivo punto 10) definisce "firma elettronica" *"dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare"*.

Oltre alla firma elettronica, il regolamento eIDAS interviene a definire anche le firme elettroniche avanzate e le firme elettroniche qualificate, definendo queste ultime come *"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 primo comma punto 12).

Con riferimento alle firme elettroniche, il regolamento eIDAS introduce importanti principi base:

- le firme elettroniche sono utilizzate esclusivamente da persone fisiche;
- le firme elettroniche servono "per firmare", inteso come prova che il firmatario ha approvato il contenuto di un determinato documento, oppure come espressione di un intento o di un

consenso, e quindi un loro impiego in processi in cui dovessero servire per garantirne per esempio l'autenticità e l'integrità dei dati, sarebbe un utilizzo improprio, tranne situazioni particolari come l'impiego della firma digitale nei processi di fatturazione elettronica ad opera di persone fisiche dato la loro impossibilità ad impiegare il sigillo digitale;

- le firme elettroniche qualificate (i.e. le firme digitali) hanno *"effetti giuridici equivalenti a quelli di una firma autografa"*(art.25 secondo comma), introducendo in questo modo in tutti gli Stati membri un preciso obbligo di accettazione e di reciproco riconoscimento;
- le firme elettroniche qualificate (i.e. le firme digitali), al fine di *"estendere l'affidabilità della firma elettronica qualificata oltre il periodo di validità tecnologica"* hanno necessità di essere sottoposte ad un servizio di conservazione qualificato (art.34), rilevando però che il suddetto servizio non deve essere confuso con il servizio di conservazione digitale dei documenti informatici da anni presente in Italia (che peraltro il regolamento eIDAS non interviene a disciplinare), in quanto si tratta di un servizio di conservazione qualificato atto a preservare l'affidabilità (non quindi la validità) delle firme elettroniche qualificate;
- a norma dell'art.51 secondo comma del regolamento eIDAS, *"I certificati qualificati rilasciati a persone fisiche a norma della direttiva 1999/93/CE sono considerati certificati qualificati di firma elettronica a norma del presente regolamento fino alla loro scadenza"*, e quindi coloro che alla data del 1° luglio 2016 sono in possesso di una firma digitale, potranno continuare ad utilizzarla fino alla scadenza del relativo certificato qualificato;

► Sigilli elettronici

Il servizio fiduciario che certamente presenta aspetti interessanti oltre che essere nuovo per il nostro ordinamento giuridico, è il sigillo elettronico, dato che da tempo vi era l'esigenza di uno strumento simile al "sigillo" che nel medioevo veniva apposto alle lettere che fidati corrieri a cavallo consegnavano nelle mani del destinatario. In quell'epoca il sigillo era ottenuto mediante l'impressione di un modello (e.g. timbro, anello, etc) su un materiale morbido che si induriva rapidamente (e.g. cera riscaldata, piombo fuso, argilla bagnata, etc) e consentiva al destinatario di avere la garanzia sia sulla provenienza della lettera (autenticità dell'origine), sia che la lettera non era stata alterata o modificata (integrità del contenuto).

L'art.3 primo comma punto 24) del regolamento eIDAS, definisce "creatore di un sigillo", una *"persona giuridica che crea un sigillo elettronico"*, mentre al successivo punto 25) definisce

“sigillo elettronico” “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”.

Oltre al sigillo elettronico, il regolamento eIDAS interviene a definire anche il sigillo elettronico avanzato ed il sigillo elettronico qualificato, definendo quest’ultimo come *“un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici”* (art.3 primo comma punto 27) .

Anche con riferimento ai sigilli elettronici, il regolamento eIDAS introduce importanti principi base:

- i sigilli elettronici sono utilizzati esclusivamente da persone giuridiche;
- i sigilli elettronici servono per garantire l’autenticità e l’integrità dei dati trasmessi, e ciò porta a ritenere siano stati pensati proprio per le fatture elettroniche, ove l’art.21 terzo comma del DPR 633/72 contempla che *“il soggetto passivo assicura l’autenticità dell’origine, l’integrità del contenuto e la leggibilità della fattura dal momento della sua emissione fino al termine del suo periodo di conservazione”*. Ma naturalmente il sigillo elettronico potrà essere impiegato in altri contesti, come per esempio attestare la provenienza e l’integrità del file trasmesso o scaricato da un sito web (e.g. software, file audio, file video, antivirus, etc), oppure se associato ad uno scanner o ad una macchina fotografica o ad uno smartphone attestare l’autenticità e l’integrità dell’immagine scansionata o della fotografia scattata, oppure congiuntamente ad una marca temporale attestare l’esistenza in capo ad una certa società e ad una certa data di un particolare documento informatico (e.g. progetto, disegno, idea di brevetto, invenzione), etc;
- i sigilli elettronici qualificati (i.e. sigilli digitali) godono della *“presunzione di integrità dei dati e di correttezza dell’origine di quei dati a cui il sigillo elettronico qualificato è associato”* (art.35 secondo comma). Questo nei processi di fatturazione elettronica è certamente un aspetto rilevante da considerare, e che dovrebbe indurre le persone giuridiche ad impiegare il sigillo digitale anziché la firma digitale;
- i sigilli elettronici qualificati (i.e. sigilli digitali) sono creati tramite appositi dispositivi e, diversamente dalle firme elettroniche qualificate ove il dispositivo deve essere utilizzato sotto l’ *”esclusivo controllo”* del firmatario, con i sigilli elettronici qualificati il dispositivo deve essere utilizzato sotto il *“controllo”* della persona giuridica, consentendo una maggiore flessibilità nella custodia ed attivazione del dispositivo all’interno dell’organizzazione;
- i sigilli elettronici qualificati (i.e. sigilli digitali), così come già visto per le firme elettroniche

qualificate, al fine di *"estendere l'affidabilità del sigillo elettronico qualificato oltre il periodo di validità tecnologica"* hanno necessità di essere sottoposti ad un servizio di conservazione qualificato (art.40).

► Validazione temporale elettronica

L'art.3 primo comma punto 33) del regolamento eIDAS, definisce "validazione temporale elettronica", *"dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento"* e, oltre alla validazione temporale elettronica, il regolamento eIDAS contempla anche la validazione temporale elettronica qualificata, prevedendo che *"gode della presunzione di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali tale data e ora sono associate"* (art.41 secondo comma).

Una validazione temporale elettronica qualificata è, per esempio, la marca temporale che da tempo utilizziamo nei processi di conservazione digitale oppure in altri contesti al fine di provare che un determinato documento informatico esisteva ad una certa data, oltre che certificarne la sua integrità.

► Sevizi elettronici di recapito certificato

L'art.3 primo comma punto 36) del regolamento eIDAS, definisce "servizio elettronico di recapito certificato", *"un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate"*, ed oltre al servizio elettronico di recapito certificato il regolamento eIDAS contempla anche il servizio elettronico di recapito certificato qualificato, prevedendo che gode della *"presunzione di integrità dei dati, dell'invio di tali dati da parte del mittente identificato, della loro ricezione da parte del destinatario identificato e di accuratezza della data e dell'ora dell'invio e della ricezione indicate dal servizio elettronico di recapito certificato qualificato"* (art.43 secondo comma).

Diversamente da quanto si possa pensare, ad oggi la PEC non è ritenuta un servizio elettronico di recapito certificato qualificato, dato che non vi è l'assoluta certezza nell'identificazione del mittente, e quindi nei prossimi anni ci potrebbe essere un'evoluzione dell'attuale servizio PEC.

► Autenticazione dei siti web

L'art.3 primo comma punto 38) del regolamento eIDAS, definisce "certificato di autenticazione di sito web", *"un attestato che consente di autenticare un sito web e collega il sito alla persona fisica o giuridica a cui il certificato è rilasciato"*.

Il suddetto servizio fiduciario quindi, consente all'utente che intende usufruire di taluni servizi online oppure acquistare dei prodotti via web, di avere la certezza della persona fisica o giuridica titolare del sito web.

Figura 18. ***Overview dei servizi fiduciari***

Principali caratteristiche	Firma elettronica			Sigillo elettronico			Validazione temporale		Recapito elettronico		Autenticaz. sito web
	FE	FEA	FEQ	SE	SEA	SEQ	VTE	VTEQ	REC	RECQ	ASWQ
Usato dalle persone fisiche per firmare	●	●	●								
Effetti giuridici equivalenti alla firma autografa			●								
Usato dalle persone giuridiche per garantire l'origine e l'integrità				●	●	●					
Presunzione di correttezza dell'origine ed integrità dati						●					
Usato per collegare i dati ad una particolare ora e data							●	●			
Presunzione di accuratezza della data e dell'ora e di integrità dati								●			
Usato per provare l'avvenuto invio e l'avvenuta ricezione									●	●	
Presunzione di integrità dei dati, di invio da parte del mittente, di ricezione da parte del destinatario e di accuratezza data ed ora										●	
Usato dalle persone fisiche e giuridiche per autenticare un sito web											●

2.7 - I documenti elettronici

L'art.3 primo comma punto 35) del regolamento eIDAS, definisce "documento elettronico", *"qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva"*, mentre l'art. 46 riporta testualmente che *"A un documento elettronico non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica"*.

Un aspetto da rilevare è che, nel tradurre in lingua italiana la definizione di documento elettronico contenuta nel regolamento eIDAS, è stato erroneamente utilizzato il termine "conservato" anziché "memorizzato", ed infatti mentre nella versione originale in lingua inglese veniva correttamente impiegato il termine "stored", cioè memorizzato, nella versione in italiano veniva erroneamente utilizzato il termine conservato, che tradotto sarebbe "preserved".

La differenza non è di poco conto, se si pensa che un documento elettronico memorizzato è per esempio una semplice email oppure un PDF, mentre un documento elettronico conservato è quando la email oppure il documento PDF sono stati sottoposti al processo di conservazione digitale secondo le attuali disposizioni normative italiane in tema di sistemi di conservazione.
Premesso quindi che il termine corretto da impiegare dovrebbe essere "memorizzato" anziché "conservato", anche perché coerente con la definizione di documento informatico presente da anni nell'ordinamento giuridico del nostro Paese, per avere una eventuale definitiva conferma si dovrà attendere la pubblicazione del decreto legislativo che, così come previsto dall'art.1 della legge 7 agosto 2015 n.124, il Governo è delegato ad emanare al fine di modificare ed integrare il decreto legislativo 7 marzo 2005 n.82 (codice dell'amministrazione digitale – CAD) ed utile ad *"adeguare il testo delle disposizioni vigenti alle disposizioni adottate a livello europeo"*.

CAPITOLO 3

La digitalizzazione dei DDT nelle imprese e nella PA

3.1 - Il documento di trasporto

Istituito con il DPR 14 agosto 1996 n.472, dal 27 settembre 1996 il documento di trasporto (DDT) ha sostituito la bolla di accompagnamento nei processi di fatturazione differita, ed i contenuti minimi richiesti sono: *"indicazione della data, delle generalità del cedente, del cessionario e dell'eventuale incaricato del trasporto, nonché la descrizione della natura, della qualità e della quantità dei beni ceduti"*.

In un processo di digitalizzazione dei DDT eseguito nell'ambito di imprese o della pubblica amministrazione, è utile rammentare alcuni importanti aspetti:

► Il DDT è un documento rilevante ai fini fiscali

Il DDT è un documento rilevante ai fini fiscali e così come stabilito dall'articolo 1 terzo comma del DPR 472/96, *"Per la conservazione di tale documento si applicano le disposizioni di cui all'art. 39, terzo comma, del decreto del Presidente della Repubblica 26 ottobre 1972, n. 633"*, il che significa che in caso di conservazione digitale si dovranno rispettare le norme di cui al DMEF 17 giugno 2014 e DPCM 3 dicembre 2013;

► Il DDT può non essere sul mezzo durante la consegna della merce e può essere trasmesso telematicamente

Il DDT non deve obbligatoriamente essere sul mezzo del vettore durante la consegna della merce dato che può anche essere trasmesso telematicamente tramite per esempio PEC, email oppure sistemi EDI, ed in questi casi, così come contemplato dalla circolare del Ministero delle Finanze del 11 ottobre 1996 n.249, i DDT devono *"essere spediti nel giorno in cui è iniziato il trasporto dei beni"*;

► Il DDT può essere un documento informatico elaborabile

In caso di trasmissione telematica, il DDT può anche essere in un formato strutturato e quindi elaborabile dai sistemi informativi, per esempio in formato XML oppure TXT, dato che la circolare del Ministero delle Finanze del 16 settembre 1996 n. 225, specifica che il DDT deve essere emesso *"prima dell'inizio del trasporto o della consegna, a cura del cedente, secondo le normali esigenze aziendali, in forma libera (senza, cioè, vincoli di forma, di dimensioni o di tracciato)"*.

In sostanza quindi il DDT, oltre che essere emesso in formato digitale, può anche essere emesso in formato strutturato senza vincoli di "tracciato" e quindi secondo lo standard UBL[40], oppure EDIFACT.

In caso di trasmissione telematica del DDT, è quindi necessario tener presente che va emesso *"prima dell'inizio del trasporto o della consegna"*, nel senso che il documento informatico deve avere le caratteristiche di immodificabilità ed integrità richieste dalle regole tecniche prima dell'inizio del trasporto o della consegna, apponendo per esempio una firma digitale, dopodichè dovrà essere trasmesso telematicamente entro il giorno in cui è iniziato il trasporto dei beni;

► Il DDT può essere sostituito dal DesAdv

Il DDT può anche essere sostituito da un altro documento, come per esempio l'avviso di spedizione merce, meglio conosciuto come "despatch advice" (DesAdv), dato che in tema di fatturazione differita, l'art.21 quarto comma del DPR 633/72 contempla la possibilità di impiegare, oltre al documento di traporto, anche *"altro documento idoneo a identificare i soggetti tra i quali è effettuata l'operazione ed avente le caratteristiche determinate con decreto del Presidente della Repubblica 14 agosto 1996, n. 472"*. In buona sostanza, anziché trasmettere telematicamente il DDT entro il giorno in cui è iniziato il trasporto dei beni, è possibile trasmettere alcuni giorni prima il DesAdv, il quale, oltre ad avvertire l'acquirente sulla merce in arrivo, potrà sostituire il DDT purché riporti le medesime informazioni;

► Il DDT può non essere firmato dal cliente

Non vi è alcun obbligo fiscale di richiedere all'acquirente di apporre la propria firma sul DDT, sia essa una firma autografa, una firma grafometrica oppure una firma digitale, ed infatti la circolare n.36/E del 6 dicembre 2006 riporta che *"Dal momento che il documento di trasporto è completo di ogni elemento obbligatorio sin dall'origine, senza che né il soggetto emittente né i successivi soggetti riceventi siano tenuti ad eseguire sul d.d.t. ulteriori annotazioni, deve ritenersi ammissibile l'emissione del d.d.t. sotto forma di documento informatico"*.

Diversamente, se per esempio il fornitore ha l'esigenza di richiedere all'acquirente l'apposizione di una firma utile a comprovare sia l'avvenuta consegna della merce che la conformità della stessa all'ordine, è sempre possibile impiegare nuove soluzioni quali la firma grafometrica, oppure altre forme di firme elettroniche;

40 Universal Business Language

► Il DDT può non contenere le note di rettifica

In caso di ritiro parziale dei beni, la risoluzione del Ministero delle Finanze n.2426 del 18 giugno 1994 prevede che il destinatario debba annotare sul suo esemplare di DDT *"i quantitativi di beni o di colli parzialmente ritirati"*, dopodichè la fotocopia del suddetto DDT scorterà i beni nel tragitto di ritorno, al fine di poter emettere, entro il giorno 15 del mese successivo, una corretta fattura differita comprendente le suddette rettifiche a seguito del parziale ritiro dei colli.

In un contesto totalmente digitale, la suddetta attività potrà essere certamente semplificata, tramite per esempio l'ausilio di tablet/palmari da impiegare nel rettificare il DDT, oppure più speditamente impiegando l'avviso di ricezione merce, conosciuto anche come "receiving advice" (RecAdv) trasmesso telematicamente dall'acquirente al fornitore, ed indicando la merce presa in carico.

3.2 - La digitalizzazione dei DDT emessi e ricevuti

Passando ad analizzare alcuni processi di digitalizzazione dei DDT che imprese e PA potrebbero adottare, affronteremo dapprima i DDT emessi ai clienti, dopodichè quelli ricevuti dai fornitori.

► La digitalizzazione dei DDT emessi ai clienti

I DDT emessi ai clienti possono essere conservati in solo formato digitale sia nei casi in cui il DDT è un documento analogico (cioè cartaceo), sia nei casi in cui il DDT è già un documento informatico, e quindi possiamo schematizzare la conservazione digitale dei suddetti DDT in almeno 2 diverse modalità:

1 - conservazione digitale di DDT cartacei;

2 - conservazione digitale di DDT informatici.

Conservazione digitale di DDT cartacei

La conservazione digitale dei DDT emessi su carta, può essere schematizzata nelle seguenti fasi:

1. stampa del DDT in duplice copia (tre copie se si impiega un vettore terzo), di cui una copia da consegnare al cliente, e la restante copia riportante il barcode da riconsegnare all'azienda;
2. dopo i controlli eseguiti in fase di ritiro merce, apposizione da parte del cliente della firma autografa sulla copia del DDT da restituire all'azienda;
3. dopo che il DDT è stato consegnato all'azienda, periodicamente si procede alla scansione del DDT cartaceo con immediata produzione degli indici di ricerca grazie al riconoscimento

del barcode eseguito dal medesimo software di gestione documentale che lo aveva generato;

4. il DDT in formato digitale è già ricercabile e consultabile nel sistema di gestione documentale e pronto per essere consultato dagli addetti amministrativi in possesso delle opportune credenziali di accesso;
5. periodicamente, per esempio semestralmente oppure annualmente, conservazione digitale dei DDT con apposizione alle immagini dei singoli DDT della firma digitale, e successiva chiusura del processo di conservazione con firma digitale del responsabile della conservazione e marca temporale sull'indice del pacchetto di archiviazione, dopodichè sarà possibile procedere alla distruzione dei DDT cartacei.

Conservazione digitale di DDT informatici

La conservazione digitale dei DDT emessi come documenti informatici può essere schematizzata nelle seguenti fasi:

1. produzione del DDT come documento informatico, per esempio in formato PDF o XML, ed apposizione allo stesso della firma digitale utile a garantirne l'integrità e l'immodificabilità;
2. trasmissione telematica del DDT al cliente tramite email oppure PEC, da eseguirsi entro il giorno il cui è iniziato il trasporto dei beni. In questo caso è prevista la sola trasmissione telematica del DDT al cliente, e se l'azienda fornitrice ritenesse utile richiedere la firma del cliente sul DDT, è sempre possibile adottare innovative soluzioni quali la firma grafometrica (e.g. tablet/palmari) oppure altre tipologie di firme elettroniche;
3. periodicamente, per esempio semestralmente oppure annualmente, conservazione digitale dei DDT con firma digitale del responsabile della conservazione e marca temporale sull'indice del pacchetto di archiviazione.

► La digitalizzazione dei DDT ricevuti dai fornitori

I DDT ricevuti dai fornitori possono essere conservati in solo formato digitale sia nei casi in cui il DDT è un documento analogico (cioè cartaceo), sia nei casi in cui il DDT è già un documento informatico, e quindi possiamo schematizzare la conservazione digitale dei suddetti DDT in almeno 2 diverse modalità:

1 - conservazione digitale di DDT cartacei;

2 - conservazione digitale di DDT informatici.

Conservazione digitale di DDT cartacei

La conservazione digitale dei DDT ricevuti su carta può essere schematizzata nelle seguenti fasi:

1 - ricezione della copia del DDT;

2 - scansione del DDT cartaceo con associazione degli indici di ricerca tramite inserimento manuale oppure con l'ausilio di sistemi di riconoscimento OCR (Optical Character Recognition), e con successiva acquisizione dell'immagine nel sistema di gestione documentale al fine di poter essere consultata dagli addetti amministrativi in possesso delle opportune credenziali di accesso;

3 - periodicamente, per esempio semestralmente oppure annualmente, conservazione digitale dei DDT con apposizione alle immagini dei singoli DDT della firma digitale, e successiva chiusura del processo di conservazione con firma digitale del responsabile della conservazione e marca temporale sull'indice del pacchetto di archiviazione, dopodichè sarà possibile procedere alla distruzione dei DDT cartacei.

Conservazione digitale di DDT informatici

La conservazione digitale dei DDT ricevuti come documenti informatici, può essere schematizzata nelle seguenti fasi:

1 - ricezione del DDT come documento informatico in formato PDF e firmato digitalmente utile a garantirne l'integrità e l'immodificabilità;

2 - associazione al DDT degli indici di ricerca tramite inserimento manuale oppure con l'ausilio di sistemi di riconoscimento OCR, e con successiva acquisizione dell'immagine nel sistema di gestione documentale al fine di poter essere consultata dagli addetti amministrativi in possesso delle opportune credenziali di accesso;

3 - periodicamente, per esempio semestralmente oppure annualmente, conservazione digitale dei DDT con firma digitale del responsabile della conservazione e marca temporale sull'indice del pacchetto di archiviazione.

3.3 - L'obbligo introdotto dalla regione Emilia Romagna

Con la delibera della Giunta regionale n.287 del 23 marzo 2015, la regione Emilia Romagna ha introdotto dal 30 giugno 2016 l'obbligo per le pubbliche amministrazioni di emettere ordini oltre che di ricevere DDT dai propri fornitori in solo formato elettronico, ed in particolare:

- Dal 31 gennaio 2016 le amministrazioni e gli enti della regione Emilia Romagna sono

tenuti ad inserire nelle procedure di gara indette per l'acquisto di beni e servizi clausole che prevedono l'obbligo per i fornitori di ricevere ordini elettronici ed inviare DDT elettronici attraverso il Nodo Telematico di Interscambio (NoTI-ER);

- Dal 30 giugno 2016 le aziende e gli enti del sistema sanitario regionale emettono ordini esclusivamente in formato elettronico attraverso il sistema NoTI-ER;
- Dal 30 giugno 2016 le aziende e gli enti del sistema sanitario regionale emettono DDT indirizzati ad altre aziende ed enti del sistema sanitario regionale esclusivamente in formato elettronico attraverso il sistema NoTI-ER.

La scelta coraggiosa adottata dalla regione Emilia Romagna, primo caso nel panorama regionale Italiano ad avere imposto ai fornitori un obbligo di ricezione degli ordini ed emissione dei DDT in solo formato elettronico, è incentrata su due importanti aspetti:

- impiego di PEPPOL (Pan-European Public Procurement OnLine) quale infrastruttura open source in grado di veicolare i documenti del processo eProcurement in formato XML secondo prestabiliti standard internazionali;
- supporto alle PA coinvolte nell'obbligo tramite l'ausilio di NoTI-ER quale infrastruttura tecnologica in grado di gestire la trasmissione degli ordini e la ricezione dei DDT, e più in generale del "Sistema Regionale per la dematerializzazione del Ciclo Passivo dell'Emilia Romagna" (SiCiPa-ER) in grado di gestire anche le fatture elettroniche oltre che provvedere alla conservazione digitale di tutti i documenti prodotti in ambito eProcurement.

► PEPPOL

Il settore della pubblica amministrazione in Europa partecipa alla creazione della ricchezza con una quota del 19,7% del PIL, ma molte imprese, in particolar modo le PMI, riscontrano problemi nel partecipare alle gare pubbliche, soprattutto per la documentazione amministrativa da presentare, ed in particolare se la PA è situata in un altro Stato membro.

Il principale obiettivo di PEPPOL è quello di **consentire alle imprese di uno Stato membro di trasmettere elettronicamente alla PA di un diverso Stato membro la documentazione amministrativa di un intero processo di acquisto B2G** (eProcurement), senza problemi di interoperabilità legati a standard nei protocolli di trasmissione o formato dei documenti, ed

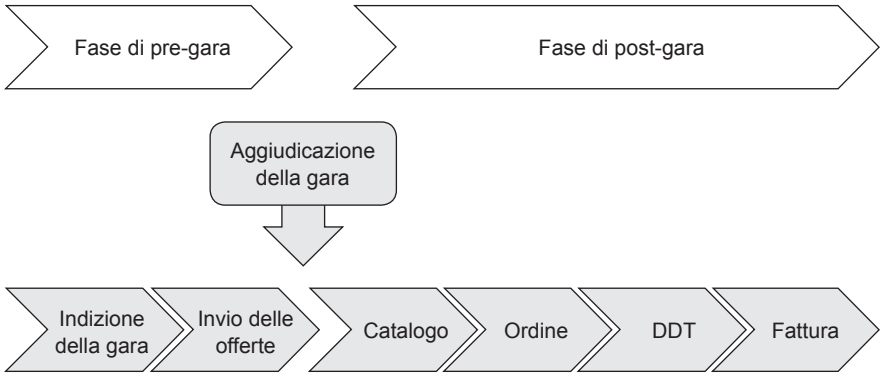
adottando una infrastruttura tecnica open source che consente di veicolare i dati tra i diversi Access Point aderenti al network.

Il progetto PEPPOL venne avviato nel 2008 dalla Commissione europea e da un consorzio di 18 PA di 11 Stati membri tra cui l'Italia, sottoscrivendo un accordo su un comune standard da adottare nei contenuti dei documenti (e.g. catalogo, ordine, fattura) e negli aspetti tecnici in fase di trasmissione dei dati (e.g. infrastruttura di trasmissione, caratteristiche degli Access Point, etc).

La principale caratteristica di PEPPOL è che è una soluzione di eProcurement tecnologicamente sicura ed open source, basata su accordi di trasmissione tra gli aderenti al network del tipo "many-to-many" (e non quindi "1-to-1" che richiederebbe singoli accordi bilaterali) ed a cui è possibile accedere tramite 142 Access Point di cui ben 16 situati in Italia, e tramite i quali per una impresa Italiana è possibile colloquiare elettronicamente con una qualsiasi PA aderente al network.

Con riguardo allo standard dei documenti, PEPPOL ha sviluppato un proprio Business Interoperability Specifications (PEPPOL BIS) del catalogo (BIS 1A), degli ordini (BIS 3A) e delle fatture (BIS4A), adottando il CEN WS BII, cioè i risultati del *CEN workshop Interoperability Interfaces for Public Procurement in Europe.*

Figura 19. ***Principali documenti in ambito eProcurement***



► NoTI-ER

Nell'ambito "Sistema Regionale per la dematerializzazione del Ciclo Passivo dell'Emilia Romagna" (SiCiPa-ER), al fine di supportare le PA coinvolte nell'obbligo introdotto dal 30 giugno 2016, la regione Emilia Romagna ha istituito il "Nodo Telematico di Interscambio" (NoTI-ER) quale sistema che interfacciandosi sia con la PA che con i fornitori è in grado di ricevere e gestire gli ordini ed i DDT elettronici, così come il SDI riceve e gestisce le fatture elettroniche trasmesse dai fornitori della PA.

È possibile riassumere il seguente funzionamento nei seguenti passaggi chiave:

1. la PA crea l'ordine di acquisto in formato XML e lo trasmette a NoTI-ER, che tramite Intercent-ER quale Access Point lo veicola al network PEPPOL e quindi all'Access Point del fornitore che provvederà a trasmetterlo al fornitore;
2. in fase di consegna dei beni e quindi di emissione del DDT, il fornitore crea il DDT elettronico in formato XML e lo trasmette al proprio Access Point, il quale tramite il network PEPPOL lo veicola ad Intercent-ER e quindi al servizio NoTI-ER che provvederà a comunicarlo alla PA destinataria;
3. periodicamente viene avviata la conservazione digitale degli ordini e dei DDT, sia da parte del fornitore tramite una soluzione in house oppure esternalizzando il servizio ad un conservatore, sia da parte della PA tramite l'ausilio del "Polo Archivistico dell'Emilia Romagna" (PARER) quale conservatore accreditato.

Figura 20. ***Schema di funzionamento di SiCiPa-ER***

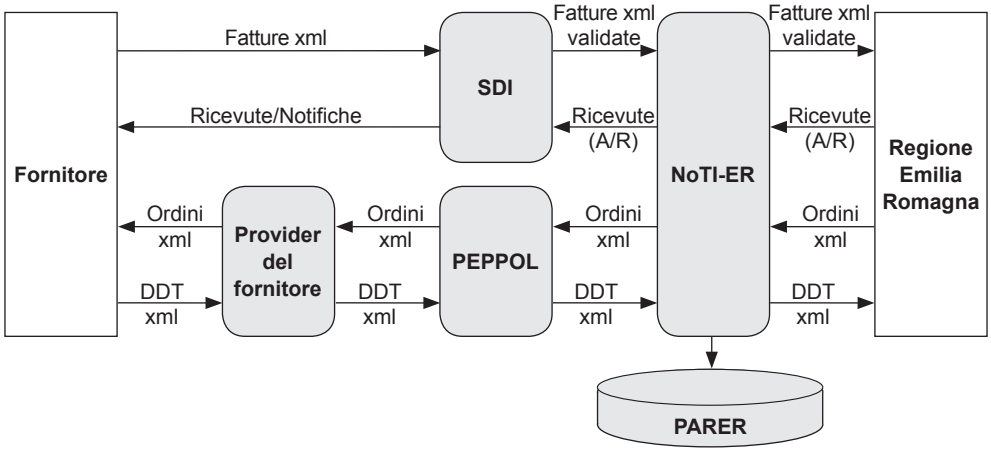
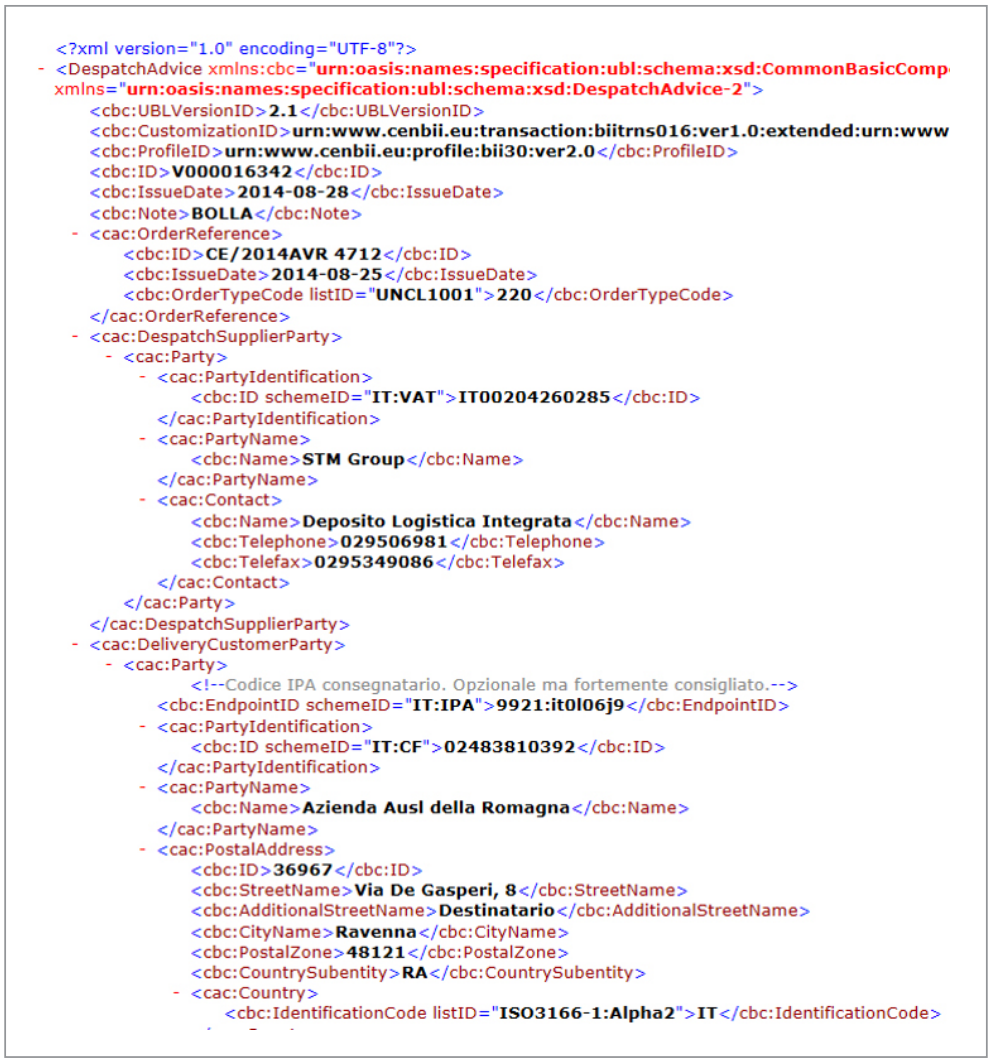


Figura 21. ***Immagine di DDT in formato XML***



```
<?xml version="1.0" encoding="UTF-8"?>
- <DespatchAdvice xmlns:cbc="urn:oasis:names:specification:ubl:schema:xsd:CommonBasicComp
xmlns="urn:oasis:names:specification:ubl:schema:xsd:DespatchAdvice-2">
    <cbc:UBLVersionID>2.1</cbc:UBLVersionID>
    <cbc:CustomizationID>urn:www.cenbii.eu:transaction:biitrns016:ver1.0:extended:urn:www
    <cbc:ProfileID>urn:www.cenbii.eu:profile:bii30:ver2.0</cbc:ProfileID>
    <cbc:ID>V000016342</cbc:ID>
    <cbc:IssueDate>2014-08-28</cbc:IssueDate>
    <cbc:Note>BOLLA</cbc:Note>
  - <cac:OrderReference>
      <cbc:ID>CE/2014AVR 4712</cbc:ID>
      <cbc:IssueDate>2014-08-25</cbc:IssueDate>
      <cbc:OrderTypeCode listID="UNCL1001">220</cbc:OrderTypeCode>
    </cac:OrderReference>
  - <cac:DespatchSupplierParty>
    - <cac:Party>
      - <cac:PartyIdentification>
          <cbc:ID schemeID="IT:VAT">IT00204260285</cbc:ID>
        </cac:PartyIdentification>
      - <cac:PartyName>
          <cbc:Name>STM Group</cbc:Name>
        </cac:PartyName>
      - <cac:Contact>
          <cbc:Name>Deposito Logistica Integrata</cbc:Name>
          <cbc:Telephone>029506981</cbc:Telephone>
          <cbc:Telefax>0295349086</cbc:Telefax>
        </cac:Contact>
      </cac:Party>
    </cac:DespatchSupplierParty>
  - <cac:DeliveryCustomerParty>
    - <cac:Party>
          <!--Codice IPA consegnatario. Opzionale ma fortemente consigliato.-->
        <cbc:EndpointID schemeID="IT:IPA">9921:it0l06j9</cbc:EndpointID>
      - <cac:PartyIdentification>
          <cbc:ID schemeID="IT:CF">02483810392</cbc:ID>
        </cac:PartyIdentification>
      - <cac:PartyName>
          <cbc:Name>Azienda Ausl della Romagna</cbc:Name>
        </cac:PartyName>
      - <cac:PostalAddress>
          <cbc:ID>36967</cbc:ID>
          <cbc:StreetName>Via De Gasperi, 8</cbc:StreetName>
          <cbc:AdditionalStreetName>Destinatario</cbc:AdditionalStreetName>
          <cbc:CityName>Ravenna</cbc:CityName>
          <cbc:PostalZone>48121</cbc:PostalZone>
          <cbc:CountrySubentity>RA</cbc:CountrySubentity>
        - <cac:Country>
            <cbc:IdentificationCode listID="ISO3166-1:Alpha2">IT</cbc:IdentificationCode>
```

CAPITOLO 4

PEC e firma grafometrica

4.1 - La PEC

4.1.1. - Funzionamento della PEC

La Posta Elettronica Certificata (PEC), introdotta nel nostro ordinamento con il DPR 11 febbraio 2005 n.68 e con il decreto 2 novembre 2005 che ne stabiliva le regole tecniche, viene definita all'art.1 lettera v/bis del CAD, come un "*sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi".*

La trasmissione di un messaggio tramite l'impiego della PEC, che prevede il rilascio all'emittente di una "*ricevuta di accettazione*" e di una "*ricevuta di avvenuta consegna*", equivale ad una raccomandata con avviso di ricevimento, dato che l'art.48 secondo comma del CAD stabilisce 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."*

La PEC è quindi un "*sistema di comunicazione*" che consente di certificare data ed ora di spedizione del messaggio, data ed ora di ricezione del messaggio, integrità del messaggio trasmesso e tracciabilità delle attività svolte, e necessita della presenza di almeno quattro soggetti:

- il mittente;
- il gestore PEC del mittente;
- il destinatario;
- il gestore PEC del destinatario.

L'impiego della PEC nell'ambito delle comunicazioni eseguite dalle imprese e dagli studi professionali, sta riscuotendo una crescente diffusione, sia perché per i suddetti soggetti vi è un preciso obbligo normativo che ne richiede la dotazione[41], sia perché è lo stesso legislatore che ne sta accelerando il suo utilizzo.

È il caso per esempio dell'art.17 del decreto legge 18 ottobre 2012 n.179 che prevede che i Curatori fallimentari debbano comunicare con i creditori solo tramite PEC, oppure dell'art. 62 del decreto legge 24 gennaio 2012, n. 1 che introducendo nel settore agroalimentare un

41 Decreto Legge 29 novembre 2008, n. 185

obbligo di pagamento dei fornitori entro 60 giorni dalla ricezione della fattura, prevede la PEC quale strumento in grado di certificarne la ricezione, oppure l'obbligo della fatturazione elettronica alla PA dove la PEC è uno dei 5 canali di trasmissione previsti per comunicare con il SDI.

È possibile riassumere il funzionamento della PEC nei seguenti 10 passaggi:

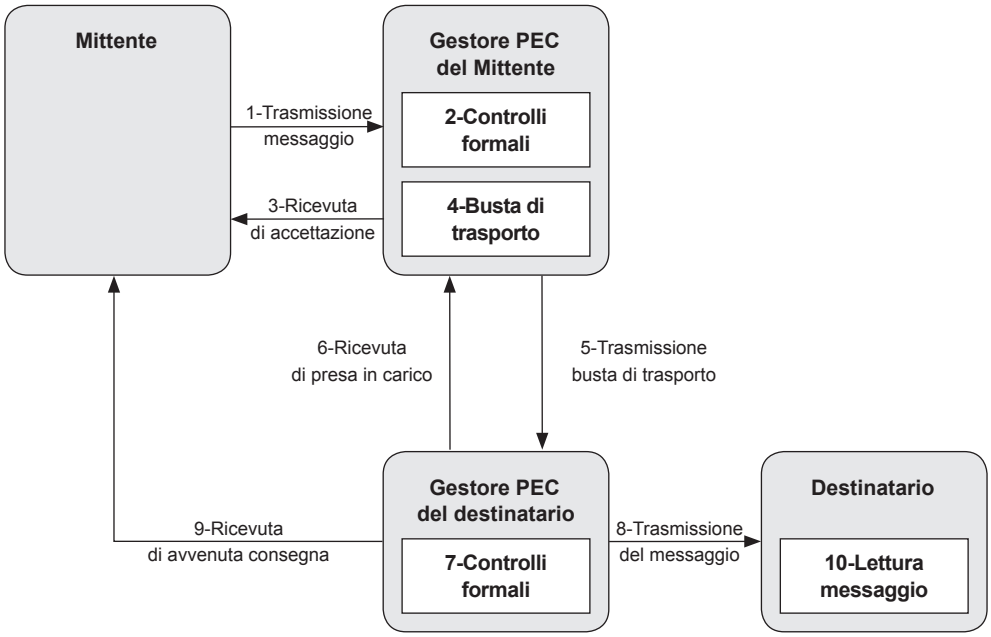
1. il mittente, tramite il proprio punto di accesso e previa autenticazione (User-ID e password), accede ai servizi PEC resi disponibili dal proprio gestore PEC ed invia il messaggio;
2. il gestore PEC del mittente svolge una serie di controlli formali sui messaggi (esistenza di un campo "From" con indirizzo email conforme alle specifiche RFC 2822, assenza di indirizzi dei destinatari nel campo "Ccn", assenza di virus, etc). In caso di anomalie il messaggio non verrà inoltrato ed al mittente verrà comunicato un "*avviso di non accettazione"* firmato dal gestore PEC del mittente riportante l'impossibilità ad accettare il messaggio in ingresso, le motivazioni per cui non è possibile accettare il messaggio e l'indicazione che il messaggio non potrà essere consegnato al destinatario;
3. in caso di controlli andati a buon fine, rilascio al mittente da parte del suo gestore PEC della "*ricevuta di accettazione*" con firma del gestore PEC del mittente e contenente i "*dati di certificazione*" che costituiscono prova dell'avvenuta accettazione di un messaggio: data ed ora di accettazione, mittente, destinatario ed oggetto. I "*dati di certificazione*" sono altresì inseriti in un file XML allegato alla ricevuta per consentire una elaborazione automatica;
4. il messaggio originale immodificato ed i "*dati di certificazione*" (in formato XML) vengono imbustati in una *busta di trasporto* a cui verrà apposta una firma da parte del gestore PEC del mittente;
5. trasmissione della *busta di trasporto* dal gestore PEC del mittente al gestore PEC del destinatario tramite l'impiego del protocollo SMTP su trasporto TLS (standard RFC 3207);
6. trasmissione da parte del gestore PEC del destinatario al gestore PEC del mittente della *"ricevuta di presa in carico"* (contenente i "*dati di certificazione*"), al fine di poter attestare l'avvenuta presa in carico del messaggio e consentire il tracciamento del messaggio nel passaggio da un gestore PEC ad un altro gestore PEC;
7. il gestore PEC del destinatario, ricevuto il messaggio, svolge una serie di controlli (controllo dell'esistenza della firma, controllo che la firma sia stata emessa da un gestore PEC, controllo validità della firma, controlli sulla correttezza formale, controlli presenza di virus) ed in caso di riscontro di anomalie, invia al mittente un *"avviso di mancata consegna";*
8. in caso di controlli andati a buon fine, il gestore del destinatario provvede a depositare il messaggio nella casella PEC del destinatario;

9. il gestore PEC del destinatario provvede ad inviare al mittente la *"ricevuta di avvenuta consegna"* firmata dallo stesso gestore del destinatario e contenente i "*dati di certificazione*" che costituiscono prova che il messaggio è stato depositato nella casella PEC del destinatario: data ed ora di avvenuta consegna, mittente, destinatario ed oggetto. I "*dati di certificazione*" sono altresì inseriti in un file XML allegato alla ricevuta per consentire una elaborazione automatica;
10. il destinatario tramite il proprio punto di accesso e previa autenticazione (User-ID e password), accede ai servizi PEC resi disponibili dal proprio gestore PEC e legge il messaggio.

Vanno infine ricordati i seguenti aspetti:

- le firme apposte dai gestori PEC ai messaggi (ricevute, avvisi, buste), sono firme elettroniche avanzate basate su sistemi a chiavi asimmetriche al fine garantire l'autenticità e l'integrità dei messaggi trasmessi nel sistema di comunicazione PEC;
- sui singoli messaggi (ricevute, avvisi, buste) il gestore PEC appone un riferimento temporale e quotidianamente una marca temporale sui *log* dei messaggi;
- per tutte le attività eseguite durante la fase di trasmissione del messaggio vengono creati appositi *log* delle operazioni svolte che saranno conservati dai gestori PEC in appositi registri per trenta mesi e che sono:
  1. il codice identificativo univoco assegnato al messaggio originale;
  2. la data e l'ora dell'evento;
  3. il mittente del messaggio originale;
  4. i destinatari del messaggio originale;
  5. l'oggetto del messaggio originale;
  6. il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.);
  7. il codice identificativo (Message-ID) dei messaggi correlati generati (ricevute, errori, ecc.).

Figura 22. ***Funzionamento della PEC***



4.1.2 - Gestire correttamente la PEC

Al fine di consentire una corretta gestione della PEC da parte di imprese e studi professionali, vanno rilevati alcuni aspetti ed utili suggerimenti:

► La PEC non può sostituire la firma digitale

La PEC è un "*sistema di comunicazione*" in grado di certificare data ed ora di spedizione e di ricezione del messaggio oltre che la sua integrità durante la trasmissione, mentre la firma digitale attribuisce al documento informatico l'efficacia prevista dall'articolo 2702 del Codice civile: *"La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta."* La sottoscrizione di un documento informatico (e.g. scrittura privata, etc) dovrà quindi avvenire tramite l'impiego della firma digitale, dopodichè il documento informatico sottoscritto potrà essere trasmesso alla controparte tramite la PEC.

► La PEC non può sostituire la marca temporale

Pur essendo la PEC un "*sistema di comunicazione*" che consente comunque di ottenere una validazione temporale, va rilevato che la marca temporale è certamente insostituibile in alcuni contesti, come per esempio nell'ambito dei processi di conservazione digitale di documenti tributari.

► La PEC non è un sistema di conservazione

Dopo che l'impresa o lo studio hanno utilizzato lo strumento PEC per trasmettere e/o ricevere documenti informatici, è necessario che i messaggi rilasciati dal sistema PEC (ricevute ed avvisi) vengano conservati in modalità digitale secondo le disposizioni di cui al DPCM 3 dicembre 2013 e DMEF 17 giugno 2014, dato che a norma dell'art. 2220 del Codice civile:
"Le scritture devono essere conservate per dieci anni dalla data dell'ultima registrazione. Per lo stesso periodo devono conservarsi le fatture, le lettere e i telegrammi ricevuti e le copie delle fatture, delle lettere e dei telegrammi spediti. Le scritture e documenti di cui al presente articolo possono essere conservati sotto forma di registrazioni su supporti di immagini, sempre che le registrazioni corrispondano ai documenti e possano in ogni momento essere rese leggibili con mezzi messi a disposizione dal soggetto che utilizza detti supporti."
In sostanza quindi, la semplice archiviazione dei messaggi PEC (ricevute ed avvisi) in un sistema di gestione elettronica documentale oppure ancora più semplicemente nella casella PEC senza che questi siano stati conservati in un valido sistema di conservazione è una pratica non conforme alle disposizioni normative, da evitare e da sconsigliare.

► Verificare periodicamente lo spazio disponibile della casella PEC

La casella PEC ha una dimensione limitata che è stabilita dal gestore PEC e che dipende dal tipo di servizio acquistato (le offerte basi prevedono solitamente uno spazio compreso tra 1-2 GB) ed è quindi necessario verificare periodicamente la presenza di un sufficiente spazio disponibile, dato che diversamente i messaggi in arrivo verranno rifiutati per mancanza di spazio libero. Questo vale soprattutto quando si trasmette un file di notevole dimensione a più destinatari (la normativa prevede la possibilità di poter inviare lo stesso messaggio ad almeno 50 destinatari), dato che le ricevute di avvenuta consegna hanno in allegato l'intero messaggio originale trasmesso.

► Il messaggio trasmesso può avere una dimensione massima di 30 MB

Il messaggio trasmesso può avere una dimensione massima di 30 MB e quindi in caso di trasmissione di file aventi una dimensione superiore, sarà necessario suddividerlo in più file ed eseguire più trasmissioni oppure impiegare altri strumenti di trasmissione.

► I log vengono conservati dai gestori PEC per 30 mesi

I log generati nel corso di tutte le attività svolte durante la fase di trasmissione del messaggio, vengono conservati dai gestori PEC in appositi registri per trenta mesi. Nel corso del suddetto periodo è quindi possibile per gli utenti richiedere al gestore PEC la visione delle informazioni contenute nel "registro dei log" oltre che l'esibizione di specifici report estratti dal "registro dei log" riportanti i dati attestanti il transito dei messaggi nell'ambito del sistema PEC.

Decorso quindi i 30 mesi previsti dall'art. 11 del DPR 11 febbraio 2005 n.68, i gestori PEC non hanno più alcun obbligo di garantire ai propri utenti la possibilità di poter visionare ed estrarre report dei log prodotti dal sistema PEC. Questo potrebbe essere un eventuale aspetto di criticità e si suggerisce quindi, se il servizio del gestore PEC lo prevede, di valutare una estensione del suddetto periodo.

► La PEC è un sistema di comunicazione solo Italiano

La PEC è un sistema di comunicazione che può essere adottato solo in ambito Italiano, dato che ad oggi non vi è alcuna interoperabilità con analoghi sistemi presenti in altri Stati membri, come per esempio con la De-Mail introdotta in Germania dal 2 maggio 2011 con la legge *De-Mail-Gesetz*, oppure con la *electronic registered mail* introdotta nel 2010 in Belgio, oppure con la *registered mail* introdotta nel 2011 in Francia.

Figura 23. ***Elenco dei gestori PEC***

Ragione Sociale	Indirizzo della sede legale	Rappresentante legale	Data iscrizione elenco
ACI Informatica S.p.A.	Via Fiume delle Perle, 24 – 00144 Roma	Angelo Sticchi Damiani, Mauro Minenna	17-12-09
Actalis S.p.A.	Via dell'Aprica, 18 – 20158 Milano	Simone Braccagni	22-12-05
Ancitel S.p.A.	Via dei Prefetti, 46 – 00186 Roma (RM)	Osvaldo Napoli, Giuseppe Paolo Teti	19-07-07
ARUBA PEC S.p.A.	Via Sergio Ramelli, 8 – 52100 Arezzo (AR)	Simone Braccagni	12-10-06
Cedacri S.p.A.	Via del Conventino, 1 – 43044 Collecchio (PR)	Sergio Capatti	09-02-06
Consiglio Nazionale del Notariato	Via Flaminia, 160 – 00196 Roma	Maurizio D'Errico	22-12-05
Fastweb S.p.A.	Via Caracciolo, 51 – Milano (MI)	Carsten Schloter, Ulrich Dietiker	04-10-07
HP ES Italia S.r.l. (già EDS Italia S.r.l.)	Via G. Di Vittorio, 9 – 20063 Cernusco sul Naviglio (MI)	Stefano Venturi	13-07-06
IN.TE.S.A. S.p.A.	Corso Orbassano 367 - 10137 Torino	Enrico Cereda	12-10-06
Infocert S.p.A.	Piazza Sallustio, 9 - 00187 Roma	Fernando Zilio	19-01-07
Innova Puglia S.p.A.	Str. Prov. Per Casamassima Km.3 – 70010 Valenzano BA	Pasquale Chieco	14-06-07
INTRED S.p.A.	Via Creta, 15 – 25124 - Brescia	Daniele Peli	04-05-11
ITnet S.r.l.	Via Lorenteggio, 257 – 20148 Milano	Gianni Signa	30-03-06
KPNQwest Italia S.p.A.	Via Leopardi, 9 - 20123 Milano (MI)	Marco Fiorentino	14-12-10
Namirial S.p.A.	Via Caduti sul Lavoro, 4 - 60019 Senigallia (AN)	Paolo Giacometti	27-02-07
Numera Sistemi e Informatica S.p.A.	Via Quarto, 2 – 07100 Sassari	Antonio Capitta	27-07-06
Poste Italiane S.p.A.	Viale Europa, 190 – 00144 Roma	Luisa Todini, Francesco Caio	19-01-06
Postecom S.p.A.	Viale Europa, 175 – 00144 Roma	Vincenzo Pompa	22-12-05
Regione Basilicata	Via Vincenzo Verrastro, 4 - 85100 Potenza (PZ)	Angelo Pietro Paolo Nardozza	19-01-12
Regione Marche	Via Gentile da Fabriano 9 - 60125 Ancona	Gian Mario Spacca	30-10-12
Register.it S.p.A.	Piazza Pietro Annigoni, 9/B - 50122 Firenz	Claudio Corbetta	31-10-12
Sogei – Società Generale d'Informatica S.p.A.	Via Mario Carucci, 99 – 00143 Roma	Cristiano Cannarsa	21-09-06
Telecom Italia Trust Technologies S.r.l. (già I.T. Telecom S.r.l.)	VS.S. 148 Pontina, km 29,100 – 00040 Pomezia (RM)	Leopoldo Genovesi	22-12-05
TWT S.p.A.	Via A. Sangiorgio, 12 – 20145 Milano (MI)	Marco Rodolfi	26-06-07
Università degli studi di Napoli Federico II	Corso Umberto I , 80138 Napoli (NA)	Magnifico Rettore Prof. Massimo Marrelli	01-10-09

4.2 - La firma grafometrica

4.2.1 - Funzionamento della firma grafometrica

La firma grafometrica è una particolare firma elettronica che sta riscuotendo una notevole diffusione, soprattutto in specifici settori come per esempio il settore bancario ed assicurativo, ma anche in ambito aziendale (e.g. DDT) oltre che negli studi professionali.

Uno dei principali motivi di questo successo è dovuto alla circostanza che il gesto che il firmatario compie nel firmare non cambia rispetto ad una sottoscrizione su carta, e l'unica differenza è che la firma viene eseguita su una particolare tavoletta (tablet o palmare) in grado di intercettare i dati grafometrici ed associarli al documento informatico firmato.

La tecnologia che consente alla tavoletta di generare i dati grafometrici del firmatario è generalmente basata su sistemi elettromagnetici, con rilevanti proprietà come per esempio la possibilità di intercettare i movimenti della penna anche se non vi è un reale contatto con il piano di firma (tablet).
I dati grafometrici che vengono intercettati dalla tavoletta dipendono in gran parte dalle caratteristiche tecniche della tavoletta e della penna impiegata, ma sono solitamente la velocità, l'accelerazione, la decelerazione e la pressione.
Dopo che i dati grafometrici sono stati intercettati dalla tavoletta, al fine di evitare un qualsiasi loro utilizzo, vengono immediatamente cifrati (solitamente tramite cifratura asimmetrica) ed inseriti all'interno del documento informatico che si è appena firmato, dopodichè il documento informatico verrà conservato in solo formato digitale secondo le regole sui sistemi di conservazione.

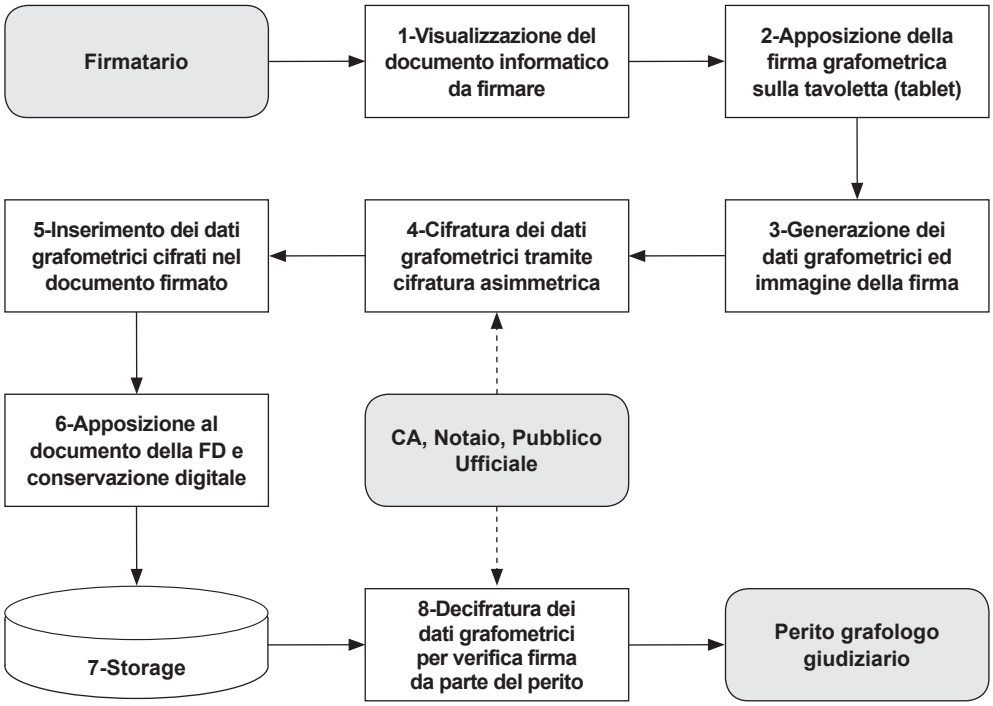
La firma grafometrica è una particolare tipologia di firma elettronica che se rispettate tutte le garanzie richieste dal legislatore in tema di firma elettronica avanzata riportate al titolo V del DPCM 22 febbraio 2013, consente di stabilire che*:" Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria"* (art. 21 secondo comma del CAD).
Diversamente quindi dalla firma digitale e dalla firma elettronica qualificata in cui l'utilizzo del dispositivo (smart-card, USB token) "*si presume riconducibile al titolare, salvo che questi dia prova contraria",* nel caso della firma grafometrica **è sempre possibile** disconoscerla e sarà quindi necessario l'intervento di un perito grafologo giudiziario in grado di verificare se è originale oppure se è stata falsificata.

Figura 24. ***Firma grafometrica***

Il processo di firma di un documento informatico tramite firma grafometrica lo possiamo riassumere nei seguenti principali passaggi:

1. visualizzazione da parte del firmatario del documento informatico che sarà oggetto di firma, direttamente sullo screen della tavoletta oppure su computer a supporto del processo;
2. apposizione della firma grafometrica sulla tavoletta (tablet o palmare) tramite l'impiego di una apposita penna e con richiesta finale di conferma della firma apposta;
3. generazione dei dati grafometrici da parte della tavoletta e dell'immagine della firma grafometrica;
4. immediata cifratura dei dati grafometrici, tramite per esempio sistema di cifratura asimmetrica la cui chiave privata è depositata presso un terzo soggetto garante (Certificatore Accreditato, Notaio, pubblico ufficiale, etc);
5. inserimento dei dati grafometrici cifrati all'interno del documento informatico in formato PDF appena sottoscritto;
6. apposizione al documento informatico della firma digitale al fine di garantirne l'autenticità e l'integrità;
7. conservazione digitale del documento informatico tramite l'impiego di un valido sistema di conservazione conforme al DPCM 3 dicembre 2013,
8. in caso di disconoscimento della firma grafometrica che potrà svolgersi a distanza di anni, vi sarà la decifratura tramite chiave privata dei dati grafometrici da parte del terzo garante (Certificatore Accreditato, Notaio, pubblico ufficiale, etc) e l'intervento del perito grafologo giudiziario per verificare l'attendibilità della firma.

Figura 25. ***Processo di firma tramite firma grafometrica***



4.2.2 - Corretta gestione della firma grafometrica

Al fine di consentire una corretta gestione della firma grafometrica da parte di imprese e studi professionali, è utile rilevare alcuni aspetti ed utili suggerimenti:

► La firma grafometrica non è una firma digitale

La firma grafometrica non è una firma digitale, ma è una firma elettronica che nei casi in cui venga eseguita in totale conformità alle disposizioni normative di cui al titolo V del DPCM 22 febbraio 2013, potrà essere definita come firma elettronica avanzata. In sostanza, mentre la firma digitale si chiama appunto "digitale" perché viene generata tramite l'impiego di un sistema di cifratura asimmetrico all'interno di un dispositivo di firma (senza quindi alcun margine di errore) ed il cui utilizzo *"si presume riconducibile al titolare, salvo che questi dia prova contraria",* la firma grafometrica è una firma elettronica generata da processi e

procedure informatiche che se non implementati correttamente potrebbero mettere a rischio il valore probatorio dei documenti informatici sottoscritti.

► Conservazione digitale dei documenti con firma grafometrica

I documenti informatici riportanti una firma grafometrica necessitano di una loro conservazione unicamente in formato digitale, dato che è necessario preservare oltre al documento informatico anche i dati grafometrici in essi contenuti. È necessario quindi conservarli secondo le regole sui sistemi di conservazione di cui al DPCM 3 Dicembre 2013 garantendo la loro autenticità, integrità, affidabilità, leggibilità e reperibilità.

► Conformità a standard internazionali

La firma grafometrica produce dei dati grafometrici (*vettori grafometrici*) che vengono cifrati ed inseriti nel documento informatico sottoscritto e che potranno eventualmente essere utilizzati dal perito grafologo giudiziario in sede di perizia a distanza di anni rispetto al momento in cui si è firmato o di decenni rispetto al momento in cui si è implementato il processo di firma grafometrica.

È quindi necessario assicurarsi che l'intero processo di generazione della firma grafometrica, così come la generazione ed il trattamento dei dati grafometrici, vengano eseguiti secondo regole, procedure e standard riconosciuti a livello internazionale. Diversamente potrebbe verificarsi il caso che a distanza di anni si scopra che i dati grafometrici siano inutilizzabili da parte del perito grafologo giudiziario perché generati secondo specifiche di proprietà della software house produttrice del sistema di firma, che nel frattempo ha chiuso l'attività.

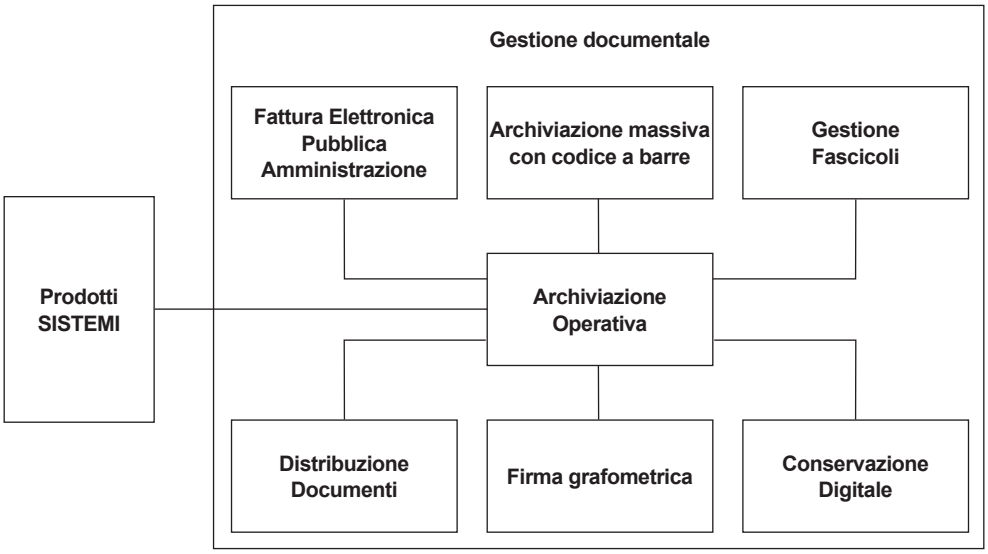
CAPITOLO 5

Le procedure Sistemi a supporto della conservazione digitale

5.1 - La digitalizzazione dei documenti

La digitalizzazione è il processo operativo che permette di archiviare in modo automatico i documenti informatici prodotti dalle procedure Sistemi e i documenti di origine esterna.

Figura 26. ***Flusso di digitalizzazione dei documenti***



5.1.1 - Archiviazione automatica dei documenti

L'archiviazione avviene contestualmente alla stampa o all'emissione del documento o in momento successivo mediante funzioni di elaborazione massiva.

Il processo di archiviazione automatica si articola nelle seguenti fasi:

1. l'emissione singola o massiva dei documenti da archiviare;
2. l'indicizzazione dei documenti attraverso l'estrazione automatica delle chiavi di ricerca;
3. l'archiviazione dei documenti in formato PDF o XML.

Il sistema di configurazione permette di effettuare l'archiviazione "d'ufficio" al momento della formazione del documento, oppure di lasciare all'operatore la facoltà di decidere se eseguire o meno l'archiviazione in fasi di stampa.

I documenti archiviati sono catalogati per tipologia di documento (ad esempio: Bilancio) e indicizzati sulla base delle informazioni rilevanti, definite chiavi di ricerca.
Le categorie di archiviazione aggregano le tipologie documenti in insiemi omogenei e definiscono l'insieme delle chiavi di ricerca previste per i documenti.

Figura 27. ***Esempio di classificazione dei documenti***

Tipologie documenti	Categoria di archivizione	Chiavi di ricerca
Prospetto di bilancio	Bilancio	Ragione sociale
Nota integrativa		Partita IVA
Relazione sulla gestione		Esercizio
…..		….

La classificazione dei documenti, ed in particolare le informazioni presenti nelle chiavi di ricerca, costituiscono la base che il sistema utilizza per ricercare il documento o tutti i documenti che condividono la stessa informazione

5.1.2 - Archiviazione manuale dei documenti

I documenti esterni, ossia non prodotti dalle procedure Sistemi, possono essere archiviati manualmente secondo diverse modalità.

Il documento da archiviare può essere:

- acquisito da file, se già esiste in formato elettronico;
- acquisito mediante scanner.

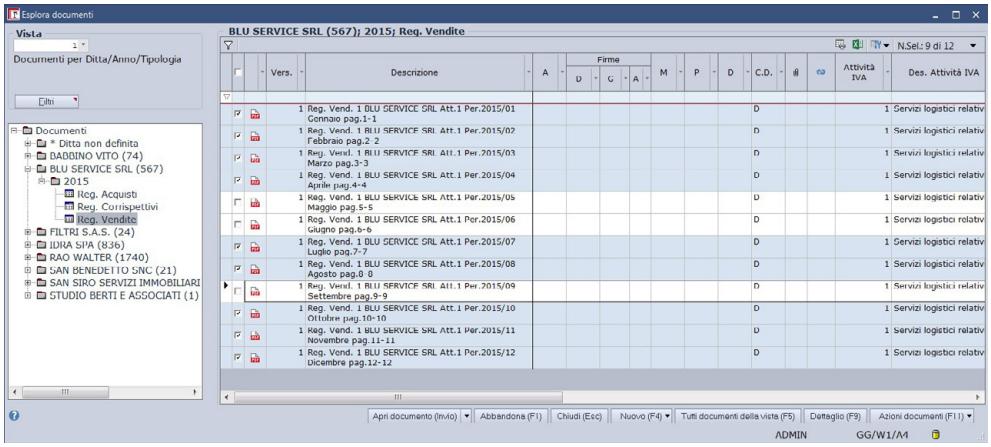
In presenza di una quantità significativa di documenti esterni il sistema prevede una modalità massiva di archiviazione tramite ***bar code***.
L'acquisizione massiva prevede che i documenti cartacei siano registrati dall'applicativo SISTEMI, catalogati con etichette che riportano il relativo codice a barre identificativo e successivamente scansionati ed acquisiti nel sistema.

5.1.3 - La consultazione dei documenti

I documenti archiviati possono essere richiamati direttamente dalle applicazioni: ad esempio la delega in formato pdf può essere consultata dalla funzione di gestione del modello F24.
La consultazione può avvenire da una specifica funzione di navigazione che consente la rappresentazione dei dati secondo una struttura gerarchica del tutto simile all'esplora risorse di MS Windows.

L'albero di visualizzazione non corrisponde ad una struttura fisica di cartelle, ma viene costruito dinamicamente secondo le esigenze di ricerca dell'operatore.
La consultazione dei documenti può quindi essere organizzata secondo varie viste, che costituiscono le regole con cui i dati sono rappresentati sul sistema.

Figura 28. ***Consultazione dei documenti archiviati***



Il sistema di archiviazione crea automaticamente dei collegamenti tra documenti, denominati correlazioni, che hanno una connessione logica con il documento d'origine: riprendendo l'esempio precedente, dall'interrogazione del modello F24 è possibile accedere alle sue ricevute di presentazione e pagamento.

5.1.4 - Le azioni sui documenti

Dalla funzione di consultazione è possibile eseguire una serie di operazioni sui documenti archiviati.
Il sistema permette di associare ad un documento altri documenti qualificati come allegati, ossia quei documenti che non hanno una qualificazione autonoma nel sistema, ma che condividono con il documento principale tutte le chiavi.
Anche gli allegati possono essere acquisiti da file se già presenti su file system o da scanner interfacciato con standard Twain.

Operando sui documenti archiviati è inoltre possibile:

- firmare digitalmente e marcare temporalmente i documenti;
- firmare grafometricamente i documenti;
- inviare il singolo documento e i suoi allegati/correlati via e-mail;
- stampare i documenti.

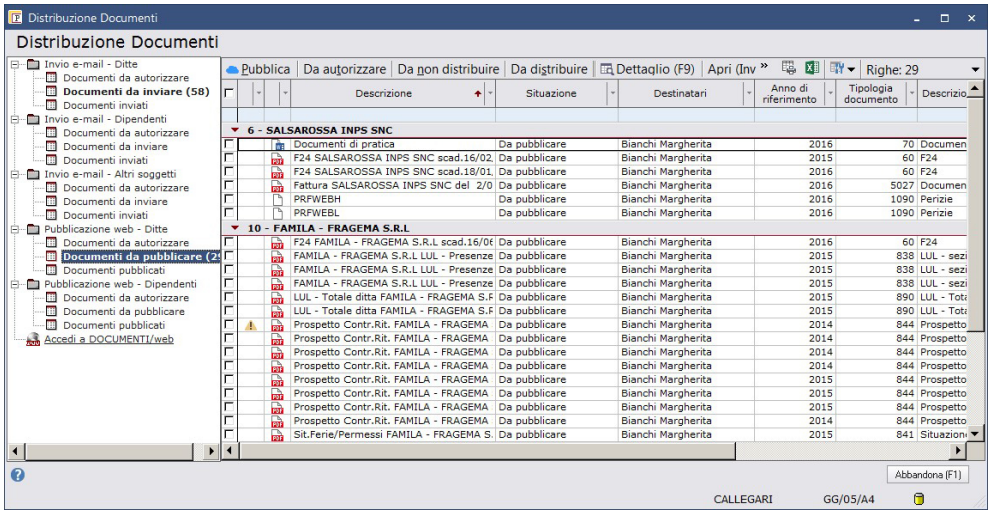
5.1.5 - La condivisione dei documenti

Il sistema prevede la possibilità di condividere i documenti archiviati mediante due canali di distribuzione:

- invio via e-mail;
- pubblicazione sul web.

L'invio tramite email consente di predefinire quali documenti inviare attraverso il canale e-mail e a quali clienti, dipendenti o altri soggetti, e di effettuare l'invio massivo.
Con la pubblicazione su **DOCUMENTI/web** i documenti sono pubblicati su un'area web riservata, residente presso la server farm SISTEMI, a cui i destinatari dei documenti pubblicati fanno accesso in maniera profilata.

Figura 29. ***Distribuzione dei documenti***



5.2 - La conservazione digitale nelle aziende e negli studi professionali

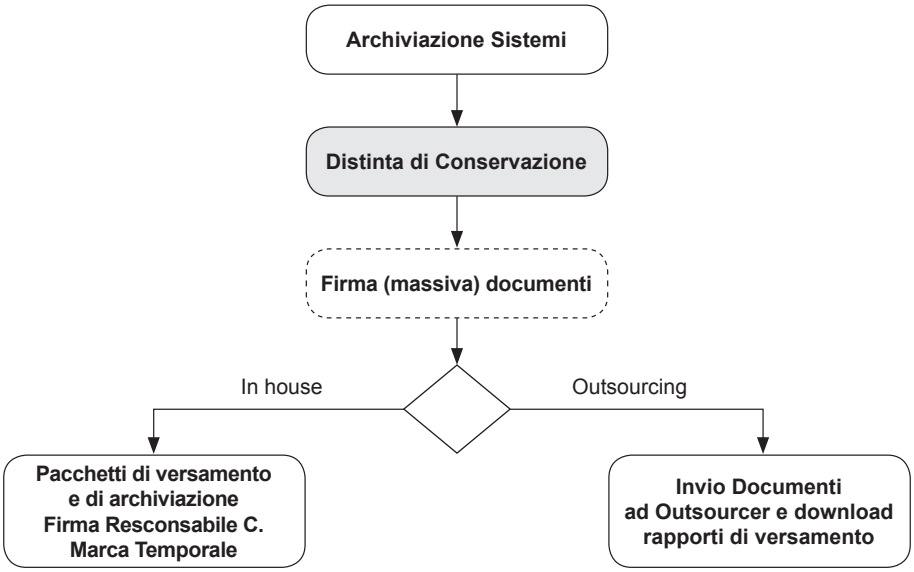
Il sistema di conservazione consente di attribuire e mantenere inalterato nel tempo il valore legale dei documenti per i quali esiste l'obbligo di conservazione ai fini civilistici e fiscali, rendendo superflua la materializzazione su supporto cartaceo.

Il processo di conservazione è gestito dal sistema mediante lo strumento della distinta di conservazione, che fornisce il corretto supporto organizzativo per ottemperare agli adempimenti in modo aderente alle disposizioni normative vigenti.

Per la conservazione del Libro Unico del Lavoro, date le peculiarità previste dalla normativa, dovute in particolare dal concatenamento delle scritture tra un mese e l'altro, è prevista una specifica "Distinta di Conservazione".

Il processo prevede diverse fasi che possono essere gestite per interno **all'interno del sistema (conservazione in house)** o gestite **in parte dal sistema e in parte da un soggetto terzo (conservazione in outsourcing).**

Figura 30. ***Processo di conservazione in house e in outsourcing a confronto***



Tutti i documenti destinati alla conservazione devono essere firmati digitalmente dall'emittente o da altra persona titolata a farlo. Il sistema supporta l'operatore non solo nella firma dei documenti, ma crea un sistema di classificazione dei documenti e dei firmatari, che garantisce che la firma sia apposta dalle persone titolate.
La firma può essere apposta sia in fase di archiviazione, sia successivamente nel corso del processo di conservazione digitale.

I paragrafi successivi analizzano nel dettaglio le fasi del processo per entrambe le modalità di conservazione.

5.2.1 - Modalità di conservazione in house

Il processo di **conservazione in house** provvede a creare i pacchetti di versamento, i relativi RdV e gli indici dei pacchetti di archiviazione (secondo lo standard SInCRO) e si conclude con l'apposizione della marca temporale e della firma da parte del soggetto incaricato al ruolo di Responsabile della conservazione. Il processo si articola in tre fasi.

Creazione della distinta di conservazione

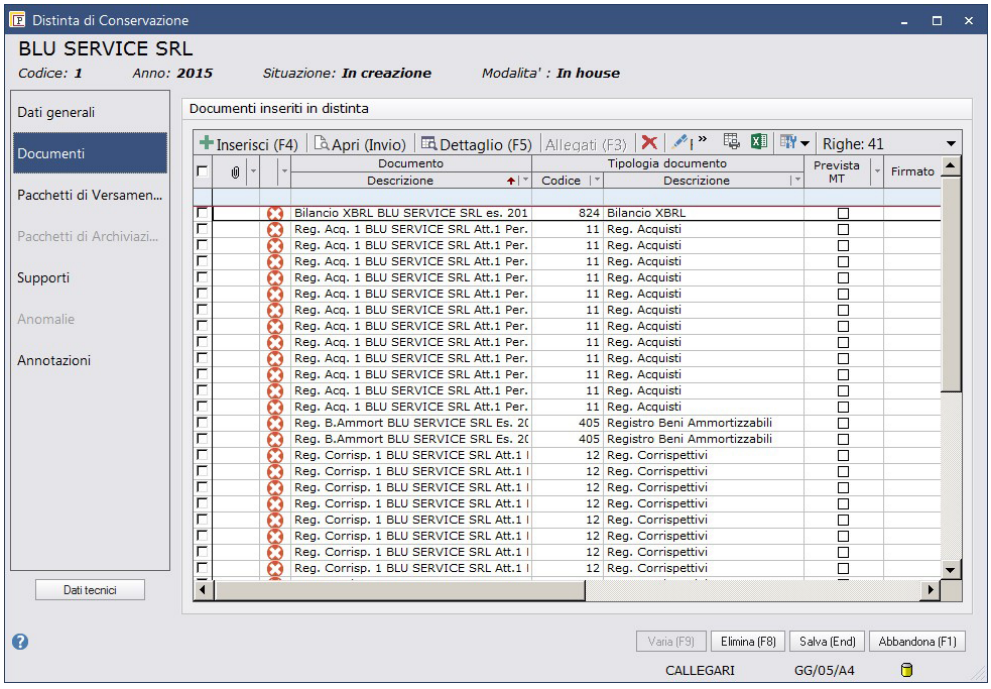
La distinta **raccoglie l'elenco dei documenti da conservare**, con riferimento ad un determinato anno, per una certa ditta o intermediario ed eventualmente limitatamente a determinate tipologie di documento e/o sezionali IVA.

In fase di creazione, il sistema identifica tutti i documenti che devono essere inseriti nella distinta, includendo i soli documenti per i quali è prevista la conservazione.

Un sistema di **creazione multipla** permette di creare automaticamente una distinta per ciascuna ditta che presenta documenti da conservare nell'anno di riferimento.

Per gestire la fase successiva è inoltre richiesta l'indicazione del responsabile della conservazione e del soggetto conservatore per conto del quale esplica l'attività di responsabile.

Figura 31. ***Distinta di conservazione***



Invio della distinta in conservazione

Quando la distinta è inviata in conservazione, il sistema verifica se tutti i documenti sono correttamente firmati ed eventualmente provvede alla firma massiva di tutti i documenti.

Il sistema svolge tutte le operazioni che garantiscono il corretto processo:

1. crea i pacchetti di versamento, raggruppando i documenti della distinta in base alla categoria di conservazione;
2. calcola l'impronta di *hash*, ovvero una sequenza di simboli binari che garantisce l'univocità del documento;
3. genera per ciascun pacchetto un rapporto di versamento, che viene firmato digitalmente dal Responsabile della Conservazione e archiviato.

Con l'invio in conservazione si ottiene il "blocco" dei documenti riferiti alla distinta: da questo momento i documenti non possono essere modificati, annullati o sostituiti. La sostituzione può essere effettuata soltanto creando una nuova versione del documento.

Conservazione della distinta

In questa fase, per ciascun pacchetto, che in questa fase assume la denominazione di pacchetto di archiviazione, il sistema genera secondo lo standard *SInCRO* **un indice del pacchetto** di archiviazione, vale a dire un file XML in cui sono elencati i documenti inclusi nel pacchetto, con le relative chiavi di ricerca e l'impronta di *hash*.

Il processo si conclude con l'apposizione della firma del Responsabile della Conservazione e della Marca Temporale sull'indice del pacchetto di archiviazione. Con questa operazione la distinta assume lo stato di "conservata".

I documenti conservati, il manuale della conservazione e il mandato di affidamento (o prospetto delle tipologie di documento da conservare) possono essere masterizzati su diversi tipi di supporto e consultati da qualsiasi supporto.

5.2.2 - Il manuale della conservazione e gli altri documenti del conservatore

Il sistema supporta l'operatore nella redazione del manuale. Il documento informatico è redatto sulla base di un modello standard che fornisce una traccia di base per la compilazione del documento, con la possibilità di modificare i dati proposti. Il manuale è firmato e conservato digitalmente.

Oltre al Manuale della Conservazione, il sistema consente di predisporre, archiviare e firmare i seguenti documenti che fanno capo al soggetto conservatore:

- il mandato di affidamento della Conservazione Digitale;
- il prospetto delle tipologie documento da conservare;
- l'atto di nomina del responsabile della conservazione;
- la delega delle attività del responsabile della conservazione.

I documento sono archiviati in formato pdf e firmati digitalmente e conservati in modalità digitale.

5.2.3 - Modalità di conservazione in outsourcing

Nel caso di conservazione in outsourcing, il sistema permette di configurare i parametri necessari per l'integrazione automatica con il fornitore del servizio, che assume il ruolo di responsabile della conservazione e assicura l'espletamento degli adempimenti.

Creazione della distinta di conservazione

La creazione della distinta avviene in modo del tutto simile alla creazione in house, con la differenza che in outsourcing il sistema richiede l'indicazione del produttore del servizio outsourcing, ovvero il soggetto abilitato a caricare e consultare i documenti inviati al sistema di conservazione.

Invio della distinta in conservazione

Quando la distinta è inviata in conservazione, il sistema verifica se tutti i documenti sono correttamente firmati ed eventualmente provvede alla firma massiva di tutti i documenti.

Con l'invio in conservazione della distinta, il sistema:

1. esegue un controllo preventivo sui documenti da inviare in conservazione (documento firmato, validità della firma, certificato scaduto, ecc.);
2. genera i pacchetti di versamento sul portale del fornitore del servizio outsourcing, raggruppando i documenti della distinta in base alle regole definite dal fornitore, e restituisce l'esito dell'invio.

La fase di invio in conservazione determina il "blocco" dei documenti presenti in distinta.

Conservazione della distinta

In questa fase, a carico del fornitore del servizio, il sistema di conservazione esegue le operazioni di chiusura dei pacchetti di versamento ricevuti e mette a disposizione i relativi rapporti di versamento.

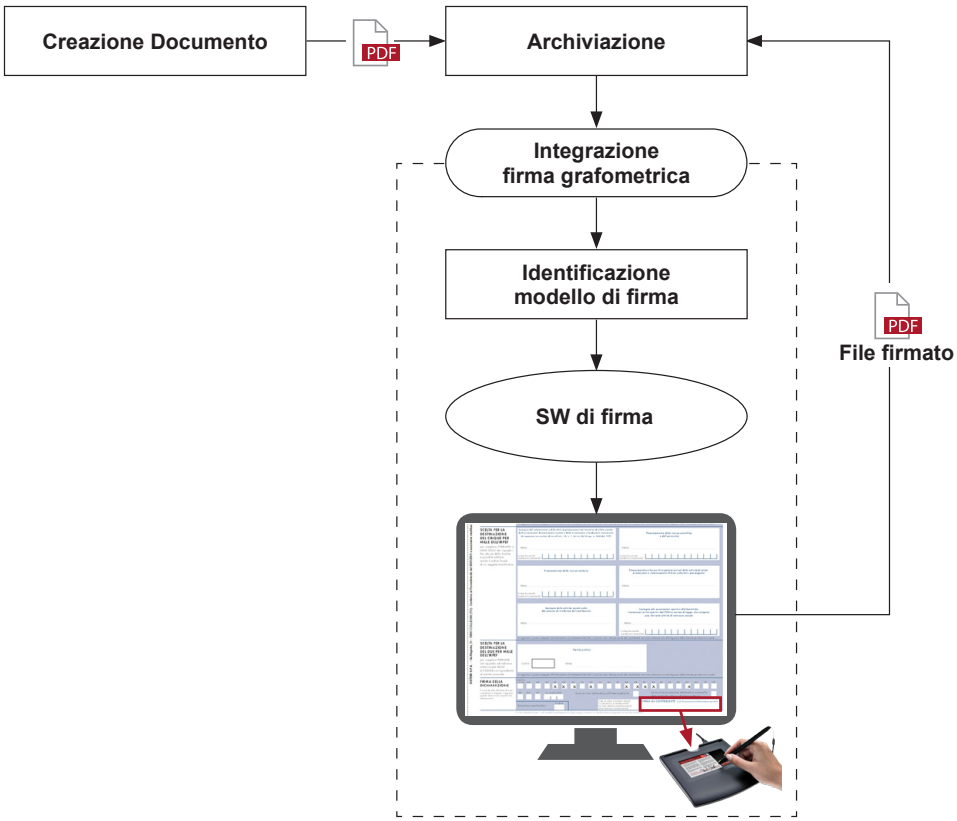
I rapporti di versamento, scaricabili direttamente dalla distinta di conservazione, sono automaticamente archiviati nel sistema.

Quando tutti i documenti risultano conservati, la procedura appone automaticamente lo stato di "conservato" sulla distinta.

5.3 - La firma grafometrica

Il sistema è progettato per gestire il processo di firma elettronica semplice o avanzata in base a quanto definito dal Codice dell'Amministrazione Digitale (CAD) ed in conformità con il "provvedimento generale prescrittivo in tema di biometria" del Garante della Privacy. Sui documenti archiviati è possibile raccogliere firme autografe, utilizzando un dispositivo (tablet) collegato al PC, mediante il software di firma.

Figura 32. ***Flusso di lavoro per la gestione della firma grafometrica***

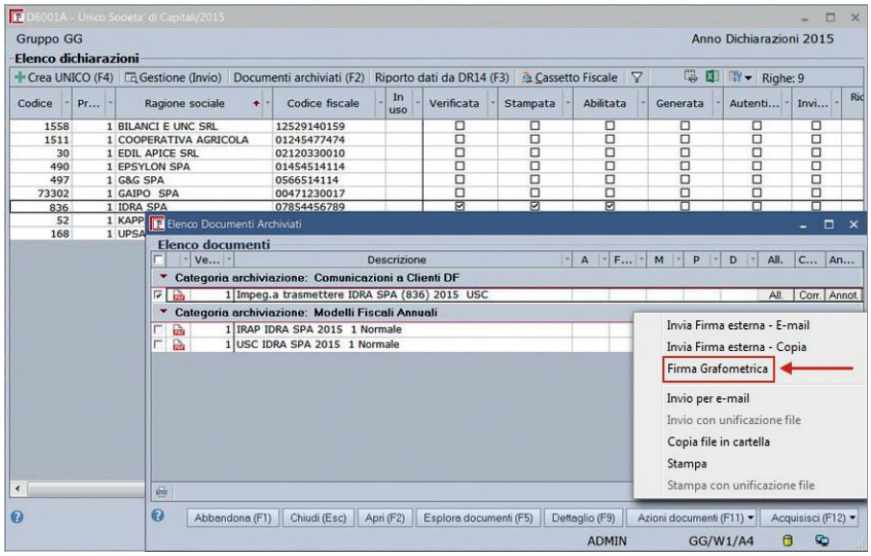


Il sistema guida il soggetto firmatario nell'apporre la firma sulla base di un modello che posiziona il cursore nel punto esatto.

Grazie all'integrazione con il processo di firma è possibile disporre del documento firmato

da archiviare ed eventualmente conservare, senza transitare dalla carta, cioè senza stamparlo, firmarlo manualmente, scansionarlo e archiviarlo.

Figura 33. ***Integrazione con la Gestione Documentale Sistemi***



In conclusione, la firma grafometrica risulta quindi un ulteriore strumento a supporto della digitalizzazione nelle aziende e negli studi professionali.

CAPITOLO 6

FAQ

Le presenti FAQ sono state raccolte nel corso di seminari o pervenute tramite e-mail.

6.1 - Conservazione digitale

Domanda

Ho terminato la conservazione digitale del libro giornale e mi sono accorto dopo qualche giorno che ho sbagliato. Posso rifare il processo?

Risposta

Sì, se si è entro i termini di conservazione è sempre possibile rifare il processo.

Domanda

È vero che posso conservare in solo formato digitale anche i libri sociali obbligatori?

Risposta

Sì, a norma dell'art.2215/bis del Codice civile è ammissibile conservare in solo formato digitale anche i libri sociali obbligatori, quali ad esempio il libro delle adunanze e delle deliberazioni delle assemblee, il libro delle adunanze e delle deliberazioni del consiglio di amministrazione, il libro delle adunanze e delle deliberazioni del collegio sindacale, etc.

Domanda

Mi conferma che dopo aver ultimato la conservazione digitale delle fatture di acquisto cartacee, è possibile procedere alla loro distruzione?

Risposta

Sì, dopo che il processo di conservazione digitale si è concluso, e cioè dopo che l'indice del pacchetto di archiviazione (SInCRO) è stato firmato digitalmente e marcato temporalmente dal responsabile della conservazione, è possibile procedere alla distruzione delle fatture di acquisto cartacee tramite per esempio triturazione, oppure macerazione.

6.2 - Regolamento eIDAS

Domanda

Ho una smart-card con firma digitale il cui certificato scade il 20 marzo del 2018, e mi chiedevo se con l'introduzione dal 1° luglio 2016 del regolamento eIDAS, devo sostituire il certificato di firma oppure posso continuare ad utilizzarlo sino alla sua scadenza?

Risposta

E' possibile continuare ad utilizzare il certificato di firma sino alla sua scadenza, dato che a norma dell'art.51 secondo comma del regolamento eIDAS *"I certificati qualificati rilasciati a persone fisiche a norma della direttiva 1999/93/CE sono considerati certificati qualificati di firma elettronica a norma del presente regolamento fino alla loro scadenza"*.

Domanda

La società in cui lavoro è una Spa che emette fatture elettroniche ai clienti in formato PDF e con firma digitale, ed ora che vi è il sigillo digitale introdotto dal regolamento eIDAS, pensavamo di utilizzarlo per "sigillare" le fatture elettroniche. Ritiene sia una scelta corretta?

Risposta

Ritengo che la decisione sia corretta, dato che l'impiego da parte delle persone giuridiche del sigillo digitale nei processi di fatturazione elettronica consente di avere una presunzione di autenticità ed integrità dei dati trasmessi, così come contemplato dall'art.35 secondo comma del regolamento eIDAS, ove rileva che un sigillo digitale *"gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico qualificato è associato"*.

Domanda

Quanti sono e chi sono i gestori SPID a cui è possibile richiedere il rilascio dell'identità digitale per accedere ai servizi dell'Agenzia delle Entrate, di INPS, e dell' INAIL?

Risposta

Ad oggi i gestori dell'identità digitale SPID sono tre, e cioè InfoCert SpA, Poste Italiane SpA e Telecom Italia Trust Technologies Srl, rilevando che da un comunicato stampa dell'AgID datato 23 luglio 2016, da settembre 2016 saranno attivi altri due gestori e cioè Aruba PEC Spa e Sielte Spa.

6.3 - La digitalizzazione dei DDT

Domanda

Mi conferma che il DDT può non essere sul mezzo durante la consegna del bene e può essere spedito tramite email?

Risposta

Sì, il DDT può non essere sul mezzo durante la consegna della merce e può essere trasmesso per email purchè trasmesso entro il giorno in cui è iniziato il trasporto del bene

Domanda

Posso conservare i DDT di vendita insieme alle fatture di vendita creando un unico file?

Risposta

No, dato che sono due diverse tipologie documentali, e quindi è necessario conservarle separatamente.

Domanda

Posso conservare alcuni DDT di vendita in formato digitale ed altri in formato cartaceo? Dovrei tenere due distinte serie di numerazione?

Risposta

E' possibile conservare alcuni DDT di vendita in formato digitale ed altri in formato cartaceo, ma in questi casi è necessario istituire due distinte serie di numerazione progressive: una numerazione con riferimento ai DDT conservati su carta ed una diversa numerazione con riguardo ai DDT conservati in digitale.

6.4 - PEC e firma grafometrica

Domanda

È vero che con la PEC non posso trasmettere messaggi in modalità “Ccn”?

Risposta

Sì, con la PEC non è possibile trasmettere messaggi a destinatari nascosti tramite la funzionalità “Ccn”.

Domanda

Sono un collega Dottore Commercialista, e mi chiedevo se posso usare il tablet (firma grafometrica conforme alla firma elettronica avanzata) per la firma dei clienti sulla copia intermediario della dichiarazione redditi, dato che andrò poi a conservarle in solo formato digitale?

Risposta

Sì, è una procedura corretta e da consigliare.

Domanda

Posso trasmettere tramite email documenti con firme grafometriche oppure vi è il rischio

che i dati grafometrici contenuti vengano intercettati ed utilizzati fraudolentemente da malintenzionati?

Risposta

Se i dati grafometrici sono stati inseriti nel documento informatico dopo che sono stati cifrati tramite l'ausilio di un sistema di cifratura asimmetrica (e.g. RSA), non vi è alcun rischio che vengano decifrati ed utilizzati in modo fraudolento.

CAPITOLO 7

Principali riferimenti normativi

7.1 - Conservazione digitale

DPR 26 ottobre 1972 n.633 *Istituzione e disciplina dell'imposta sul valore aggiunto.*

Decreto legislativo 7 marzo 2005 , n. 82 *Codice dell'amministrazione digitale.*

Circolare dell'Agenzia delle Entrate n. 36/E del 6 dicembre 2006 *Decreto ministeriale 23 gennaio 2004 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione in diversi tipi di supporto.*

Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 *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.*

Decreto Ministero dell'Economia e delle Finanze del 17 giugno 2014 *Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.*

Circolare dell'Agenzia delle Entrate n. 18/E del 24 giugno 2014 *IVA. Ulteriori istruzioni in tema di fatturazione.*

7.2 - Regolamento eIDAS

Regolamento (UE) n. 910/2014 *del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.*

Decreto del Presidente del Consiglio dei Ministri del 24 ottobre 2014 *Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese.*

7.3 - La digitalizzazione dei DDT

Decreto del Presidente della Repubblica del 14 agosto 1996 n. 472 *Regolamento di attuazione delle disposizioni contenute nell'art. 3, comma 147, lettera d), della legge 28 dicembre 1995, n. 549, relativamente alla soppressione dell'obbligo della bolla di accompagnamento delle merci viaggianti.*

Circolare del Ministero delle finanze n. 225 del 16 settembre 1996 *D.P.R. 14 agosto 1996, n. 472, concernente la soppressione dell'obbligo di emissione della bolla di accompagnamento.*

Circolare del Ministero delle finanze n. 249 del 11 ottobre 1996 *D.P.R. 14 agosto 1996, n. 472 - Ulteriori chiarimenti in ordine alla soppressione dell'obbligo di emissione della bolla di accompagnamento.*

7.4 - PEC

Decreto del presidente della Repubblica 11 febbraio 2005 n. 68 *Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003 n.3.*

Decreto 2 novembre 2005 *Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata.*

7.5 - Firma grafometrica

Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71. (G.U. n. 117 del 21 maggio 2013).*

Figure

Acronimi

AIL	Autenticità, integrità e leggibilità
B2B	Business to Business
B2G	Business to Government
CAD	Decreto legislativo 7 marzo 2005 n.82, Codice dell'Amministrazione Digitale
CIE	Carta d'identità elettronica
CNS	Carta nazionale dei servizi
EDI	Electronic Data Interchange
ERP	Enterprise resource planning
FD	Firma digitale
FEA	Firma elettronica avanzata
FEQ	Firma elettronica qualificata
GED	Gestione elettronica documentale
IPdA	Indice del pacchetto di archiviazione
MT	Marca temporale
OTP	One time password
PA	Pubblica amministrazione
PdA	Pacchetto di archiviazione
PdD	Pacchetto di distribuzione
PdV	Pacchetto di versamento
PEC	Posta elettronica certificate
PEPPOL	Pan-European public procurement online
RT	Riferimento temporale
SaaS	Software as a service
SDI	Sistema di Interscambio
SPID	Sistema pubblico per la gestione dell'identità digitale
UBL	Universal business language

Sistemi S.p.A. è una società italiana leader, che da 40 anni produce software per professionisti, imprese e associazioni.

Con i nostri Partner, sempre aggiornati e vicinissimi agli Utenti è capillarmente presente in tutta Italia e per questo conosce a fondo le esigenze di commercialisti, consulenti del lavoro, avvocati e piccole e medie imprese.

La sua missione è quella di offrire ai suoi 30.000 Utenti Soluzioni, semplici ed efficaci, frutto di una tecnologia di alta qualità, sviluppata tutta all'interno dell'azienda; di una conoscenza profonda delle esigenze e dei problemi dell'utenza; di una vicinanza e di una assistenza continue; di una grande esperienza e di un continuo aggiornamento in tempo reale.

Il rapporto con l'Utente è improntato alla massima trasparenza. **www.sistemi.com**

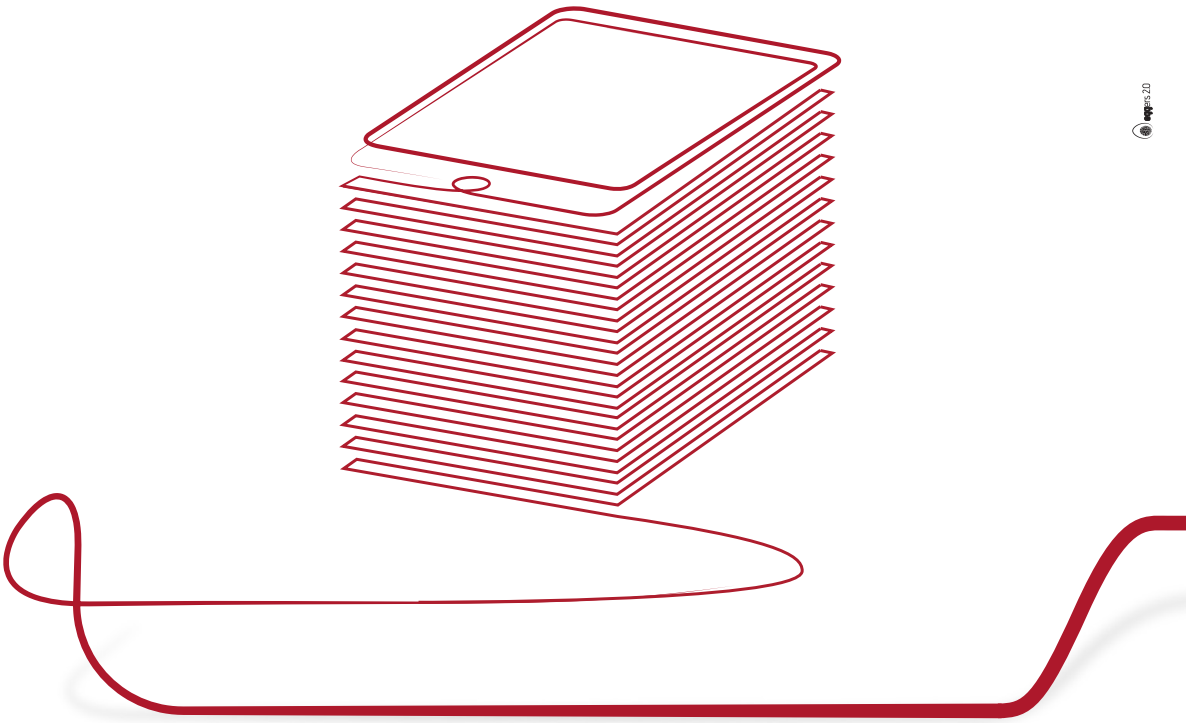
Umberto Zanini

Dottore Commercialista e Revisore Legale, Chartered Accountant in England and Wales, svolge dal 1993 la professione occupandosi principalmente di aspetti normativi, tecnici e gestionali delle nuove tecnologie informatiche e telematiche, e di nuovi modelli di business che dette innovazioni consentono di introdurre nei processi logistici, amministrativi e finanziari delle aziende.

Responsabile dal 2006 delle attività di ricerca tecnico-normativo dell'*"Osservatorio fatturazione elettronica e dematerializzazione"* della School of Management del Politecnico di Milano, e componente degli Osservatori *"Professionisti & Innovazione digitale"* e *"Supply Chain Finance"*, è relatore in numerosi convegni e seminari, oltre che autore di elaborati, approfondimenti e studi.

Da anni a fianco di Sistemi S.p.A. con attività di consulenza e seminari di formazione rivolti a commercialisti ed aziende in ambito digitalizzazione dei documenti, cura da luglio 2014 la sezione Digitalizzazione del portale www.sistemiamolitalia.it

Molta carta in meno, molta efficienza in più.



Le fatture diventano digitali.

sistemiamo l'Italia

Basta con le pile di fogli di carta: la fattura elettronica B2B è un'opportunità che farà risparmiare tempo nell'imputazione dei dati e lascerà più spazio al controllo e all'analisi del business, con un grande guadagno in termini di efficienza. Noi di Sistemi siamo pronti ad offrire alle aziende il modo di beneficiare di questa novità e ai commercialisti la possibilità di rimanere un punto cardine nella mediazione tra le imprese e l'Agenzia delle Entrate. Un'efficienza che si integra in tutte le nostre soluzioni.

eSOLVER: soluzione gestionale progettata per le imprese di diversi settori che necessitano di un sistema informativo per gestire le attività amministrative, controllare la gestione e automatizzare i processi aziendali.

PROFIS: insieme di applicazioni progettate per soddisfare le esigenze degli studi professionali che erogano servizi di consulenza amministrativa, gestionale e fiscale.

PROFIS/az: la contabilità condivisa in cloud, tra studio e azienda. Con PROFIS/az sia l'azienda sia lo studio accedono in rete allo stesso sistema gestionale condiviso, senza duplicazione di dati e di documenti.

Metteteci alla prova, chiamate noi o il più vicino dei nostri Partner.
Insieme a voi per lavorare, produrre, creare e innovare, perché solo insieme sistemiamo l'Italia.

www.sistemiamolitalia.it

sistemi®
Professione Informatica

www.sistemi.com

www.sistemiamolitalia.it

sistemi®
Professione Informatica

www.sistemi.com