#CANTIERI DELLA PA DIGITALE

DOCUMENTI DIGITALI | REPORT 2018

FPA

DIGITAL360

La redazione del report 2018 del Cantiere Documenti digitali
è stata curata da un gruppo di lavoro coordinato da Maria Guercio (Anai), con il supporto di Eleonora Bove (FPA).

I contenuti del report rappresentano il risultato del lavoro di rielaborazione degli spunti emersi nel corso del dibattito tra tutti i protagonisti del Cantiere.

CANTIERI DELLA PA DIGITALE
Cantiere Documenti digitali - Report 2018 - Edizioni ForumPA – ISBN 9788897169581

Finito di impaginare: Febbraio 2019
con il contributo di:

DEDAGROUP PUBLIC SERVICES

Gruppo Filippetti

DOCUMENTI DIGITALI | REPORT 2018

INDICE

L'iniziativa Cantieri della PA

Lanciati nel 2016, i Cantieri sono i laboratori permanenti di FPA dedicati ai temi dell'innovazione digitale e organizzativa della PA italiana, nati con l'obiettivo di monitorare e supportare i percorsi di cambiamento nelle principali aree verticali e trasversali del processo di digitalizzazione della pubblica amministrazione, attraverso attività di analisi, networking, comunicazione e advocacy.

I Cantieri operano attraverso tavoli di lavoro che mirano ad individuare i principali ostacoli all'attuazione dell'innovazione, analizzando criticità comuni, opportunità e possibili soluzioni. Non un'indagine quantitativa, ma un'analisi basata sull'esperienza quotidiana dei protagonisti dell'innovazione, pubblici e privati. Tavoli di confronto che integrano soggetti, approcci epistemologici e interessi differenti in un ambiente realmente collaborativo, ma strutturato.

I Cantieri aggregano le community dei più autorevoli operatori pubblici e privati responsabili dell'attuazione dei processi di innovazione della PA italiana. Nell'arco dei primi tre anni di vita dell'iniziativa sono stati attivati 10 tavoli di lavoro e realizzati 76 incontri a porte chiuse, che hanno visto la partecipazione di 430 operatori, tra cui 388 dirigenti pubblici provenienti da 95 differenti amministrazioni (30 centrali, 65 locali), 42 accademici ed esperti della digital trasformation e 37 imprese e grandi aziende sponsor.

Ogni Cantiere è orientato alla costruzione di relazioni e partnership tra amministratori, dirigenti pubblici e rappresentanti delle aziende partner per contribuire al processo di attuazione della strategia digitale italiana. Gli incontri in presenza si alternano con momenti di riflessioni e confronto sulla piattaforma di knowledge sharing e community management di FPA, che ospita gli oltre 500 contenuti prodotti, tra documenti di approfondimento, dossier e post. La comunicazione e l'attività di analisi e l'approfondimento dei temi trattati dai tavoli di lavoro viene ospitata sul sito cantieripadigitale.it, che ospita video interviste e contributi a firma dei protagonisti dei tavoli di lavoro, raccoglie buone pratiche ed esperienze realizzate dalle amministrazioni e dalle aziende aderenti all'iniziativa. I contenuti prodotti vengono veicolati attraverso una newsletter settimanale, rivolta a una community di oltre 70.000 operatori.

Al termine del ciclo annuale di attività, ogni Cantiere produce un report pubblico contenente una serie raccomandazioni rivolte ai decisori politici, ai responsabili delle

diverse policy verticali e trasversali e a tutte le amministrazioni italiane, ad ogni livello. Le raccomandazioni possono consistere in indicazioni di metodo, punti di attenzione o in vere e proprie linee guida per facilitare l'effettiva attuazione dei processi di innovazione della PA.

Introduzione

di **Maria Guercio**, Presidente ANAI e coordinatore del Cantiere Documenti digitali

Il rapporto 2018 del Tavolo Cantieri Documenti digitali è ricco di ben tre impegnativi e corposi documenti dedicati tutti a questioni cruciali nella fase ormai matura di trasformazione digitale che impegna le amministrazioni pubbliche italiane. I rapporti affrontano rispettivamente i seguenti temi:

1. *Qualità dei software di gestione documentale: i requisiti archivistici*
2. *Il fascicolo informatico nella gestione documentale*
3. *Prova di identità, firma e sigillo elettronico*

Sebbene ritenuti da tutti gli interlocutori del Tavolo (e non solo) di estrema rilevanza, si tratta tuttavia di nodi tutt'altro che risolti o, comunque, affrontati in passato senza l'approfondimento che la loro complessità e rilevanza avrebbero richiesto. Le ragioni di questi ritardi sono diverse. In parte (è il caso del documento dedicato alla prova di identità, firma e sigillo elettronico) sono dovute alle continue modifiche che hanno a lungo caratterizzato il quadro normativo in questo settore e hanno reso poco conclusivo il lavoro di analisi delle disposizioni che si sono in questi anni sedimentate in materia di documento informatico, identità digitale, formazione e gestione di sistemi documentari. In parte (è il caso degli altri due rapporti, intitolati rispettivamente alla qualità archivistica dei software di gestione documentale e al fascicolo informatico nella gestione documentale) è la natura stessa dei problemi da considerare ad aver rallentato la loro soluzione: si tratta infatti di aspetti di natura metodologica o di rilievo operativo che richiedono necessariamente un confronto multi- e interdisciplinari, che nel nostro Paese fatica a realizzarsi compiutamente.

L'iniziativa di FPA, condotta nel 2018 d'intesa con l'Associazione nazionale archivistica italiana, ha permesso di superare le criticità legate alla mancanza di occasioni di condivisione grazie alla partecipazione di decine di amministrazioni pubbliche e di alcune imprese e alla presenza dei principali interlocutori istituzionali cui è affidata l'azione di supporto normativo e di tutela nel settore specifico della gestione documentale (Agenzia per l'Italia digitale, Direzione generale degli archivi, Istituto centrale degli archivi, Archivio centrale dello Stato). Contemporaneamente, il consolidarsi dell'impianto normativo (inclusi i regolamenti europei 679/2016 sulla protezione dei dati personali e 910/2014

eIDAS) ha consentito di affrontare in modo sistematico e approfondito il nodo della prova di identità esaminato dal punto di vista specifico della fruizione di documenti informatici.

Senza entrare nel merito dei singoli contributi qui pubblicati, la cui natura tecnica richiede una lettura attenta e approfondita, in questa sede introduttiva ci limitiamo a sottolineare la specificità del metodo di lavoro seguito, non diverso da quello sperimentato nella edizione del 2017. In particolare:

- si sono definiti (nell'ambito dell'intesa tra Forum PA e Anai) i temi su cui concentrare l'attenzione dei partecipanti a partire da una riflessione congiunta con i portatori di interesse nel settore;
- si sono raccolte le adesioni dei diversi interlocutori, che sono stati sollecitati ad aderire ai diversi *focus group* sulla base dei propri interesse e delle proprie competenze;
- si sono identificati *obiettivi sostenibili e operativi* per ciascun gruppo di lavoro;
- i gruppi hanno operato *in parallelo* usufruendo della piattaforma digitale di FPA ma anche attraverso l'adozione di autonome e flessibili forme di interazione;
- per ogni gruppo sono stati individuati i *coordinatori* (anche più d'uno in ragione della particolare complessità del tema e alla luce della disponibilità dei partecipanti al tavolo);
- ogni incontro in seduta plenaria (quattro in tutto) ha previsto la *discussione condivisa dei risultati parziali* raggiunti da ciascun gruppo.

Merita sottolineare che il numero dei partecipanti è cresciuto nel corso dell'anno e che tutti gli incontri hanno visto una larga presenza degli enti e degli esperti che hanno aderito originariamente all'iniziativa. Nelle more della conferma della prosecuzione del lavoro nel 2019 (sia di alcune attività che richiedono ulteriori approfondimenti sia di nuove proposte da attivare) i partecipanti del gruppo di lavoro sul fascicolo informatico hanno chiesto all'Anai di proseguire gli incontri. Sono tutti elementi che testimoniano l'interesse che gli argomenti hanno suscitato e continuano a suscitare tra gli esperti di gestione documentale, gli interlocutori istituzionali e le amministrazioni pubbliche. Personalmente credo che tra gli elementi che hanno assicurato il successo del Tavolo ha contato molto la decisione di affrontare i temi oggetto di analisi attraverso il diretto e continuo confronto con tutti i partecipanti, garantendo flessibilità nei modi ma anche occasioni concrete e aperte di condivisione. L'esperienza maturata quest'anno costituisce, del resto, una prosecuzione di un precedente progetto, che si è dovuto arrestare per mancanza di risorse e di strumenti

operativi, il progetto Recap[1], il cui obiettivo era proprio la creazione di una rete di collaborazione nel campo degli archivi digitali.

Come nel caso di Recap, anche il Tavolo Cantieri Documenti digitali ha l'ambizione di promuovere e sostenere un percorso condiviso che consenta a chi partecipa di lavorare insieme, superando "la natura tradizionalmente episodica dello scambio di esperienze, nella speranza che da tutto il materiale via via accumulato sia possibile (anche al di là della durata del progetto specifico) 'estrarre' o aggiornare infrastrutture concettuali in grado di diventare veri e propri strumenti di lavoro, utilizzabili nell'interpretazione di situazioni, problemi, possibilità o nella formulazione di nuovi interrogativi di ricerca, una sorta di sedimentazione di un *know how* condiviso, relativamente formalizzato, affidato alla produzione di strumenti diversi"[2]. In questo specifico caso, i documenti resi disponibili non solo forniscono un quadro di riferimento sullo stato dell'arte, ma in tutti e tre i casi propongono soluzioni operative, casi concreti di applicazione, checklist per la valutazione delle infrastrutture e delle piattaforme applicative esistenti.

Queste iniziative, nei fatti più che nelle ambizioni, hanno sostenuto e nutrito la comune determinazione di quanti da tempo – almeno da due decenni – si dedicano allo sviluppo di modelli e soluzioni qualificate nel campo della gestione documentale, nonostante la disattenzione e l'inconsapevolezza che l'alta dirigenza pubblica e i responsabili nazionali delle politiche di digitalizzazione hanno spesso mostrato verso settori e competenze senza il cui supporto la trasformazione digitale è solo un'espressione retorica.

[1] Recap – Rete per la conservazione e l'accesso ai patrimoni digitali. Cfr *Rete di archivi per gli archivi in rete*, a cura di Gianfranco Crupi e Mariella Guercio, Roma, Edizioni Anai, 2017.
[2] M. Guercio, *Una comunità di pratiche per gli archivi digitali: questioni aperte e nuove prospettive*, in *Rete di archivi per gli archivi in rete*, cit., p. 30.

1. Qualità del software di gestione documentale: requisiti archivistici

capitolo a cura di[3]

Nel panorama organizzativo delle Pubbliche amministrazioni il sistema di gestione documentale costituisce ormai un punto di passaggio obbligatorio nella riflessione che ciascuna è chiamata a fare in relazione all'insieme degli elementi strutturali, strumentali ed organizzativi che consentono di produrre e gestire correttamente il proprio patrimonio documentario, che a sua volta costituisce strumento privilegiato di dialogo con il cittadino, oltreché fondamentale strumento di lavoro. E nello scenario digitale che caratterizza in modo sempre più pregnante l'operatività della PA italiana la componente tecnologica gioca un ruolo cruciale, specialmente in considerazione del fatto che spesso le maggiori criticità connesse al cambio di paradigma (dall'analogico al digitale, dal manuale all'automatizzato) possono essere ricondotte ad una scarsa propensione al cambiamento, piuttosto che alla difficoltà di accompagnare adeguatamente il cambiamento stesso. In tale scenario risulta quindi indispensabile mettere a fuoco le esigenze e le difficoltà comuni delle PA e fornire loro uno strumento di lavoro utile per valutare quali siano i requisiti che una piattaforma di gestione documentale deve possedere per soddisfare le esigenze dell'amministrazione che la utilizza, rispondendo non solo agli obblighi imposti dalla normativa, ma anche alle funzionalità che possono aiutare l'operatore nell'espletare al meglio i propri adempimenti quotidiani.

In relazione ai *software* di gestione documentale, che ovviamente costituiscono il fondamentale supporto strumentale per l'operatività quotidiana, un sondaggio informativo condotto fra le PA coinvolte nel progetto ha consentito di individuare alcune esigenze comuni e trasversali, che possono essere così sintetizzate:

- versatilità di configurazione
- scalabilità
- modularità

[3] Loredana **Bozzi** (Provincia Autonoma di Trento), Anna **Ponti** (Università degli Studi dell'Insubria) e Armando **Tomasi** (Provincia Autonoma di Trento) (coordinatori), Elisabetta **Belloni** (Comune di Bergamo), Luca **Cicinelli** (InnovaPuglia), Giancarlo **Di Capua** (InnovaPuglia), Silvia **Ghiani** (Lepida Spa), Costantino **Landino** (Istituto centrale per gli Archivi), Antonio **Massari** (Dedagroup Public Services), Andrea **Presta** (Regione Friuli Venezia Giulia), Valeria **Sisti** (Dedagroup Public Services).

- adattabilità ad esigenze particolari
- possibilità di realizzare efficacemente l'interoperabilità interenti
- possibilità di utilizzo di *kit* aggiuntivi (ad esempio per la sottoscrizione, anche massiva e/o automatica, di documenti)
- possibilità di gestire agilmente assegnazioni di visibilità sui documenti
- interfacciamento con i sistemi di conservazione documentale
- automatismo nel confezionamento dei pacchetti di archiviazione
- possibilità di gestione dei flussi documentali e dei procedimenti amministrativi (nonché dei processi ad essi collegati)
- integrazione con gli applicativi verticali
- gestione automatica delle funzioni di protocollazione e classificazione
- agevole e efficiente gestione (produzione e scambio) dei *files* di grandi dimensioni
- efficiente interfacciamento con i portali *on line*
- differenziazione delle interfacce e delle funzionalità a seconda delle necessità delle varie categorie di utilizzatori
- possibilità di tipizzare i documenti dotandoli di set di metadati aggiuntivi e caratterizzanti

Di qui l'opportunità di elaborare uno strumento che sia in grado di indirizzare le PA verso soluzioni tecnologiche adeguate alle proprie esigenze (oltreché – naturalmente – in linea con gli obblighi di norma), mediante l'individuazione di requisiti funzionali chiari e inequivocabilmente riconducibili all'operatività quotidiana, contestualizzati all'interno di un solido quadro concettuale di riferimento, e accompagnati da uno strumento di valutazione degli stessi che consenta di attribuire a ciascun requisito il giusto valore in relazione alle specifiche esigenze delle amministrazioni.

Lo strumento elaborato può servire alle PA per "fotografare lo stato dell'arte" dei sistemi di gestione documentale in uso, nonché per misurare quanto essi si discostino eventualmente rispetto al pieno soddisfacimento delle necessità e per indirizzare verso scelte che colmino le lacune e le problematiche ancora aperte.

1.1 Il modello concettuale di riferimento[4]

Prima di addentrarsi nella definizione dei requisiti risulta però necessario dedicare qualche riflessione ad un modello di riferimento al cui interno risulta vantaggioso declinare lo strumento che si intende proporre.

[4] Paragrafo a cura di Antonio **Massari** e Valeria **Sisti**, Dedagroup Public Services.

1.1.1 L'evoluzione dei sistemi di protocollo informatico e gestione documentale: architettura modulare e monolitica

I sistemi di protocollo informatico e di gestione documentale per la pubblica amministrazione si sono evoluti nel corso degli ultimi 20 anni sulla base delle indicazioni normative e sulla base della progressiva adozione del documento digitale. Al giorno d'oggi esistono numerose implementazioni di sistemi che hanno accompagnato le amministrazioni nella trasformazione verso il documento digitale durante questo lungo periodo. Diversi sistemi attualmente in uso hanno visto la nascita nei primi anni di entrata in vigore delle normative di riferimento ovvero i primi anni duemila. In ogni caso si è assistito ad una evoluzione di sistemi che, oltre a rispondere agli obblighi normativi, tendevano a realizzare molte funzioni che, pur se non strettamente obbligatorie, risultavano fondamentali per consentire una efficace adozione dei documenti digitali. Tra queste si citano: funzioni di assegnazione, smistamento e "movimentazione" digitale dei documenti, funzioni per facilitare i processi di apposizione di firme digitali o elettroniche, funzioni per la gestione coordinata ed integrata dei messaggi di posta elettronica sia ordinaria che certificata, funzioni orientate alla trasparenza anche verso i cittadini e le imprese.

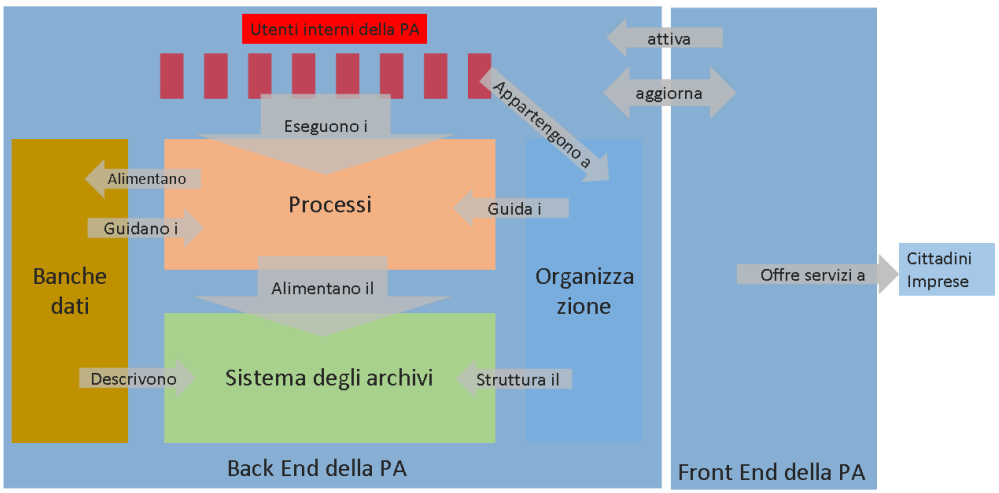
Questa evoluzione a macchia d'olio delle funzioni attribuite ai sistemi di protocollo e gestione documentale non ha corrisposto, il più delle volte, ad un adeguato aggiornamento architetturale delle soluzioni informatiche. Nonostante le indicazioni date dall'Autorità per l'Informatica nella Pubblica Amministrazione in uno dei primi documenti di indirizzo sul tema gestione documentale (GEDOC2[5]), orientate alla definizione di architetture modulari, ancora oggi sono presenti numerosi sistemi che, pur rispondendo egregiamente alle esigenze operative delle amministrazioni, presentano una architettura di tipo "monolitico" dove l'insieme delle funzioni offerte è realizzato come evoluzioni da un nucleo iniziale con una unica base dati ed un unico modello concettuale comprensivo di elementi che dovrebbero avere dignità autonoma.

1.1.2 Il modello di riferimento per la classificazione dei requisiti

L'obiettivo di definire una metodologia condivisa di valutazione delle piattaforme documentali non può prescindere dalla definizione di un modello di riferimento, ispirato al principio di modularità, dove inquadrare i requisiti, non tanto di un unico singolo sistema software, ma di un insieme dei sistemi che complessivamente contribuiscono alla corretta gestione documentale, nel rispetto delle normative e seguendo le linee guida per la trasformazione digitale. Nella figura seguente viene illustrata una proposta di ripartizione dei principali blocchi funzionali che entrano in gioco durante l'esecuzione delle attività

[5] capitolo 5

svolte dalle pubbliche amministrazioni che danno luogo alla registrazione e produzioni di documenti:



La prima principale ripartizione a cui si vuole fare riferimento è quella tra *back end* e *front end*.

1.1.3 Il front end

Per *front end* della PA si intende quell'insieme di moduli, sistemi e funzionalità il cui scopo principale è la comunicazione sia dall'interno verso l'esterno dell'ente che viceversa. Rientrano in questa categoria i portali per la trasparenza, i portali o le applicazioni per l'inoltro di istanze alla PA, i portali di servizi o più in generale per comunicare in via telematica. Grazie alla diffusione di SPID e grazie alle recenti innovazioni del CAD i cittadini potranno sempre di più interagire con la PA in modo nativamente digitale e la sola autenticazione con SPID potrà, in taluni casi, costituire elemento sufficiente per conferire validità ad una comunicazione. Tipicamente sui sistemi di *front end* verranno presentati dati o aggregazioni di dati che derivano dai sistemi di gestione documentale ai fini della trasparenza o per aggiornare lo stato di avanzamento di un procedimento amministrativo, mentre dai sistemi di *front end* potrà provenire l'*input* per l'attivazione di un nuovo procedimento amministrativo (es. istanza *on line*). Tantissime altre invece potranno essere le funzioni tipiche di un sistema di *front end* che non hanno relazione alcuna con la gestione documentale, o per lo meno la gestione documentale ufficiale dell'ente, come ad esempio pagine informative o sistemi di CRM.

1.1.4 Il back end

Il *back end* della PA rappresenta quell'insieme di sistemi e servizi che complessivamente sono a supporto della esecuzione delle attività amministrative e che vedono come attori principali gli utenti interni della PA stessa. Storicamente il *focus* di tutti i sistemi di gestione

documentale è concentrato sul *back end*. Il modello proposto prevede una ripartizione del *back end* in quattro ulteriori ambiti: il sistema degli archivi, l'operatività (intesa come l'insieme delle attività collegate all'espletamento di processi e/o procedimenti amministrativi), le banche dati e l'organizzazione.

1.1.5 Il sistema degli archivi

Il sistema degli archivi è il cuore di tutto il modello, e rappresenta l'insieme delle funzionalità che consentono la registrazione, la descrizione, la organizzazione dei *documenti ufficiali* dell'ente, i documenti che ne costituiscono l'archivio. Il sistema degli archivi è l'insieme di tutte le componenti applicative necessarie per rappresentare i documenti e le informazioni ufficialmente registrate dall'ente. Il sistema degli archivi astrae un modello concettuale ben noto e derivante dalla tradizione archivistica italiana. Documenti registrati con registrazione di protocollo o di repertorio o altra forma di registrazione, file rappresentanti specifici contenuti, metadati anche dipendenti dalle tipologie documentarie, informazioni sulla provenienza, allegati, versioni di un contenuto di cui si vuole mantenere traccia, collegamenti tra documenti, catene documentarie, fascicoli procedimentali, sottofascicoli, metadati e dati di registrazione associati ai fascicoli, *log* delle operazioni effettuate associati agli oggetti, dati relativi alla persistenza del documento archivistico (derivanti o calcolabili dal massimario di conservazione), dati sulla classificazione archivistica associata a documenti o fascicoli, dati sulla visibilità, sulla riservatezza e sulla *privacy* ecc. Nel corso degli anni innumerevoli modelli sono stati proposti ed implementati ispirandosi ai concetti sommariamente descritti. Purtroppo la mancanza di un unico schema di riferimento standard ha dato origine a modelli non sempre riconducibili l'uno all'altro o modelli con una profonda differenza come livello di dettaglio delle rappresentazioni. Tra i modelli più evoluti come possibilità di rappresentazione dei documenti archivistici e delle relazioni si citano il modello concettuale del P.I.Tre (della Provincia Autonoma di Trento) e quello di Doc.Er (della Regione Emilia Romagna).

Sarà responsabilità del sistema degli archivi garantire registrazioni formalmente valide (tra cui quella di protocollo), accessibilità alle informazioni registrate secondo regole di visibilità stabilite, sicurezza, accessibilità alle informazioni anche sul lungo periodo, diritto all'oblio, coerenza dell'insieme complessivo dei documenti archivistici e delle loro relazioni, efficienza nell'accesso e pulizia complessiva dell'archivio anche attraverso il ricorso alle operazioni di cancellazione controllata e verificata dei documenti non più necessari (scarto d'archivio).

Il sistema degli archivi è costituito da più componenti: in particolare dall'archivio corrente, dall'archivio di deposito e da quello storico (che pure fa riferimento a organizzazioni e responsabilità diverse rispetto agli altri due), le cui definizioni, scopi e modalità di funzionamento sono patrimonio comune della prassi archivistica italiana. La quasi totalità dei sistemi informatici nati per la gestione documentale e il protocollo informatico nei primi anni 2000 si sono concentrati esclusivamente sull'archivio corrente, ponendo non pochi

problemi, col passare degli anni, nella minimizzazione dei costi di esercizio, o nella gestione dei costi derivanti da riorganizzazioni a fronte di archivi la cui dimensione era sostanzialmente monotona crescente, o nei processi di versamento su sistemi caratterizzati da costi di esercizio minori, o nel tentativo di applicare politiche di eliminazione di documenti non più necessari.

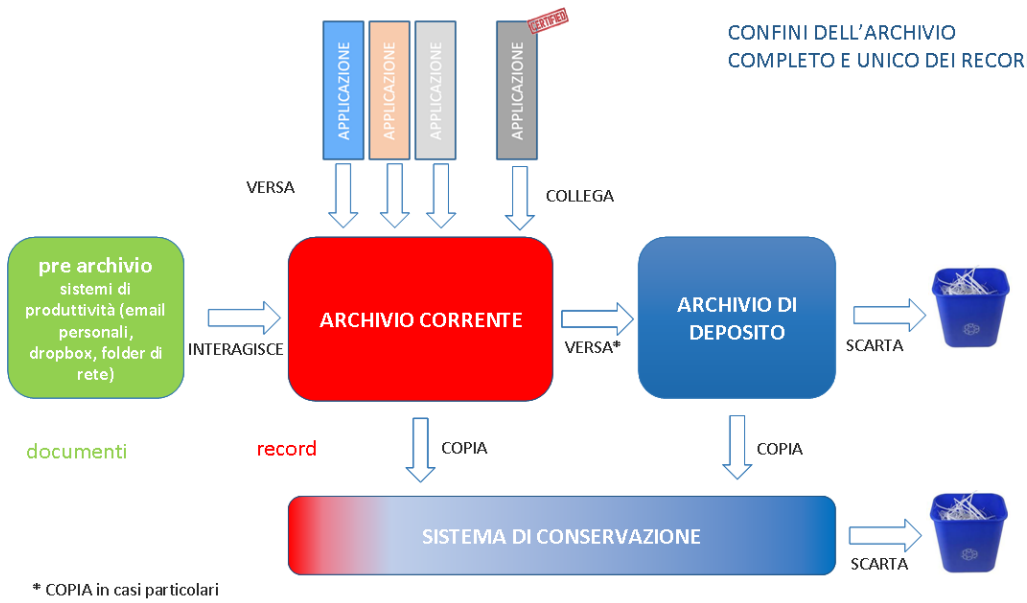
Accanto a questa suddivisione classica, con l'introduzione del documento nativo digitale, si è venuto ad aggiungere un nuovo archivio, ovvero l'archivio costituito dai documenti inviati in conservazione. Alla prova dei fatti nessuna delle definizioni "classiche" si adatta perfettamente a descrivere questo archivio. Può accadere infatti che un documento ancora nella fase attiva venga inviato in conservazione e che venga mantenuto ancora sul sistema corrente, oppure che il documento inviato in conservazione perda, nel versamento, numerose informazioni come la relazione con i fascicoli o con gli altri documenti dell'archivio o altri metadati. La possibilità di inviare un documento in conservazione presso operatori privati esterni all'amministrazione e la frequente mancanza di precisi standard di rappresentazione, impediscono di fatto di considerare il sistema di conservazione digitale come un vero e proprio archivio, ma piuttosto viene ad assumere un ruolo di *repository* di sicurezza dove memorizzare, a cura di una terza parte fidata, documenti dei quali l'amministrazione deve garantire, anche davanti all'autorità giudiziaria, integrità, leggibilità, collocazione temporale e autenticità nel tempo.

Risulta pertanto centrale nella definizione dell'insieme dei requisiti di un sistema di gestione documentale per le pubbliche amministrazioni definire con esattezza il ruolo di ciascun archivio e il ciclo di vita dei documenti. Ad esempio, nel caso in cui si consideri il sistema di conservazione come mero *repository* di sicurezza, sarà indispensabile affiancare al sistema che rappresenta l'archivio corrente un secondo sistema che svolga il ruolo di archivio di deposito per fare in modo che il sistema corrente possa avere dei costi di esercizio contenuti, *performances* sempre adeguate e minimizzare le complessità dovute alle riorganizzazioni. Nel caso in cui l'amministrazione decida di sviluppare un sistema di conservazione *in house*, strettamente coordinato, sia come modello concettuale di riferimento che come gestione del ciclo di vita del documento, con il sistema corrente, allora il sistema di conservazione potrà con ogni probabilità assumere anche il ruolo di archivio di deposito rendendo pertanto non necessaria la definizione di un sistema specifico dedicato per questa fase del ciclo di vita del documento.

Comunque sia articolato il sistema degli archivi esso dovrà, nella sua interezza e unitarietà, rappresentare l'unico luogo dove un ente dovrà registrare i propri documenti. Il sistema degli archivi dovrebbe essere elevato al rango di *archivio unico* dell'ente fornendo all'amministrazione e ai suoi interlocutori, cittadini e imprese, uno strumento formidabile di certezza, efficienza e trasparenza. Le condizioni per rendere il sistema degli archivi un *archivio unico* sono sì di natura tecnica (esistenza di interfacce programmative per collegare applicativi verticali ed altri potenziali detentori di informazioni registrabili), ma

soprattutto deve esistere una ferma volontà da parte del vertice dell'amministrazione. Un *archivio unico* si ottiene con la volontà organizzativa (e con il budget adeguato!) piuttosto che con uno strumento tecnologico, che può essere solo un mezzo abilitante. Per rendere un archivio unico sarà necessario emanare delle opportune direttive a livello organizzativo che necessariamente dovranno dare luogo a interventi di tipo evolutivo sulla quasi totalità dei sistemi *software* esistenti all'interno di un ente per fare in modo che, in presenza di un documento da registrare, tali documenti vengano ottenuti attraverso invocazione di interfacce applicative con il sistema degli archivi. In piccola parte questo già avviene con la registrazione di protocollo: tutti i sistemi di protocollo esistenti espongono interfacce programmative per consentire agli applicativi verticali di "staccare il numero" sul registro ufficiale e garantire l'ufficialità di un passaggio amministrativo che prevede l'interazione con l'esterno. Non tutti i sistemi, tuttavia, vanno oltre la mera registrazione di protocollo, non fornendo al sistema di gestione documentale tutte le altre informazioni fondamentali per l'alimentazione dell'archivio come (ad esempio) il documento stesso o le relazioni con gli altri documenti o le informazioni per la classificazione o la fascicolazione. Non in tutte le realtà, infine, il sistema di protocollo e gestione documentale viene usato consapevolmente per gestire tutte le altre forme di registrazione formale, quali deliberazioni, determinazioni o altri atti repertoriati, creando in tal modo una sorta di barriera invalicabile tra archivi indipendenti gestiti con sistemi diversi e pressoché nessuna possibilità di preservare il vincolo archivistico nel tempo.

Nella figura seguente si mostra una possibile ripartizione in sottocomponenti del sistema degli archivi che realizza il concetto di archivio unico:



1.1.6 L'operatività

Con il termine "operatività" si intende l'insieme di tutte le funzionalità offerte agli utenti interni della PA per svolgere efficacemente le loro operazioni. I sistemi che supportano gli utenti nello svolgimento delle attività lavorative potranno essere di tipo collaborativo o strutturato a seconda delle esigenze, delle tipologie di attività da svolgere, dei carichi di lavoro, dell'esistenza o meno di formalizzazioni o prassi consolidate. Nei sistemi di protocollo e gestione documentale classici una prima forma di gestione di micro processi era rappresentata dalle funzioni per la gestione delle assegnazioni dei documenti. I processi di assegnazione, smistamento, o altra forma di gestione dei flussi documentali hanno assunto le forme più diverse nelle varie implementazioni. Per esemplificare, volendo rimanere sul terreno della semplice assegnazione di un documento ricevuto non esiste, e non può esistere, un modello operativo standard in cui tutte le amministrazioni possano riconoscersi. Esistono casi in cui un'assegnazione necessita di una espressa accettazione, con conseguente restituzione all'assegnante, altri casi in cui ciò non è necessario, altri ancora in cui l'assegnante dopo un primo rifiuto può imporre d'autorità la presa in carico ecc.

Ciascuna amministrazione dovrà verificare, in relazione alle proprie complessità interne e necessità organizzative quali siano gli strumenti più adeguati per supportare al meglio la esecuzione delle attività dei propri uffici. Sta di fatto che mentre nel sistema degli archivi la necessità di organizzare, registrare, strutturare i documenti ufficiali resta un requisito pressoché invariante, anzi un requisito da preservare e ribadire anche con disposizioni di livello strategico (ad esempio la istituzione del concetto di *archivio unico*), nel mondo dell'operatività ci si trova di fronte ad una realtà in forte trasformazione, dove quindi la individuazione di precisi requisiti funzionali appare più sfuggente.

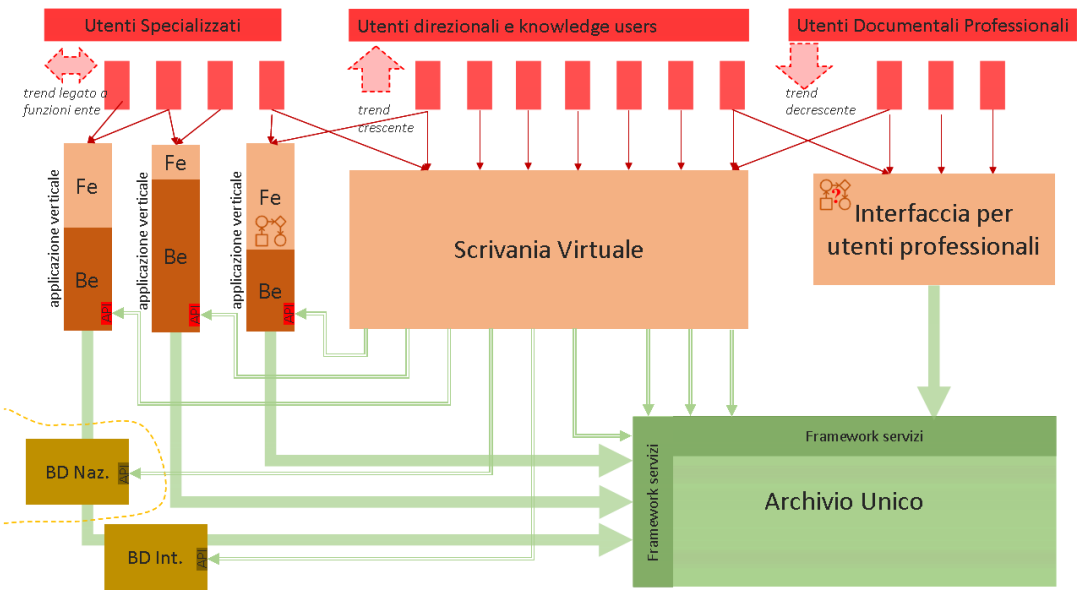
All'inizio degli anni 2000 le registrazioni riguardavano per la quasi totalità documenti cartacei ed erano effettuate da operatori umani. Questo ha dato luogo alla definizione di funzionalità degli applicativi di protocollo di ausilio a questi scenari, come ad esempio: riproposizione di dati nel caso di protocollazione di documenti simili, funzioni di modellizzazione di assegnazioni per velocizzare operazioni ripetitive, oppure funzioni di annullamento o modifica conservativa delle informazioni facenti parte dei documenti immodificabili. Nello scenario attuale questi modelli operativi sono, fortunatamente, in via di superamento. Le operazioni di registrazione, classificazione e fascicolazione, ad esempio, potranno essere svolte in modo del tutto automatico se le informazioni provengono da un portale di servizi *on line* esposto dall'amministrazione dove il cittadino, scegliendo un servizio e fornendo le informazioni necessarie per la sua attivazione, implicitamente forma il documento che rappresenta l'istanza di richiesta, lo firma, lo invia, questo viene protocollato, classificato, fascicolato ed assegnato al responsabile del procedimento.

Il campo dell'operatività va quindi interpretato come una entità logica dove trovano collocazione tutte le funzioni operative che vengono utilizzate dagli utenti interni dell'ente

per lo svolgimento di attività che possono alimentare in qualche modo il sistema degli archivi. All'interno di questo ambito potranno essere collocati sistemi con caratteristiche completamente differenti. Funzionalità per la registrazione "vecchio stile" per supportare le operazioni manuali da parte di utenti specializzati (protocollatori, strutture di segreteria), funzionalità più orientate alla supervisione e controllo o al lavoro collaborativo con la presenza di scrivanie virtuali e *dashboard* di controllo, funzioni associate alla lavorazione di procedimenti amministrativi a prevalente caratterizzazione documentale (workflow documentali), funzioni immerse in applicativi verticali esistenti dedicati alla gestione di procedimenti complessi. Tutte queste categorie di funzionalità potrebbero appartenere a sistemi diversi, ma dovranno essere tutte accomunate dalla necessità di interagire in modo coordinato con il sistema degli archivi.

Come estremizzazione del concetto, il sistema degli archivi potrebbe non avere alcuna interfaccia utente ed essere raggiungibile esclusivamente attraverso la invocazione di API, lasciando agli applicativi verticali, ai sistemi per utenti specializzati o alle scrivanie virtuali il compito di offrire le necessarie funzionalità per la gestione efficace delle attività lavorative interne, vale a dire i processi.

Nella figura seguente si presenta una possibile ripartizione logica in sottocomponenti del modulo Operatività dove vengono evidenziate tre possibili tipologie di sistemi: applicazioni verticali, scrivanie virtuali ed interfacce per utenti specializzati:



1.1.7 Le banche dati

Nella definizione ed evoluzione dei sistemi di protocollo e gestione documentale ci si è presto resi conto che, oltre agli archivi documentali, giocavano un ruolo essenziale elenchi controllati ed informazioni strutturate, inizialmente funzionali solo alla corretta registrazione, ricerca e classificazione dei documenti (rubriche, elenchi, tipologie, classi…), ma che con il tempo hanno iniziato ad assumere un ruolo di risorse informative con una valenza autonoma: vere e proprie banche dati di informazioni strutturate spesso frutto di dettagliatissime e preziose attività di censimento ed analisi effettuate a partire non solo dall'analisi della produzione documentale ma soprattutto dall'analisi delle funzioni svolte dall'ente, dalle normative di riferimento e dai regolamenti. Come è anche accennato nel citato documento di indirizzo GEDOC2, tali banche dati dovrebbero assumere una valenza autonoma e non risiedere all'interno dei sistemi monolitici.

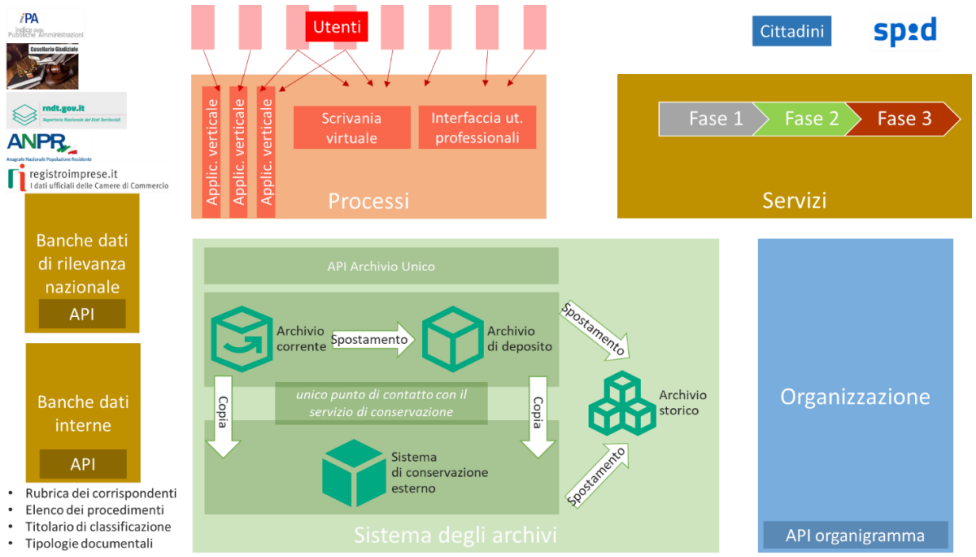
Oltre a quelle che potremmo definire banche dati interne evolute dai sistemi di gestione documentale, che includono rubriche dei mittenti e dei destinatari, titolario di classificazione, elenco dei procedimenti amministrativi, tipologie documentali e tipologie di fascicoli, potranno essere utilizzate nell'ambito della metadatazione e descrizione dei documenti tutte le fonti di dati strutturati presenti all'interno dell'ente e derivanti da fonti ufficiali di qualsiasi tipo. A titolo di esempio di citano: dati relativi a beni immobili, dati relativi a località geografiche, dati relativi ad oggetti gestiti e censiti per qualunque motivo dall'amministrazione.

In aggiunta alle banche dati interne sarà possibile utilizzare tutto il patrimonio informativo della pubblica amministrazione italiana, che sarà via via reso disponibile attraverso interfacce programmative standard, relativo alle cosiddette banche dati di rilevanza nazionale (ANPR, Casellario giudiziale ecc.).

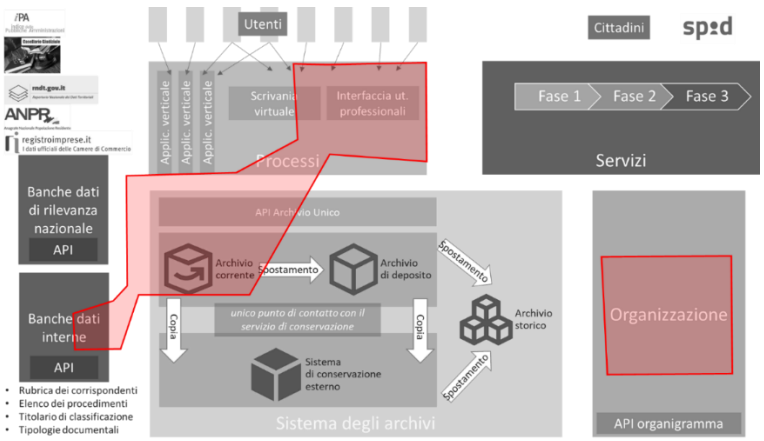
1.1.8 L'organizzazione

Di fondamentale importanza in ogni sistema di protocollo e gestione documentale è la disponibilità di una corretta ed aggiornata rappresentazione della struttura organizzativa dell'ente. L'organigramma e il funzionigramma vengono utilizzati nei sistemi per determinare la visibilità dei documenti presenti in archivio, individuare i possibili flussi documentali, partizionare le rubriche, assegnare e bilanciare i carichi di lavoro, definire i profili funzionali ecc. In alcuni sistemi la ricchezza informativa associata all'organigramma/funzioningramma ha assunto un valore tale da non poter essere più considerata come risorsa informativa asservita alla sola funzione di supporto per la gestione documentale ma occorre che venga elevata al rango di informazione primaria da mettere a disposizione di tutti i sistemi interni dell'ente.

Nella figura seguente si illustra il modello complessivo ad un maggiore livello di dettaglio:



Con riferimento al modello generale proposto, nella figura successiva si illustrano infine i confini dei primi sistemi di gestione documentale e protocollo informatico, tipicamente caratterizzati da un'architettura monolitica. In particolare in tali sistemi vengono coperte tutte le funzionalità associate all'archivio corrente, le funzioni relative ai processi di supporto alle attività per utenti professionali (protocollatori , strutture di segreteria ecc.) qualche funzione per utenti direzionali assimilabile ad una forma di scrivania virtuale, funzionalità relative alla rappresentazione della struttura organizzativa (organigramma) e alcune banche dati interne per la gestione di rubriche, il titolario, le tipologie documentali e elenchi di procedimenti amministrativi:



1.2 La checklist

Allo scopo di fornire alle Amministrazioni un elenco di sintesi delle funzionalità delle quali un sistema di gestione documentale deve essere dotato, nonché uno strumento utile per capire il grado di rispondenza del sistema stesso alle esigenze, è stata predisposta una *checklist*; essa è stata elaborata basandosi sul presupposto di base di limitare l'analisi ai requisiti del sistema di gestione documentale, ignorando volutamente gli aspetti relativi a requisiti più generali, non funzionali, quali ad esempio quelli relativi alla sicurezza sistemistica, all'architettura ed allo sviluppo del *software*.

Poiché il numero dei requisiti identificati è considerevole (169), si propone un criterio di lettura basato sul seguente ordinamento:

- requisiti relativi all'area funzionale Sistema degli archivi
- requisiti relativi all'area funzionale Organizzazione
- requisiti relativi all'area funzionale Operatività
- requisiti relativi all'area funzionale Servizi ai cittadini, imprese e altre PA
- requisiti relativi all'area funzionale Banche dati.

All'interno di ogni area funzionale sono riportati in testa i requisiti *ex lege*, se esistenti, e successivamente gli altri. La sequenza proposta è tuttavia soltanto un suggerimento: è possibile riordinare i requisiti tenendo conto di caratteristiche diverse, a seconda delle informazioni che il singolo ente vorrà far emergere. La tabella è articolata in 5 colonne principali:

- la prima colonna, denominata "Numero requisito", riporta il numero sequenziale del requisito e serve per identificarlo univocamente;
- la seconda colonna, denominata "Tipo", è valorizzata con l'informazione *ex lege* quando il requisito è obbligatorio, in quanto derivato in via diretta dalla normativa, mentre è vuota nel caso in cui il requisito non sia obbligatorio ma derivi da esigenze organizzative, funzionali, operative, ecc.;
- la terza colonna, denominata "Aree funzionali", è utilizzata per assegnare i requisiti ad una delle cinque aree individuate dal modello: Sistema degli archivi, Organizzazione, Operatività, Servizi ai cittadini, imprese e altre PA e Banche dati;
- la quarta colonna, denominata "Categorie", individua la categoria di appartenenza del requisito.
- la quinta colonna, denominata "Descrizione requisito", contiene la formulazione sintetica dei requisiti.

Per ogni area funzionale sono state definite le possibili categorie, secondo lo schema seguente:

Sistema degli archivi	archivio di deposito
	archivio storico
	conservazione
	fascicoli
	gestione massimario conservazione e scarto
	serie archivistiche
Organizzazione	assegnazione e gestione ruoli
	assegnazione funzioni e visibilità
	gestione delle sostituzioni
Operatività	assegnazione documenti per la lavorazione
	gestione dei fascicoli
	gestione dei workflow
	gestione delle informazioni aggiuntive di profilo per tutte le categorie di documenti (tipizzazione)
	gestione documenti non protocollati
	gestione protocollo d'emergenza
	gestione scambio informazioni con altri applicativi (integrazione con altre PA e con verticali di settore)
	monitoraggio e statistiche
	predisposizione dei versamenti in conservazione
	predisposizione dei registri accessi foia
	predisposizione documento (versioni, firme elettroniche e digitali)
	produzione registro giornaliero protocollo e repertori
	registrazione
	ricerche documenti e fascicoli
	tracciabilità accessi e modifiche

Servizi ai cittadini, imprese e altre PA	canali di comunicazione: portale, PEC, IS. Interoperabilità
	domicilio digitale e gestione delle ricevute
	gestione dati personali e sensibili secondo la normativa privacy GDPR
	gestione delle ricerche relative ai propri procedimenti
	uso tecnologie nell'attività amministrativa
	visibilità
Banche dati	altre basi dati di supporto
	anagrafica degli utenti interni
	anagrafica dei corrispondenti
	anagrafica dei ruoli
	elenco procedimenti
	gestione documenti vitali
	struttura organizzativa (raggruppamenti funzionali)
	tipologie documentali
	titolario

1.2.2 La composizione[6]

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
1	Ex lege	Sistema degli archivi	serie archivistiche	Possibilità di creare aggregazioni su base cronologica o numerica all'interno di serie di documenti omogenei

[6] Nella presente versione la checklist è priva della colonna relativa ai riferimenti normativi, presente invece nella versione elettronica del documento, del quale costituisce un allegato

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
2	Ex lege	Sistema degli archivi	archivio di deposito	Possedere funzioni che consentano la consultazione dei documenti ad altre PA. Deve essere possibile definire nel sistema le diverse amministrazioni procedenti e i limiti di accesso per ogni amministrazione procedente identificata.
3	Ex lege	Sistema degli archivi	archivio di deposito	Consentire l'estensione della consultabilità ai fini storici anche della parte attiva e semiattiva degli archivi con l'identificazione delle sole parti che sono state richieste per la consultazione.
4	Ex lege	Sistema degli archivi	archivio storico	Consentire di gestire unitariamente la componente analogica e quella digitale dell'archivio, in unico sistema in quanto l'archivio non può essere smembrato in componenti separate, né tra analogico e digitale, né delle diverse componenti digitali (per es. tra più conservatori digitali).
5	Ex lege	Sistema degli archivi	conservazione	Consentire l'integrazione con il sistema di conservazione mediante funzioni che consentano di predisporre pacchetti di versamento nel rispetto della struttura dei documenti e dei fascicoli nell'archivio corrente e di eventuale annullo degli stessi e funzioni per la ricerca e l'estrazione di documento versati, anche in archivio di deposito e storico

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
6	Ex lege	Sistema degli archivi	fascicoli	Prevedere che i documenti possano essere raccolti in fascicoli con un insieme minimo di metadati: identificativo (classificazione e numero), amministrazione produttrice, amministrazioni partecipanti al procedimento, responsabile del procedimento, data di apertura e chiusura, oggetto, elenco dei documenti contenuti
7	Ex lege	Sistema degli archivi	gestione massimario conservazione e scarto	Gestire le informazioni relative al piano di conservazione associato al piano di classificazione in modo da consentire le operazioni di selezione ai fini dell'eliminazione legale una volta decorsi i termini e il passaggio da archivio di deposito ad archivio storico (e quindi liberamente consultabile) delle componenti soggette a conservazione permanente.
8	Ex lege	Sistema degli archivi	serie archivistiche	Mantenere informazione di ciò che è stato trasferito in archivio di deposito e storico
9		Sistema degli archivi	archivio di deposito	Prevedere la produzione ed il mantenimento nell'archivio di deposito di un elenco di versamento dettagliato per ogni versamento effettuato.
10		Sistema degli archivi	conservazione	Possibilità di collegamenti con più conservatori accreditati
11		Sistema degli archivi	conservazione	Disponibilità di connettori certificati con conservatori accreditati
12		Sistema degli archivi	conservazione	Possibilità di selezionare i metadati da inviare in conservazione

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
13		Sistema degli archivi	conservazione	Possibilità di collegare pacchetti di conservazione relativi a documenti e fascicoli inviati più volte in conservazione
14		Sistema degli archivi	conservazione	Possibilità di definire, memorizzare ed inviare in conservazione metadati e dati di log
15		Sistema degli archivi	conservazione	Possibilità di inviare in conservazione i metadati relativi alle istanze di workflow
16		Sistema degli archivi	conservazione	Possibilità di definire informazioni di contesto per la conservazione (intellectual entities Premis)
17		Sistema degli archivi	fascicoli	Possibilità di classificare documenti o fascicoli a qualunque livello di titolario
18		Sistema degli archivi	fascicoli	Possibilità di gestire sottofascicoli ed inserti
19		Sistema degli archivi	fascicoli	Presenza dei metadati minimi del fascicolo informatico o della aggregazione documentale informatica, elencati nell'allegato 5 del DPCM 3 dicembre 2013
20		Sistema degli archivi	fascicoli	Possibilità di definire metadati che connettano fascicoli e documenti associati a diverse voci di titolario (iperfascicolo)
21		Sistema degli archivi	fascicoli	Presenza di un ambiente separato (archivio di deposito) per i documenti appartenenti a fascicoli e serie chiuse

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
22		Sistema degli archivi	fascicoli	Possibilità di gestire vari stati di un fascicolo
23		Sistema degli archivi	fascicoli	Possibilità di accedere al fascicolo con visualizzazione "Storica"
24		Sistema degli archivi	gestione massimario conservazione e scarto	Possibilità di tracciare eventuali variazioni sulle tempistiche di conservazione di documenti e fascicoli
25		Organizzazione	Assegnazione e gestione ruoli	Possibilità di consentire l'accesso al sistema ed alle informazioni solo agli utenti abilitati
26		Organizzazione	Assegnazione e gestione ruoli	Possibilità di riallineare le visibilità documentali a seguito di modifiche di organigramma/funzionigramma
27		Organizzazione	Assegnazione e gestione ruoli	Possibilità di storicizzare organigramma documentale/funzionigramma
28		Organizzazione	assegnazione funzioni e visibilità	Possibilità di differenziazione della visibilità sul titolario in base al ruolo funzionale dell'utente
29		Organizzazione	assegnazione funzioni e visibilità	Possibilità di differenziazione della visibilità documentale in base al ruolo funzionale dell'utente
30		Organizzazione	gestione delle sostituzioni	Possibilità di gestione di deleghe e sostituzioni
31	Ex lege	Operatività	registrazione	Consentire, per ogni documento che lo prevede, la registrazione ad un albo, repertorio o registro particolare, compreso il registro di protocollo.
32	Ex lege	Operatività	registrazione	Consentire per ogni documento l'inserimento delle informazioni obbligatorie di cui all'art 53 c. 1 del dpr 445/00.

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
33	Ex lege	Operatività	gestione dei fascicoli	Possibilità di inserire documenti non protocollati nei fascicoli
34	Ex lege	Operatività	gestione protocollo d'emergenza	Consentire il recupero dei dati dal registro di emergenza, una volta ripristinate le funzionalità del sistema.
35	Ex lege	Operatività	gestione scambio informazioni con altri applicativi (integrazione con altre PA e con verticali di settore)	Creazione automatica del file di segnatura comprensivo delle informazioni minime previste per l'interoperabilità tra Pa
36	Ex lege	Operatività	monitoraggio e statistiche	Consentire la possibilità di elaborazioni statistiche sulle informazioni registrate
37	Ex lege	Operatività	monitoraggio e statistiche	Consentire il tracciamento delle modifiche delle informazioni trattate e l'individuazione dell'autore.
38	Ex lege	Operatività	predisposizione dei versamenti in conservazione	Predisporre pacchetti di versamento per l'invio in conservazione di registri, documenti, fascicoli e aggregazioni documentali.
39	Ex lege	Operatività	produzione registro giornaliero protocollo e repertori	Consentire la produzione del registro giornaliero di protocollo e di ogni tipo di registro/repertorio/albo previsto dall'amministrazione e garantirne l'immodificabilità.

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
40	Ex lege	Operatività	registrazione	Garantire, in fase di registrazione, la gestione dei legami archivistici tra il documento registrato, gli altri documenti e i fascicoli. Il sistema di gestione informatica dei documenti deve garantire la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita in modo da fornire, ad esempio, informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali.
41	Ex lege	Operatività	gestione dei fascicoli	Garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato e del relativo repertorio dei fascicoli
42	Ex lege	Operatività	registrazione	Non consentire la modifica delle informazioni attribuite in automatico in sede di registrazione, ma solo l'annullamento della registrazione stessa.

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
44	Ex lege	Operatività	registrazione	Nell'effettuare l'operazione di registrazione dei documenti informatici l'impronta deve essere calcolata per ciascun documento associato alla registrazione. La funzione crittografica di hash da impiegare per la generazione dell'impronta deve essere conforme alle specifiche AgID.
45	Ex lege	Operatività	registrazione	Le regole che valgono per la registrazione di protocollo devono valere anche per la registrazione in tutti gli altri registri, repertori, albi ecc.
46	Ex lege	Operatività	ricerche documenti e fascicoli	Consentire ricerche semplici e complesse, con operatori logici, basate su tutti i tipi di informazioni registrate
47	Ex lege	Operatività	tracciabilità accessi e modifiche	Consentire la gestione degli accessi e il tracciamento delle modifiche.
48	Ex lege	Operatività	tracciabilità accessi e modifiche	Possibilità di modificare/revocare abilitazioni per ruoli/utenti, anche con valenza retroattiva

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
49	Ex lege	Operatività	gestione dei fascicoli	Garantire l'immediata conoscibilità per via telematica dello stato di avanzamento del procedimento, del nominativo e del recapito elettronico del responsabile del procedimento
50	Ex lege	Operatività	gestione dei fascicoli	Consentire l'accesso ai fascicoli e la movimentazione dei documenti ivi contenuti alle amministrazioni esterne che ne hanno titolo (partecipanti al procedimento)
51	Ex lege	Operatività	gestione dei fascicoli	Prevedere funzioni di ricerca sui documenti che diano evidenza delle relazioni degli stessi con i fascicoli a cui appartengono.
52	Ex lege	Operatività	gestione dei fascicoli	Presenza di funzioni di ricerca per fascicolo che rendano evidente chi è il responsabile del procedimento e, qualora esistente un sistema di workflow, quale sia la fase del procedimento.
53	Ex lege	Operatività	gestione dei fascicoli	Consentire lo scambio di informazioni con sistemi per la gestione dei flussi documentali di altre amministrazioni al fine di determinare lo stato e l'iter dei procedimenti complessi.
54	Ex lege	Operatività	gestione dei fascicoli	Consentire di produrre informazioni statistiche sull'attività dell'ufficio (numero fascicoli aperti e numero fascicoli chiusi e, ove presenti meccanismi di workflow, quali siano le fasi).

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
55	Ex lege	Operatività	gestione dei fascicoli	Consentire ad ogni amministrazione di poter definire requisiti e modalità per la gestione per i fascicoli diversi da quelli definiti nell'art. 41 del CAD.
56	Ex lege	Operatività	registrazione	Gestione delle documentarie attribuendo loro un identificativo univoco persistente
57	Ex lege	Operatività	registrazione	Produzione del numero di protocollo come numero progressivo, costituito da almeno sette cifre numeriche. La numerazione deve rinnovarsi ogni anno solare.
58	Ex lege	Operatività	registrazione	Garantire la memorizzazione delle informazioni di cui all'art. 53, c. 1 del TUDA nella registrazione di protocollo
59	Ex lege	Operatività	registrazione	Consentire la produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.
60	Ex lege	Operatività	registrazione	L'assegnazione delle informazioni nelle operazioni di registrazione di protocollo effettuata in unica soluzione, con esclusione di interventi intermedi, anche indiretti, da parte dell'operatore, garantendo la completezza dell'intera operazione di modifica o registrazione dei dati

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
61		Operatività	assegnazione documenti per la lavorazione	Possibilità di visualizzare documenti a prescindere dal formato nativo
62		Operatività	gestione dei workflow	Possibilità di effettuare operazioni automatiche in base a passi di processo registrazione, fascicolazione, ecc)
63		Operatività	gestione dei workflow	Possibilità di configurare flussi di lavoro sulla base di regole predefinite
64		Operatività	gestione dei workflow	Possibilità di creare workflow con strumenti grafici: definizione dei processi, degli step, integrazione con le regole di accesso e visibilità, funzione di amministrazione.
65		Operatività	gestione dei workflow	Possibilità di modificare i workflow: iter dei processi, assegnazione, riallocazione
66		Operatività	gestione dei workflow	Possibilità di automatizzare l'esecuzione dei workflow
67		Operatività	gestione dei workflow	Possibilità di gestire schemi di processo differenziati per utente e per tipologia documentaria e relativi metadati
68		Operatività	gestione dei workflow	Possibilità di automatizzare aspetti della gestione e del ciclo di vita dei documenti
69		Operatività	gestione dei workflow	Possibilità di impostare notifiche a utenti, a seguito dell'effettuazione di operazioni automatiche
70		Operatività	gestione dei workflow	Possibilità di impostare azioni automatiche

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
71		Operatività	gestione dei workflow	Possibilità di gestire liste di controllo: passi propedeutici e di gestione dell'iter procedurale
72		Operatività	gestione dei workflow	Possibilità di gestire calendari e scadenzari
73		Operatività	gestione dei workflow	Versionamento automatico o semiautomatico di documenti in funzione di eventi nel sistema
74		Operatività	gestione dei workflow	Possibilità di impostare avvisi e notifiche collegate all'effettuazione di azioni su oggetti del sistema
75		Operatività	gestione documenti non protocollati	Possibilità di tracciatura dei documenti non registrati
76		Operatività	gestione protocollo d'emergenza	Possibilità di utilizzare un software di protocollo "di emergenza" sincronizzato con il sistema ufficiale di protocollo.
77		Operatività	gestione scambio informazioni con altri applicativi (integrazione con altre PA e con verticali di settore)	Possibilità di inserire informazioni aggiuntive nel file di segnatura ai fini dell'interoperabilità con altre Pa
78		Operatività	gestione scambio informazioni con altri applicativi (integrazione con altre PA e con verticali di settore)	Possibilità di gestire l'interazione con banche dati

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
79		Operatività	gestione scambio informazioni con altri applicativi (integrazione con altre PA e con verticali di settore)	Possibilità di interazione con software esterni che gestiscono particolari tipologie di documenti o flussi di lavoro *NOTA BENE: vedi anche Allegato 1 "Web services"*
80		Operatività	gestione scambio informazioni con altri applicativi (integrazione con altre PA e con verticali di settore)	Possibilità di interfacciamento con depositi digitali sicuri e certificati.
81		Operatività	gestione scambio informazioni con altri applicativi (integrazione con altre PA e con verticali di settore)	Possibilità di esportare entità del sistema (documenti, fascicoli, log, dati degli utenti, thesauri, workflow, ecc.)
82		Operatività	monitoraggio e statistiche	Possibilità di produrre report personalizzati ai fini di monitoraggio
83		Operatività	predisposizione dei versamenti in conservazione	Possibilità di attivare invii automatici di documenti in conservazione.

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
84		Operatività	predisposizione dei versamenti in conservazione	Possibilità di consolidamento del documento e dei metadati
85		Operatività	predisposizione dei versamenti in conservazione	Possibilità di generare pacchetti di archiviazione conformi alle regole dello standard ISO 14721
86		Operatività	predisposizione dei registri accessi foia	Possibilità di procedere all'estrazione dei registri delle richieste di accesso documentale e civico
87		Operatività	predisposizione documento (versioni, firme elettroniche e digitali)	Possibilità di apporre firme e marche temporali dall'interno del sistema
88		Operatività	predisposizione documento (versioni, firme elettroniche e digitali)	Possibilità di verificare la validità dei certificati di firma digitale e/o marche temporali e memorizzazione dell'esito.
89		Operatività	predisposizione documento (versioni, firme elettroniche e digitali)	Possibilità di generare documenti con Timbro Digitale
90		Operatività	predisposizione documento (versioni, firme elettroniche e digitali)	Possibilità di gestione dei metadati per ogni versione di documento
91		Operatività	predisposizione documento (versioni, firme elettroniche e digitali)	Possibilità di procedere al versionamento del documento e garanzia di tracciatura delle versioni

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
92		Operatività	registrazione	Consentire l'annullamento anche di un solo campo delle altre informazioni registrate in forma immodificabile (non assegnate automaticamente dal sistema), necessario per correggere errori intercorsi in sede di registrazione; le informazioni annullate devono rimanere memorizzate nella base di dati per essere sottoposte alle elaborazioni previste dalla procedura e non devono essere in alcun modo cancellate. L'annullamento deve comportare la rinnovazione del campo stesso con i dati corretti e la contestuale memorizzazione, in modo permanente, del valore precedentemente attribuito unitamente alla data, l'ora e all'autore della modifica.
93		Operatività	registrazione	Garanzia di immodificabilità delle registrazioni di protocollo
94		Operatività	registrazione	Possibilità di generare avvisi in caso di presenza di duplicati di documenti.
95		Operatività	registrazione	Possibilità di protocollare come singolo documento sia il messaggio e-mail sia i relativi allegati
96		Operatività	registrazione	Possibilità di gestire la procedura di annullamento di protocollo (con la relativa autorizzazione)
97		Operatività	registrazione	Possibilità di associare alle scansioni l'attestazione di conformità al documento analogico originale (rif. art.10 del DPCM 13 Novembre 2014)

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
98		Operatività	registrazione	Possibilità di attivazione di avviso per mancato completamento registrazione
99		Operatività	registrazione	Possibilità di estrarre dati e metadati dai documenti XML
100		Operatività	registrazione	Possibilità di attivazione di servizi di criptazione dei documenti e dei metadati
101		Operatività	registrazione	Garanzia di immodificabilità ed integrità del documento elettronico
102		Operatività	registrazione	Possibilità di attivazione di avvisi per formati di file non conformi
103		Operatività	ricerche documenti e fascicoli	Possibilità di eseguire ricerche full text
104		Operatività	ricerche documenti e fascicoli	Possibilità di salvataggio delle ricerche effettuate
105		Operatività	ricerche documenti e fascicoli	Possibilità di eseguire statistiche sulle ricerche effettuate
106		Operatività	ricerche documenti e fascicoli	Possibilità di conservare i log delle ricerche effettuate
107		Operatività	tracciabilità accessi e modifiche	Possibilità di certificare la cancellazione degli elementi dal sistema informatico
108		Operatività	tracciabilità accessi e modifiche	Possibilità di tracciare le modifiche ai metadati in caso di errore
109		Operatività	tracciabilità accessi e modifiche	Possibilità di tracciare e conservare i dati di protocollo annullati.

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
110		Operatività	tracciabilità accessi e modifiche	Possibilità di tracciare la movimentazione dei documenti nei fascicoli
111		Operatività	tracciabilità accessi e modifiche	Possibilità di tracciare le modifiche dei metadati dei fascicoli
112		Operatività	tracciabilità accessi e modifiche	Possibilità di generare log di sistema che permettano di tracciare tutte le azioni effettuate nel sistema
113		Operatività	tracciabilità accessi e modifiche	Immodificabilità dei log di sistema
114		Operatività	tracciabilità accessi e modifiche	Possibilità di esportazione dei log di sistema
115		Operatività	tracciabilità accessi e modifiche	Possibilità di conservazione dei log secondo policy
116		Operatività	gestione dei fascicoli	Possibilità di gestire ulteriori metadati associati al fascicolo rispetto a quelli definiti nelle regole tecniche;
117		Operatività	gestione dei fascicoli	Possibilità di formare aggregazioni e fascicoli a periodicità diversa (annuali, permanenti, ecc.)
118		Operatività	gestione delle informazioni aggiuntive di profilo per tutte le categorie di documenti (tipizzazione)	Possibilità di definire metadati aggiuntivi specifici per ente

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
119		Operatività	gestione dei fascicoli	Possibilità di accesso semplificato a fascicoli e documenti (preferiti)
120		Operatività	tracciabilità accessi e modifiche	Possibilità di gestire separatamente l'eliminazione logica e fisica di documenti
121		Operatività	gestione dei fascicoli	Gestione di un documento e fascicolo unico, condivisibile tramite link
122		Operatività	gestione dei fascicoli	Possibilità di gestire notifiche ed eventi su fascicoli e documenti.
123		Operatività	gestione dei fascicoli	Possibilità di caricamento di documenti e/o fascicoli estratti da altri sistemi
124		Operatività	gestione dei fascicoli	Possibilità di generare report di metadati dei documenti/fascicoli
125		Operatività	gestione dei fascicoli	Possibilità di collegare più schemi di metadati a documenti e fascicoli
126		Operatività	gestione dei workflow	Possibilità di gestire i procedimenti amministrativi mediante sistemi informativi automatizzati che interagiscano e interoperino con il sistema di gestione documentale
127	Ex lege	Servizi ai cittadini, imprese e altre Pa	canali di comunicazione: portale, PEC, IS. Interoperabilità	Gestire le comunicazioni fra PA mediante i canali della posta elettronica e della cooperazione applicativa
128	Ex lege	Servizi ai cittadini, imprese e altre Pa	canali di comunicazione: portale, PEC, IS. Interoperabilità	Gestione della segnatura in sede di inoltro in tutte le modalità previste dalla norma, incluse quelle opzionali (es. collocazione telematica, metadati aggiuntivi)

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
129	Ex lege	Servizi ai cittadini, imprese e altre Pa	domicilio digitale e gestione delle ricevute	Generazione delle ricevute di avvenuta presentazione dell'istanza
130	Ex lege	Servizi ai cittadini, imprese e altre Pa	Gestione dati personali e sensibili secondo la normativa privacy GDPR	Possibilità di marcare i documenti contenenti dati personali e/o sensibili
131	Ex lege	Servizi ai cittadini, imprese e altre Pa	Gestione dati personali e sensibili secondo la normativa privacy GDPR	Il sistema deve consentire agli utenti aventi apposito ruolo di ricercare tutte le informazioni riguardanti un soggetto e le relative caratteristiche del trattamento dati personali.
132	Ex lege	Servizi ai cittadini, imprese e altre Pa	Gestione dati personali e sensibili secondo la normativa privacy GDPR	Consentire la cancellazione (ad es. dall'anagrafica) e/o la limitazione del trattamento dei dati, se richieste dal cittadino, ferma restando l'integrità dell'archivio e senza perdita delle informazioni collegate agli oggetti documentali già esistenti.
133	Ex lege	Servizi ai cittadini, imprese e altre Pa	gestione delle ricerche relative ai propri procedimenti	Garantire l'accesso, ai singoli documenti e ai fascicoli dei procedimenti amministrativi da parte degli interessati, attraverso i servizi di cui agli articoli 40-ter e 64-bis nonché tramite gli strumenti di identificazione informatica di cui all'art. 65, comma 1 della L 241/1990.

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
134	Ex lege	Servizi ai cittadini, imprese e altre Pa	uso tecnologie nell'attività amministrativa	Qualora il sistema di gestione documentale consenta la presentazione di istanze attraverso uno specifico portale, questo deve necessariamente essere integrato con il sistema di identità digitale SPID
135	Ex lege	Servizi ai cittadini, imprese e altre Pa	gestione delle ricerche relative ai propri procedimenti	Gestire il fascicolo in modo da consentirne l'accesso dall'esterno per via telematica da parte dei soggetti che intendano esercitare il diritto di accesso
136		Servizi ai cittadini, imprese e altre Pa	canali di comunicazione: portale, PEC, IS. Interoperabilità	Possibilità di verificare automaticamente la validità della segnatura di protocollo
137		Servizi ai cittadini, imprese e altre Pa	canali di comunicazione: portale, PEC, IS. Interoperabilità	Possibilità di interfacciamento con caselle di posta elettronica, certificata e non.
138		Servizi ai cittadini, imprese e altre Pa	canali di comunicazione: portale, PEC, IS. Interoperabilità	Possibilità di gestire i metadati di spedizione
139		Servizi ai cittadini, imprese e altre Pa	canali di comunicazione: portale, PEC, IS. Interoperabilità	Possibilità di gestire le ricevute della posta elettronica certificata

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
140		Servizi ai cittadini, imprese e altre Pa	canali di comunicazione: portale, PEC, IS. Interoperabilità	Possibilità di monitorare la ricezione di documenti gestiti con canali diversi da PEC
141		Servizi ai cittadini, imprese e altre Pa	canali di comunicazione: portale, PEC, IS. Interoperabilità	Possibilità di utilizzare servizi di interoperabilità nella gestione del fascicolo (CAD, art. 41)
142		Servizi ai cittadini, imprese e altre Pa	canali di comunicazione: portale, PEC, IS. Interoperabilità	Possibilità di condividere fascicoli e documenti su area terza rispetto al gestore documentale
143		Servizi ai cittadini, imprese e altre Pa	domicilio digitale e gestione delle ricevute	Interfacciamento con i registri dei domicili digitali previsti dal CAD relativi alle persone fisiche e alle persone giuridiche per identificare i domicili digitali da utilizzare per l'invio dei documenti e delle ricevute.
144	Ex lege	Banche dati	anagrafica degli utenti interni	Consentire l'identificazione univoca degli utenti interni, attribuire abilitazioni differenziate (lettura, scrittura, ecc.)
145	Ex lege	Banche dati	anagrafica dei corrispondenti	Nell'anagrafica dei corrispondenti consentire la rettifica, l'aggiornamento e la cancellazione dei dati, con possibilità di scelta se storicizzare o meno, senza perdita delle informazioni collegate agli oggetti documentali già esistenti.
146	Ex lege	Banche dati	anagrafica dei ruoli	Consentire la gestione di una anagrafica dei ruoli e dei relativi profili di accesso, combinabili tra loro, con possibilità di ricerca, visualizzazione, inserimento, modifica, estrazione, stampa

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
147	Ex lege	Banche dati	struttura organizzativa (raggruppamenti funzionali)	Prevedere la possibilità di censire l'articolazione dell'amministrazione per uffici
148	Ex lege	Banche dati	tipologie documentali	Il sistema deve consentire la creazione di tipologie documentarie e di associarvi metadati, quali ad esempio i tempi di conservazione previsti dal massimario di scarto.
149	Ex lege	Banche dati	titolario	Prevedere la possibilità di gestire uno o più titolari nelle AOO che costituiscono ciascuna amministrazione.
150		Banche dati	altre basi dati di supporto	Utilizzo di lessici archivistici per definire ontologie di metadati
151		Banche dati	altre basi dati di supporto	Conservazione dei dati di gestione e monitoraggio delle autenticazioni
152		Banche dati	altre basi dati di supporto	Possibilità di generare liste dei formati ammessi
153		Banche dati	altre basi dati di supporto	Possibilità di generazione di oggettari
154		Banche dati	altre basi dati di supporto	Possibilità di generazione di notari
155		Banche dati	altre basi dati di supporto	Possibilità di utilizzare modelli per la creazione di documenti standard

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
156		Banche dati	anagrafica dei corrispondenti	Possibilità di gestire liste di destinatari
157		Banche dati	anagrafica dei corrispondenti	Possibilità di gestire anagrafiche di corrispondenti
158		Banche dati	gestione documenti vitali	Possibilità di definire documenti e fascicoli vitali con separato backup e operazioni indipendenti e distinte di recupero
159		Banche dati	struttura organizzativa (raggruppamenti funzionali)	Possibilità di associare agli uffici il codice IPA
160		Banche dati	struttura organizzativa (raggruppamenti funzionali)	Possibilità di associare ad un utente diversi profili di autorizzazione
161		Banche dati	titolario	Possibilità di gestire il titolario di classificazione
162		Banche dati	titolario	Possibilità di utilizzo flessibile e differenziato dei livelli del titolario
163		Banche dati	titolario	Possibilità di utilizzare funzionalità di classificazione automatica
164		Banche dati	titolario	Possibilità di utilizzare un indice sistematico
165		Banche dati	titolario	Possibilità di gestione contemporanea di più titolari
166		Banche dati	titolario	Possibilità di storicizzazione del titolario di classificazione
167		Banche dati	titolario	Possibilità di rappresentare il titolario di classificazione in formati standard

Numero requisito	Tipo	Aree funzionali	Categorie	Descrizione Requisito
168		Banche dati	titolario	Possibilità di classificare lo stesso documento in più nodi di titolario
169		Banche dati	tipologie documentali	Possibilità di gestire un elenco di tipologie documentali con associazione del registro e dei metadati specifici per tipologia

Il file *Allegato 2.1* "Riferimenti normativi" riporta inoltre alcune colonne supplementari nelle quali, per i requisiti definiti con la tipologia *ex lege*, sono elencate puntualmente le norme e gli articoli di riferimento.

La citazione normativa è fornita quale supporto per chi avesse necessità di approfondimenti o di letture "in parallelo" delle norme. Le fonti normative citate riguardano:

- Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 e s. m., Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
- Decreto Legislativo 22 gennaio 2004, n. 42, Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 Legge 6 luglio 2002, n. 137
- Decreto legislativo 7 marzo 2005 n. 82 e s. m., Codice dell'amministrazione digitale
- Agenzia per l'Italia Digitale Agenzia per l'Italia Digitale, Circolare n. 60 23 gennaio 2013, Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni. Revisione della Circolare AIPA del 7 maggio 2001, n. 28 relativa agli standard, le modalità di trasmissione, il formato e le definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati, ai sensi dell'art. 18, comma 2, del D.P.C.M. 31 ottobre 2000 di cui al D.P.R. 28 dicembre 2000, n. 445
- Decreto legislativo 14 marzo 2013, n. 33, Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni
- Decreto del Presidente della Repubblica 3 dicembre 2013, Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005

- Decreto del Presidente della Repubblica 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 del Presidente della Repubblica 13 novembre 2014, Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23 -bis , 23 -ter , 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio 27 aprile 2016, Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
- Legge 7 agosto 1990 n. 241 e s. m., Nuove norme in materia di procedimento amministrativo e di diritto do accesso ai documenti amministrativi
- Gruppo di lavoro AgID maggio 2016, Linee guida sulla pubblicità legale dei documenti e sulla conservazione dei siti web delle PA

1.2.3 Lo schema di valutazione dei requisiti del sistema di gestione documentale[7]

Lo strumento descritto nelle pagine seguenti si prefigge lo scopo di definire un metodo per effettuare una valutazione/verifica del grado di "conformità" delle soluzioni di gestione documentale già utilizzate dalle pubbliche amministrazioni o in fase di valutazione da parte delle stesse alla griglia dei criteri di valutazione definita.

I criteri di valutazione identificano caratteristiche e funzionalità fondamentali (pur non essendo soltanto di origine normativa) di un sistema di gestione documentale e che rispondono ad esigenze comuni di tutte le pubbliche amministrazioni per una agevole e corretta gestione documentale, in un'ottica di unitarietà dell'archivio, anche in considerazione di eventuali sistemi di supporto e/o complementari che interagiscono con il sistema di gestione documentale.

Le funzionalità individuate e i corrispondenti criteri sono quanto più possibile "astratti" rispetto a una specifica modalità di adozione di un sistema di gestione documentale, e quindi sono applicabili indistintamente nel caso di adozione in riuso di un sistema di

[7] Il presente strumento è stato elaborato da Giancarlo Di Capua e Luca Cicinelli, Innova Puglia – Società *in house* della Regione Puglia

gestione documentale, o di adozione di soluzione commerciale on premise o in *software as a service*, ecc.

I criteri non sono stati pesati a priori in considerazione del fatto che le PA non sono tutte uguali, e requisiti fondamentali per una possono esserlo meno per altre. Per questo motivo si è proposto un sistema di pesatura parametrizzabile sulle proprie specificità ed esigenze che prevede l'attribuzione da parte della singola PA di coefficienti di priorità che consentono di attribuire il peso maggiore a quei requisiti che realizzano funzioni considerate essenziali dalla medesima.

L'attività di valutazione/verifica è organizzata nelle seguenti fasi:

1. determinazione delle Aree di Priorità e Attribuzione del relativo Coefficiente di Priorità

2. aggregazione dei requisiti nelle Aree di Priorità

3. attribuzione del punteggio ad ogni singolo requisito

4. calcolo del Peso del Requisito

5. definizione della soglia di accettabilità della copertura per Priorità.

La Fase 1 prevede di raggruppare in Aree di Priorità i requisiti, attribuendo a ciascuna di esse un coefficiente in modo tale da avere i requisiti essenziali raggruppati in un'area con il coefficiente pari a 1, mentre i requisiti che si danno per scontati e che vengono realizzati direttamente tramite l'uso di tecnologie già disponibili con un coefficiente pari a 0.1. L'esito della fase 1 è la determinazione di quali cluster di requisiti sono indispensabili o irrinunciabili per il sistema e quali utili. I cluster di requisiti necessari, a loro volta, si suddividono in requisiti di immediata realizzazione tramite l'ausilio di tecnologie già conosciute e diffuse e requisiti specifici connessi strettamente alla gestione documentale.

La Fase 2 consiste nel determinare la mappa con cui i requisiti vengono inseriti nelle Aree di Priorità.

La Fase 3 consiste nell'attribuire un peso ai requisiti appartenenti alla stessa area, e il risultato è un elenco che determina quanto è importante il soddisfacimento di un requisito.

La Fase 4 consente di determinare il peso complessivo di un requisito in rapporto all'intero sistema

La Fase 5 consente infine di determinare il livello di rispondenza del sistema ai requisiti e quale sia il livello di copertura/conformità raggiunta da ogni Area di Priorità.

1.2.4 Fase 1. Determinazione delle Aree di Priorità

I requisiti e/o le categorie di requisiti devono essere raggruppati in Aree di Priorità che determineranno un ordine di importanza nella valutazione di completezza di sistemi

esistenti o di priorità nella realizzazione di nuovi sistemi. Ad ogni Area di Priorità ciascuna PA deve assegnare un Coefficiente di Priorità, che influirà sul peso attribuito ad ogni singolo requisito. Il coefficiente potrà avere un valore compreso tra 1 e 0,1 con variazione di centesimi. Per esempio, in un delta di valori tra 0,25 e 1,00 possiamo ipotizzare la seguente scala di valori:

Priorità	Descrizione	Coefficiente Priorità (CP)
A	Area Prioritaria determinata dal contesto specifico di realizzazione (Es.: categoria fascicoli, gestione procedimenti)	1
B	Area Prioritaria determinata dal contesto generico. Es.: gestione di differenti formati documentali, gestione di metadati (es. categoria Repertori, categoria Massimario di scarto,	0.75
C	Area non Prioritaria che raccoglie i requisiti realizzabili anche tramite integrazioni di sistemi e/o cooperazione applicativa (es. categoria Protocollazione, categoria Altre basi dati di supporto)	0.5
D	Area non Prioritaria che raccoglie i requisiti generali di un sistema per la PA e che si ritengono necessariamente presenti (es. categoria Tracciabilità accessi e modifiche, categoria predisposizione documento in uscita o interno (versioni, firme elettroniche e digitali)	0.25

1.2.5 Fase 2. Aggregazione dei requisiti

Tutti i requisiti dovranno essere inseriti nella relativa *Area di Priorità* a seconda dei criteri di aggregazione definiti nella Fase 1. E' necessario fare attenzione ad aggregare nelle Priorità A e D i requisiti che sono specifici del contesto della gestione documentale (Area A) e quelli che sono legati a tecnologie o a funzioni che si possono ritenere assodate, come per esempio l'utilizzo delle *email* per le notifiche, o la verifica di validità di una firma, o la gestione di Utenti e Ruoli/Funzioni.

L'importanza di ogni singolo requisito, verrà poi attribuita nella fase successiva.

1.2.6 Fase 3. Attribuzione punteggio ai Requisiti

All'interno della stessa *Area di Priorità* devono essere assegnati dei punteggi con un valore compreso tra 1 e 0.1 con variazione di decimi ad ogni singolo requisito in base alla seguente tabella:

Punteggio Requisito (PR)	Descrizione
1	Requisiti obbligatori determinati dalla normativa generale
0.9	Requisiti obbligatori determinati dalla normativa specifica di settore (es. Sanità, Avvocatura, ecc.)
0.8	Requisiti non obbligatori, ma che si realizzano in funzionalità indispensabili per facilitare il lavoro degli utenti o in integrazioni con altri sistemi (es. verifica della firma digitale, protocollazione informatica, fatturazione elettronica)
0.7	Requisiti non obbligatori, ma che si realizzano in funzionalità che facilitano il lavoro di gruppi non omogenei di utenti (es. lavoro collaborativo, comunicazioni)
0.6	Requisiti non obbligatori, ma che si realizzano in funzionalità che facilitano il lavoro degli utenti (ricerca di fascicoli, ricerca di documenti, annotazioni)
0.5	Requisiti non obbligatori, ma che si realizzano in funzionalità utili agli amministratori di sistema e che semplificano le operazioni tecniche rendendole disponibili a utenti non tecnici (es. strumenti di configurazione di sistema, definizione di nuovi metadati, monitoraggio)
0.3	Requisiti non obbligatori, ma che si realizzano in funzionalità che facilitano il lavoro degli utenti Amministratori di Sistema (es. analisi dei log, analisi delle performance del sistema)
0.2	Requisiti non obbligatori, ma che si realizzano in funzionalità utili solo in determinati contesti organizzativi (es. amministrazione regionale, comuni, ASL, ecc.)
0.1	Requisiti non obbligatori, ma che si realizzano in funzionalità utili solo per il sistema stesso (es. allineamento base dati, sincronizzazione tra sistemi cooperanti)

1.2.7 Fase 4. Calcolo del Peso del Requisito

Al termine delle operazioni di classificazione, il peso di ogni singolo requisito sarà automaticamente determinato secondo la seguente formula:

Peso Requisito = Punteggio Requisito (PR) * Coefficiente Priorità (CP)/MAX(PR)

Dove MAX(PR) Rappresenta il punteggio massimo ottenuto da un Requisito nella stessa Area di Priorità. Il Peso del Requisito va arrotondato ai centesimi.

1.2.8 Fase 5. Definizione della soglia di accettabilità della copertura per Priorità

Per la valutazione della corrispondenza di un sistema già esistente o in fase di analisi per una acquisizione, si propone di calcolare, a valle del calcolo dei pesi dei singoli requisiti, il peso complessivo di ogni *Area di Priorità*. Sulla base di questo peso, in percentuale, si determina la soglia che il sistema in valutazione deve superare per ritenere che sia accettabile.

Si propone la seguente griglia di soglie:

Priorità	Descrizione	Soglia di Accettabilità
A	Area Prioritaria determinata dal contesto specifico di realizzazione. Es.: gestione fascicoli, gestione procedimenti	100%
B	Area Prioritaria determinata dal contesto generico. Es.: gestione di differenti formati documentali, gestione di metadati	75%
C	Area non Prioritaria che raccoglie i requisiti realizzabili anche tramite integrazioni di sistemi e/o cooperazione applicativa: Protocollo Informatico, Anagrafe Cittadini, Anagrafe Imprese, Fatturazione Elettronica	25%
D	Area non Prioritaria che raccoglie i requisiti generali di un sistema per la PA e che si ritengono necessariamente presenti. Es.: Raccolta dei dati e organizzazione in un Database Relazionale, utilizzo di email o PEC, firma digitale, gestione utenti	100%

Le Aree A e D si ritengono come obbligatorie per i seguenti motivi:

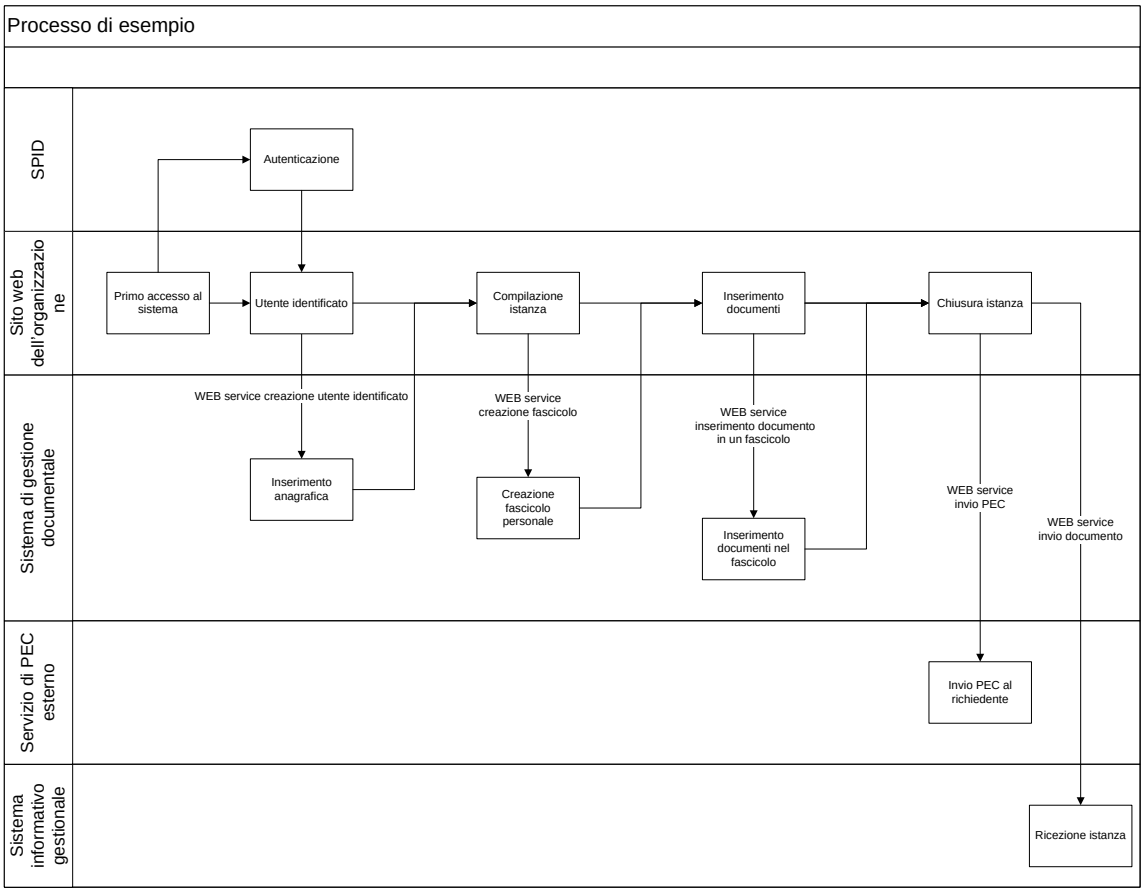
- sono presenti in questa Area i requisiti fondamentali del sistema (obblighi normativi)
- sono presenti in questa Area i requisiti afferenti all'utilizzo di tecnologie di base che non vanno implementate, ma soltanto utilizzate, e quindi si dà per scontato che siano presenti nel sistema e/o in cooperazione applicativa.

Ogni requisito soddisfatto, quindi, concorrerà ad aggiungere il proprio Peso al valore di copertura totale dell'Area.

Allegato 1.1 - Web Services[8]

Le integrazioni tra applicativi diversi avvengono per lo più tramite *web services,* che sono strumenti che consentono di automatizzare funzioni e che possono utilmente essere applicati anche ad un sistema di gestione documentale. Automatizzano quindi funzioni che il sistema già gestisce ma che sono richiamabili all'esterno dell'applicazione attraverso meccanismi e/o protocolli definiti. Si possono utilizzare come servizi base per un *workflow* che a sua volta può essere incluso in sistemi di orchestrazione (su una *service oriented architecture*) per aumentare l'interoperabilità fra sistemi informativi.

L'esposizione di questi servizi rientra nella logica del sistema adottata come modello in quanto possiamo considerarli come strumenti operativi corrispondenti alle frecce con descrizione WEB service che identificano i flussi fra i moduli, come rappresentato nell'immagine:



[8] Documento a cura di Costantino **Landino** (Ministero per i beni e le attività culturali)

Esempio di processo

Nell'esempio è illustrato un processo su cinque sistemi diversi che colloquiano via *web services.*

I cinque sistemi sono: SPID, un sito *web* di servizio per la ricezione delle istanze, il sistema di gestione documentale, un sistema di gestione delle PEC e un sistema gestionale interno.

Il flusso di lavoro (*workflow*) si svolge fra i sistemi utilizzando web service che colloquiano fra loro.

Di seguito sono riportati alcuni esempi di *web services* (suddivisi per aree) che possono essere coinvolti nelle interazioni fra i diversi applicativi (in grassetto sono evidenziati i *web services* necessari a supporto dell'esempio di processo sopra descritto).

Col variare del processo e delle funzioni o dei servizi coinvolti variano necessariamente i *web services* indispensabili all'automazione del processo e all'integrazione fra i sistemi applicativi.

Alcuni esempi di web services possono essere (suddivisi per aree):

1. *Web Services* di protocollazione (Altre funzionalità come cancellazione o registro di emergenza sono gestite con gli strumenti di amministrazioni da *backoffice*)
   - **1.1. registrazione di protocollo in ingresso a seguito di una richiesta standard con tutti i parametri necessari**
   - 1.2. Registrazione di protocollo in uscita a seguito di una richiesta standardizzata con tutti i parametri necessari
   - 1.3. elenco dei documenti protocollati in un intervallo temporale
   - 1.4. ……
2. Servizi di interazione con strumenti di posta elettronica:
   - **2.1. invio di un pacchetto di informazioni o di documenti attraverso un sistema di posta elettronica certificata**
   - 2.2. ricezione di un pacchetto di informazioni o di documenti attraverso un sistema di posta elettronica certificata
   - 2.3. invio di un pacchetto di informazioni o di documenti attraverso un sistema di posta elettronica ordinaria
   - 2.4. ricezione di un pacchetto di informazioni o di documenti attraverso un sistema di posta elettronica ordinaria
   - 2.5. ….
3. Servizi di gestione documentale:
   - **3.1. creazione fascicolo**
   - 3.2. creazione di un documento
   - **3.3. inserimento di un documento in un fascicolo**
   - 3.4. indicizzazione di un documento
   - 3.5. visualizzazione di un documento
   - 3.6. ricerca sui documenti

3.7. ……
4. Servizi di interazione OAIS *compliant* (per interoperabilità con sistemi di conservazione):
   4.1. invio pacchetti di versamento
   4.2. ricezione pacchetti di distribuzione
   4.3. ……
5. Servizi di autenticazione:
   5.1. controllo anagrafica e autorizzazioni
   5.2. inserimento utente nel sistema
   5.3. lettura informazioni su utente

Un ulteriore elemento da valutare è relativo alla tipologia dei *web services*, che possono essere di tipo restFUL o SOAP, con implicazioni differenti sugli sviluppi del relativo *software*.

Allegato 2.1 - Riferimenti normativi

L'allegato è scaricabile qui.

Allegato 3.1 - *simulazione*

Applicazione dello schema di valutazione dei requisiti del sistema di gestione documentale DIOGENE – Regione Puglia

L'*Allegato 3.1* riporta una simulazione esemplificativa effettuata in relazione al Sistema DIOGENE 2.0 in dotazione presso la Regione Puglia. L'allegato è scaricabile qui.

Allegato 4.1 – *simulazione*

Applicazione dello schema di valutazione dei requisiti del sistema di gestione documentale P.I. Tre

L'*Allegato 4.1* riporta una simulazione esemplificativa effettuata in relazione al Sistema Protocollo Informatico Trentino – P.I.Tre in dotazione presso la Provincia autonoma di Trento. L'allegato è scaricabile qui.

2. Il fascicolo informatico nella gestione documentale

capitolo a cura di[9]

2.1 Il fascicolo informatico: le sue ragioni funzionali in quanto rappresentazione credibile del processo

di Alessandro **Alfier** (Ministero dell'Economia e delle Finanze)

Qualsiasi documento, a prescindere dal suo supporto analogico o digitale, in ragione della sua natura essenziale e a condizione di essere correttamente prodotto e gestito da un sistema di gestione documentale e di essere poi eventualmente conservato correttamente a tempo illimitato da un sistema di custodia, è la rappresentazione credibile di atti e fatti (*business events and transactions* secondo lo standard ISO di riferimento)[10], così da poter fungere appieno da surrogato nel tempo e nello spazio di ciò che viene rappresentato.

[9] Il capitolo nasce dalle riflessioni e dal confronto, anche vivace e con approcci diversificati , del gruppo di lavoro coordinato da Alessandro **Alfier** (Ministero dell'Economia e delle Finanze) e Silvia **Trani** (Archivio centrale dello Stato) e composto Gabriele **Bezzi** (Polo archivistico Emilia-Romagna), Gaetano **Bruno** (Agenzia per l'Italia digitale), Barbara **Corvisieri** (Istituto nazionale di statistica), Giancarlo **Di Capua** (InnovaPuglia Spa), Patrizia **Gentili** (Agenzia per l'Italia digitale), Silvia **Ghiani** (Lepida Spa), Costantino **Landino** (Istituto centrale per gli Archivi), Elena **Lisi** (Dedagroup Public Services), Roberto **Monaco** (Federazione nazionale degli ordini dei medici chirurghi e degli odontoiatri), Cristina **Palumbo** (Regione autonoma Friuli Venezia Giulia), Stefania **Piersanti** (Direzione generale Archivi), Maria Emanuela **Pinto** (Federazione nazionale degli ordini dei medici chirurghi e degli odontoiatri), Valeria **Sisti** (Dedagroup Public Services), Brizio Leonardo **Tommasi** (Commissione nazionale per le società e la Borsa), Barbara **Troiani** (Istituto nazionale per l'assicurazione contro gli infortuni sul lavoro), Cristina **Valiante** (Agenzia per l'Italia digitale) Eurosia **Zuccolo** (Istituto nazionale della previdenza sociale).

[10] Lo standard ISO 15489-1:2016, Information and documentation – Records management – Part 1: Concepts and principles, al paragrafo 5.2.1 dichiara: «Records, regardless of form or structure, should possess the characteristics of authenticity, reliability, integrity and useability … to be considered authoritative evidence of business events or transactions …». Tale dichiarazione di principio fa ricorso al concetto di authoritative evidence, che può essere tradotta opportunamente anche se non letteralmente con l'espressione italiana di rappresentazione credibile, dal momento che lo stesso standard, al paragrafo 3.10, si preoccupa di definire l'evidence come "documentation of a transaction" in senso ampio e nient'affatto ristretta a un contesto legale.

La capacità rappresentativa del documento è una grandezza che può essere progressivamente estesa sull'onda della natura relazionale del documento medesimo. Quest'ultimo, infatti, presenta in prima battuta una capacità rappresentativa puntuale e quindi ridotta. Nella misura in cui però fuoriesce spontaneamente dalla sua "dimensione atomica" per relazionarsi con altri documenti a formare delle "catene documentali" di ampiezza variabile[11], esso amplia proporzionalmente la sua capacità di rappresentazione.

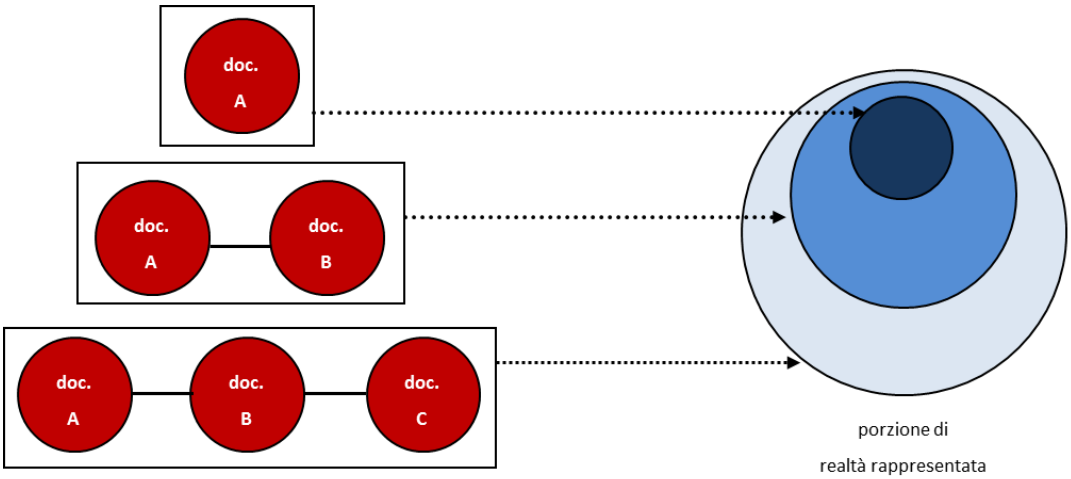


Figura 1 – L'estensione progressiva della capacità rappresentativa del documento e delle relazioni tra documenti

Di questa capacità rappresentativa estendibile del documento sono pienamente consapevoli gli standard ISO in tema di gestione documentale. Fra essi in particolare lo standard ISO 23081-2:2009, *Information and documentation – Managing metadata for records – Part 2: Conceptual and implementation issues*, stabilisce, pur per un contesto assai specifico come quello rappresentato dalla metadatazione ai fini della gestione documentale, un preciso parallelismo: da un lato le "catene documentali" che si formano a partire dal documento nella sua "configurazione atomica" (gli strati di aggregazione documentaria di cui alla Table 1 di seguito riportata), dall'altro lato le corrispondenti azioni rappresentate e caratterizzate da una dimensione di scala sempre più ampia ed estesa (gli strati di aggregazione funzionale di cui alla Table 2 di seguito riportata):

[11] La scienza archivistica denota questo meccanismo relazionale attraverso il concetto di *vincolo archivistico*.

Table 1 — Entity class: Records[12]

Layer	Indicative name for aggregation	Aspects of business environment represented
1	Item	The smallest discrete unit of records managed as an entity. Items can contain components such as an email with attachments; however, the components of the item are managed as a single entity within the system.
2	Transaction sequence	A sequence of items, physically or virtually linked, which shows one coherent transaction leading to a specific outcome.
3	File	A sequence of items, physically or virtually linked, which evidences an organizational/business activity. Individual items on the file have relationships with each other, for example a letter and a reply, and a reply to that, etc., which are preserved by being kept on file in the right order and are part of the evidence in the records. A file can be physical or electronic.

Table 2 — Entity class: Business (including records business)[13]

Layer	Indicative name for aggregation	Aspect of business environment represented
1	Transaction	The smallest unit of business activity.
2	Activity/process	The major tasks performed by an organization to accomplish each of its functions. An activity/process should be based on a cohesive grouping of transactions producing a singular outcome.
3	Function	Functions represent the major responsibilities that are managed by an organization to fulfil its goals. Functions are high-layer aggregates of the organization's activities.

[12] ISO 23081-2:2009, p. 11.

[13] ISO 23081-2:2009, p. 12.

Questa stessa visione concettuale può essere anche rappresentata ricorrendo allo schema che segue:

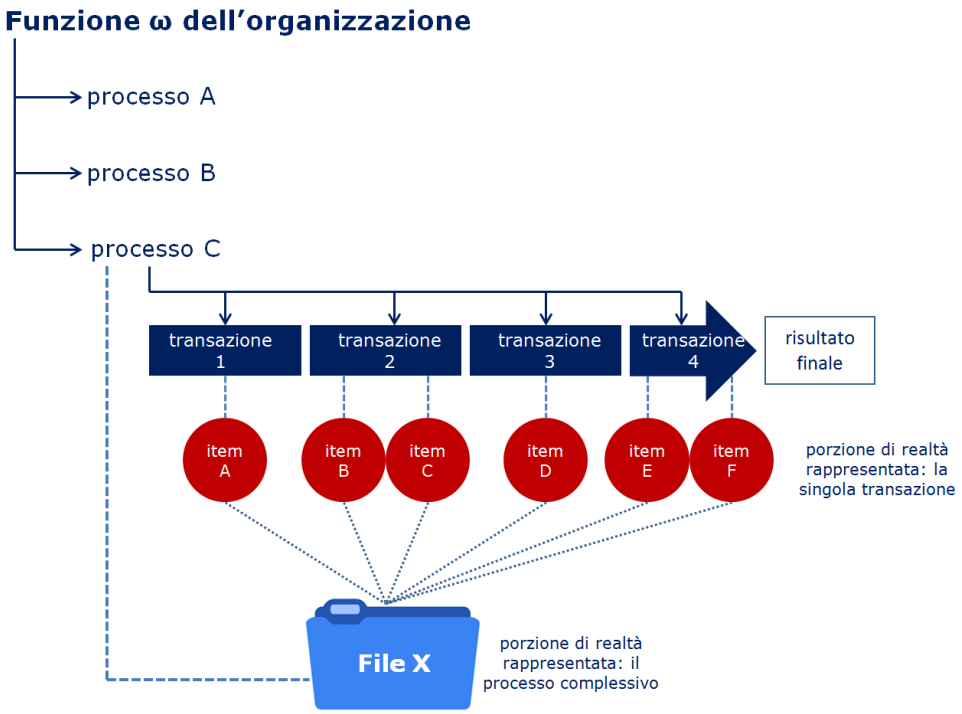


Figura 2 – Comparazione tra la capacità rappresentativa del documento (item) e quella del fascicolo (file)

Lo standard ISO aderisce, pertanto, con convinzione alla visione in cui il documento – l'entità *item* nel linguaggio dell'ISO 23081-2:2009 – a partire da una capacità rappresentativa più ridotta e meno significativa che ha come focus la singola transazione, riesce ad espandere quanto strettamente rappresentato dal documento singolo nella misura in cui si aggrega ad altri documenti, formando quella "catena documentale" che tradizionalmente chiamiamo fascicolo – l'entità *file* nel linguaggio dell'ISO 23081-2:2009: si approda così a un concetto di rappresentazione della realtà più ampio e soprattutto più pregnante, perché capace di surrogare – a fini performativi legati al perseguimento della mission, a scopi legali o di *accountability* oppure come sapere strategico – i processi intesi come le dorsali di attività di qualsiasi organizzazione, ben al di là delle singole transazioni che li compongono.

Una visione questa che si ritrova ribadita anche nel principale standard ISO dedicato alla gestione documentale: l'ISO 15489-1:2016, *Information and documentation – Records management – Part 1: Concepts and principles*. Se in prima battuta esso dichiara, in toni

per così dire sommessi, che «Records document individual events or transactions, or may form aggregations that have been designed[14] to document work processes, activities or functions»[15], nel proseguo del testo si giunge ad affermare, con riferimento alla definizione della funzione di classificazione, come «Records classification includes … providing linkages between individual records and aggregations, to provide *a continuous record of business activity*»[16]. L'affermazione è significativa perché ribalta la visione semplificata, ma ahinoi diffusa, della gestione documentale, riconducendola ad una più corretta comprensione: non una dimensione funzionale incentrata sulla gestione dei singoli documenti in sé e per sé, ma un ambito funzionale in cui la gestione dei singoli documenti è vista come un volano per la gestione in ultima istanza delle aggregazioni documentali, le sole capaci di rappresentare l'attività complessiva delle organizzazioni non solo in modo credibile, ma soprattutto senza iati e parzialità e dunque con i crismi dell'organicità.

La fondamentale e basilare forma di aggregazione documentale a cui mette capo il documento, in un contesto di corretta gestione documentale, è il fascicolo: esso assume una rilevanza centrale giacché si pone come la rappresentazione credibile del processo di lavoro, ossia l'unità di misura essenziale dell'agire e dell'operare delle organizzazioni contemporanee, tanto private quanto pubbliche. Pertanto il fascicolo – in particolare quello informatico – costituisce uno dei focus principali dei contemporanei sistemi di gestione documentale e come per il singolo documento così anche per questo tipo di aggregazione documentaria vale il principio che essa non può conseguire la sua finalità di strumento di rappresentazione credibile se non nel contesto di un corretto sistema di gestione documentale.

Va evidenziato inoltre che il fascicolo, in senso proprio, non è una rappresentazione estemporanea, contingente o puramente soggettiva di un certo processo, ma ne è per l'appunto il surrogato credibile, non altrimenti sostituibile. Tale credibilità è veicolata da molteplici fattori: in primo luogo dalla credibilità distribuita sui singoli documenti che rappresentano atomisticamente le transazioni che hanno composto il processo complessivamente inteso; in secondo luogo dalla natura del fascicolo come un'aggregazione documentale precisamente strutturata e in quanto tale votata a documentare il processo nel suo ordine storico di svolgimento, attraverso un'univoca

[14] Degno di nota il ricorso da parte dello standard al termine *designed*: se è indubbio, come più sopra ricordato, che il documento ha una profonda natura relazionale, che lo porta ad aggregarsi ad altri documenti formando livelli di aggregazione sempre più estesi ("catene documentali" che sfociano in "reti documentali"), è altrettanto certo che questa natura giunge a concretizzarsi solo qualora sia supportata *ad hoc*: non tanto da un qualsiasi sistema di gestione documentale, ma da un sistema di gestione documentale a questo scopo concepito e che pertanto abbia come focus centrale la natura relazionale del documento. Considerato che i contesti digitali sono molto meno "indulgenti" di quelli analogici, il vincolo di necessità tra predisposizione aggregativa del documento e sistema di gestione documentale è molto più stringente in quelli che non in questi.

[15] ISO 15489-1:2016, paragrafo 5.2.1, p. 4.

[16] ISO 15489-1:2016, paragrafo 9.4, p. 17. Il corsivo è di chi scrive.

successione di documenti che rappresenta il susseguirsi storico delle transazioni che hanno portato allo sviluppo complessivo del processo stesso. In quanto rappresentazione credibile, il fascicolo riesce così a documentare il processo nel suo contesto storico di esecuzione[17], dunque per lo meno per quanto attiene:

- ai suoi tempi di esecuzione;
- alle sue modalità e mezzi di svolgimento;
- ai risultati da esso conseguiti;
- agli attori che vi hanno preso parte a diverso titolo;
- alle eventuali criticità o anomalie che hanno segnalato il suo svolgimento.

Il concetto di *struttura* costituisce il fulcro del vincolo rappresentativo tra processo e fascicolo e del loro rapporto biunivoco: la struttura del processo si riverbera infatti – secondo determinate modalità decise di volta in volta dall'organizzazione in ambito di gestione documentale per la predisposizione a priori delle differenti tipologie di fascicolo – nella struttura del fascicolo e tramite questo rapporto il fascicolo si pone, come già detto, nei termini di surrogato credibile del processo stesso, non altrimenti sostituibile e per questo distinto da qualsiasi altra aggregazione documentale estemporanea, contingente o puramente soggettiva. Data questa essenziale corrispondenza, la complessità di struttura del fascicolo è una variabile tendenzialmente proporzionale alla complessità strutturale del

[17] Nella misura in cui il fascicolo funge da rappresentazione credibile del contesto storico di esecuzione del processo complessivamente considerato, esso è uno strumento di documentazione particolarmente efficace e pervasivo, in grado di sopperire non solo ai limiti di documentazione che sono naturalmente intrinseci al singolo documento considerato nella sua dimensione «atomica», ma anche ad eventuali e non voluti difetti dell'azione di documentazione che possono essere presenti sullo stesso documento. Una chiara riprova di questa circostanza si ritrova nella giurisprudenza attinente a quel particolare processo rappresentato dal procedimento amministrativo. Ad esempio la sentenza del Consiglio di Stato, Sez. IV, 4 febbraio 1997, n. 89, dichiara: «non ricorre il vizio di difetto di motivazione dell'atto amministrativo quando le ragioni poste a base del provvedimento risultano enunciate in precedenti atti del procedimento». Tale sentenza si basa su un non detto, tanto scontato quanto essenziale: affinché i precedenti possano sopperire al difetto di documentazione delle motivazioni di cui è affetto il provvedimento finale, è necessario che questo e quelli siano reciprocamente e stabilmente relazionati attraverso la loro aggregazione in un fascicolo, rappresentativo del procedimento amministrativo complessivamente considerato (la sentenza in parola è citata in GIANNI PENZO DORIA. *Due osservazioni sul fascicolo archivistico*, in *Documenti e informatica: gli archivi correnti degli enti pubblici territoriali dell'Umbria*. *Atti del 2° incontro di lavoro. Terni, 3 ottobre 2000*, a cura di GIOVANNA GIUBBINI, Perugia, Soprintendenza archivistica per l'Umbria, 2001, p. 102-111).

processo rappresentato, al punto che l'articolazione interna del fascicolo può conoscere la presenza di *sotto-fascicoli*, a loro volta strutturati in *inserti*[18].

[18] La terminologia della scienza archivistica ricorre al concetto di *inserto* per indicare una articolazione del sotto-fascicolo.

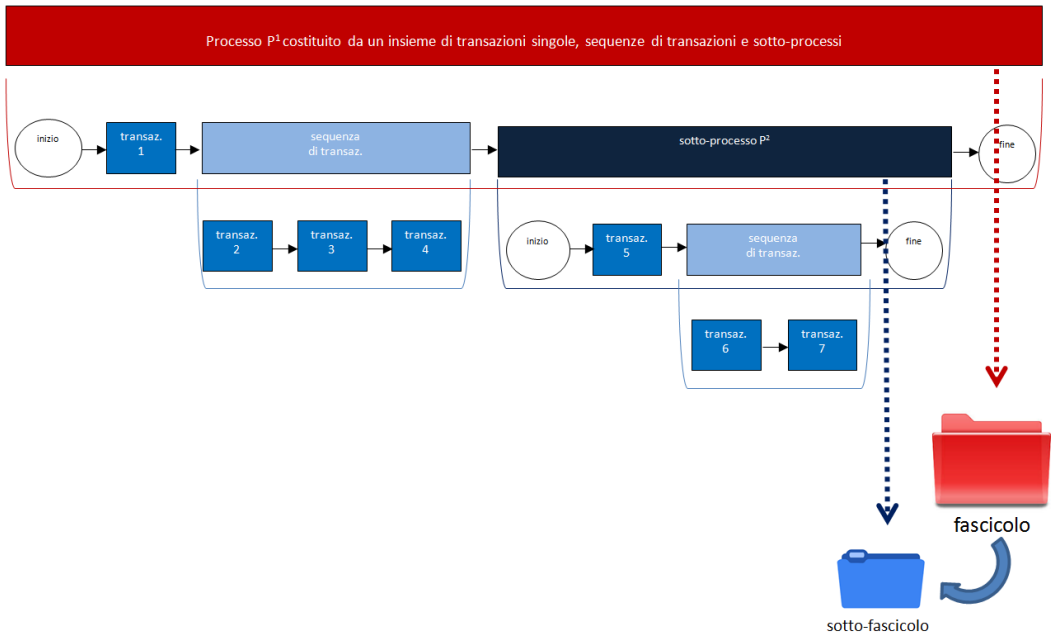


Figura 3 – Complessità di struttura del fascicolo in rapporto alla complessità di struttura del processo rappresentato

Il fascicolo in ambiente analogico era in grado di fungere da rappresentazione, surrogato credibile del processo nel suo contesto storico di esecuzione sia attraverso la propria organizzazione fisica, sia per mezzo di una serie di annotazioni che, mano a mano, venivano manualmente apposte sulla camicia dello stesso fascicolo o sui suoi documenti componenti. Il fascicolo informatico ha – potenzialmente[19] – accresciuto questa capacità rappresentativa: infatti le cosiddette applicazioni di *business*, che nel contesto dei sistemi informativi delle organizzazioni sono deputate allo svolgimento dei processi che caratterizzano l'agire e l'operare di quelle stesse organizzazioni, riescono a tracciare in modo sempre più granulare lo svolgimento storico del singolo processo nel concatenarsi delle sue transazioni costitutive, mettendo così a disposizione insiemi sempre più estesi di metadati che possono essere condivisi con il sistema di gestione documentale, per un loro riuso in vista della produzione e gestione dei fascicoli[20].

[19] Si tratta di potenzialità, dato che l'accrescimento di capacità rappresentativa del fascicolo richiede che sia preliminarmente soddisfatta una precisa condizione operativa: l'integrazione efficace e sistematica tra le applicazioni di *business* in uso nell'organizzazione e il suo sistema di gestione documentale.

[20] Non a caso lo standard ISO 23081-1:2017, *Information and documentation – Records management processes – Metadata for records – Part 1: Principles*, dichiara: «The context of records includes information about the business processes in which they are created. These metadata will allow users

Se dal punto di vista concettuale il fascicolo presenta una sua indubbia unitarietà, in quanto rappresentazione credibile di un processo, dal punto di vista empirico esso si offre con una molteplicità di possibili manifestazioni: nella misura in cui sussistono diverse tipologie di processo, ciascuna di esse condiziona, in modo più o meno peculiare, la sua concreta forma di rappresentazione documentale. Nel passaggio dal fascicolo su supporto cartaceo al fascicolo informatico sembra appannarsi la consapevolezza di questo polimorfismo, complici forse alcune formulazioni normative non sempre correttamente interpretate. Ad esempio nel contesto delle organizzazioni identificate dalle amministrazioni pubbliche domina l'impressione che l'unica istanza concreta di fascicolo informatico sia quella attinente al procedimento amministrativo, forse per effetto di quell'art. 41 del «Codice dell'amministrazione digitale» (CAD)[21], significativamente rubricato come «Procedimento e fascicolo informatico», solo parzialmente chiarito dalla voce che, all'interno del glossario presente nell'Allegato 1 delle «Regole tecniche»[22], offre la seguente definizione di fascicolo informatico:

> Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice [dell'amministrazione digitale].

La lettura congiunta dell'articolo 41 del CAD e della voce ora citata del glossario mette in evidenza il fatto che, complessivamente, la definizione normativa non stabilisce affatto che un'amministrazione pubblica sia tenuta a produrre e gestire, sempre e comunque, quell'unica specie di fascicolo informatico relativa al procedimento amministrativo, ma più semplicemente indica che qualora il processo da rappresentare su un piano documentale sia costituito da un processo procedimentalizzato ai sensi della l. 7 ago. 1990, n. 241 – un procedimento amministrativo – il corrispondente fascicolo informatico debba ottemperare alla norma inserita nel citato art. 41 del CAD. La voce di glossario in parola infatti:

- con l'espressione «aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici» rimarca in prima battuta la natura generale del

to understand … the environment in which records were created, the purpose or business activity being undertaken *and their relationships with other records or aggregations*» (paragrafo 5.2.2, p. 4. Il corsivo è di chi scrive). Lo standard dunque sottolinea che le informazioni che tracciano, in forma di metadati, i processi sono un potente catalizzatore delle dinamiche di aggregazione documentale, sulla base dell'implicito presupposto che i processi, a seguito della loro natura composita, si autorappresentano non attraverso la prospettiva atomica del singolo documento, ma grazie a «catene documentali» più o meno estese e complesse.

[21] D.lgs. 7 mar. 2005, n. 82.

[22] Decreti del presidente del Consiglio dei ministri 3 dic. 2013 e d.p.c.m. 13 nov. 2014.

fascicolo informatico: dunque il suo essere un'aggregazione documentaria caratterizzata da una struttura univoca, chiamata a dar conto della successione storica delle specifiche transazioni componenti il concreto processo rappresentato;

- con il rimando alla «specifica attività o … specifico procedimento» sottolinea, in seconda battuta, che proprio quella natura generale permette al fascicolo di essere una rappresentazione credibile di qualsiasi tipo di processo, sia esso o meno coincidente con la tipologia del procedimento amministrativo.

Ne discende che nella misura in cui una parte dell'agire e operare delle amministrazioni pubbliche non sia procedimentalizzata[23], quella stessa parte sarà popolata da processi che nulla hanno a che vedere con i procedimenti amministrativi e che pertanto saranno rappresentabili documentalmente per mezzo di fascicoli informatici, quantunque non rientrabili nella fattispecie ex art. 41 del CAD.
È pacifico pertanto che il suddetto art. 41 non esaurisce la casistica dei fascicoli informatici che le organizzazioni pubbliche sono tenute a produrre e gestire e che pertanto il tradizionale polimorfismo del fascicolo si ripropone, tale e quale, nel passaggio dallo scenario analogico allo scenario digitale. Questa visione trova un ulteriore riscontro sempre sul piano normativo, qualora però si voglia prendere come riferimento un insieme di norme più esteso di quello rappresentato dal CAD. Se il legislatore autore di tale codificazione, al pari dell'estensore del «Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa»[24], sembra dimentico del fatto che l'agire e l'operare di un'amministrazione pubblica può esprimersi anche con tipologie di processi che non sono

[23] Le riforme che hanno investito, oramai da diversi decenni, l'amministrazione pubblica italiana hanno avuto, tra le innumerevoli conseguenze, anche quella di permettere l'introduzione, nel modo di agire ed operare delle stesse, di istituti giuridici propri del diritto privato, accanto a quelli tipici del diritto pubblico, come chiaramente evidenziato dalla l. 7 ago. 1990, n. 241, che all'art. 1, co. 1-bis, afferma: «La pubblica amministrazione, nell'adozione di atti di natura non autoritativa, agisce secondo le norme di diritto privato salvo che la legge disponga diversamente». Pertanto a differenza del passato, in cui l'amministrazione pubblica doveva perseguire le proprie finalità solo ricorrendo a poteri d'imperio, ponendo in essere conseguentemente degli atti unilaterali, oggigiorno la stessa può perseguire un fine pubblico anche mediante l'attività negoziale. Va inoltre tenuto in conto che sempre più spesso l'amministrazione pubblica si orienta, per accrescere la propria efficienza ed efficacia interna, verso modelli gestionali di chiara ispirazione aziendalistica, che esaltano la dimensione del lavorare per progetti e processi: anche per questa via dunque si accresce la quota parte dell'agire e operare dei soggetti pubblici che si riflette in fascicoli informatici non rappresentativi di procedimenti amministrativi in senso stretto.
[24] D.p.r. 28 dic. 2000, n. 445.

necessariamente riducibili alla fattispecie dei procedimenti amministrativi e che pertanto quell'agire ed operare può trovare una forma di rappresentazione documentale diversa dal fascicolo regolato dall'art. 41 dello stesso «Codice», il «Codice dei beni culturali e del paesaggio»[25] all'art. 30, co. 4, offre delle indicazioni più esaustive:

> I soggetti indicati al comma 1 [cioè lo Stato, le regioni, gli altri enti pubblici territoriali e ogni altro ente ed istituto pubblico] hanno l'obbligo di conservare i propri archivi nella loro organicità e di ordinarli. I soggetti medesimi hanno altresì l'obbligo di inventariare i propri archivi storici, costituiti dai documenti relativi agli affari esauriti da oltre quarant'anni[26].

Nell'interpretare tale comma si può osservare che il termine *archivi*, presente nel primo periodo dell'articolo in parola, deve essere inteso in un'accezione ampia e generale tale da includere gli archivi correnti, gli archivi intermedi e gli archivi storici, dal momento che il legislatore quando avverte la necessità di riferirsi alla sola documentazione storica – come accade nel secondo periodo dello stesso articolo – utilizza esplicitamente la specifica dicitura di *archivi storici*. Pertanto la prima parte dell'articolo in esame deve essere interpretata come un obbligo attribuito alle organizzazioni pubbliche affinché:

- garantiscano, già a partire dai loro sistemi di gestione documentale, un'organizzazione dei documenti correnti rispettosa del principio di organicità27 e che quindi salvaguardi quelle "catene documentali" – prime fra tutte i fascicoli – che forniscono una rappresentazione credibile dei processi portati a termine, indipendentemente da ogni loro eventuale procedimentalizzazione28;

[25] D.lgs. 22 gen. 2004, n. 42.

[26] La seconda parte del co. 4 è un esempio di alcune ambiguità presenti nel «Codice dei beni culturali e del paesaggio» in materia di beni archivistici. Infatti, il riferimento all'obbligo di inventariare gli archivi storici prodotti, costituiti da documenti afferenti ad affari esauriti da oltre quarant'anni, riguarda specificatamente gli enti pubblici non statali mentre per le amministrazioni centrali e periferiche dello Stato si applicano le disposizioni dell'art. 41.

[27] Nelle terminologia della scienza archivistica il concetto di *organicità* sta esplicitamente ad indicare che l'archivio, fin dalla sua iniziale fase corrente alimentata da un sistema di gestione documentale, non è una semplice somma più o meno amorfa di documenti, ma una rete di relazioni documentarie ("catene documentale") che si pongono a diversi livelli di aggregazione e in cui il primo livello aggregativo, a partire dal basso, è appunto quello rappresentato dai fascicoli.

[28] Una conferma del fatto che le organizzazioni pubbliche siano obbligate a gestire i fascicoli informatici *tout court* e non solo i fascicoli informatici relativi a procedimenti amministrativi, si ritrova nelle «Regole tecniche per il protocollo informatico» (d.p.c.m. del 3 dic. 2013) che, all'art. 5, co. 2, let. h), afferma che il manuale di gestione documentale deve riportare «le modalità di formazione, implementazione e gestione dei fascicoli informatici relativi ai procedimenti e delle aggregazioni documentali informatiche», con ciò rimarcando il fatto che i fascicoli informatici

- rispettino coerentemente tale originaria organizzazione dei documenti lungo tutte le successive tappe del ciclo di vita della documentazione (archivio intermedio e archivio storico).

È pertanto evidente che il modello italiano di gestione documentale formalizzato a livello normativo individua nella fascicolazione *tout court* una funzione obbligata per la gestione documentale digitale da parte delle organizzazioni pubbliche, a prescindere dalle forme che i fascicoli informatici possono assumere in ragione delle differenti tipologie di processi rappresentati, procedimentalizzati o meno: detto in altri termini i sistemi di gestione documentale in uso alle amministrazioni pubbliche devono sempre consentire l'organizzazione per aggregazioni – cioè per fascicoli – di tutti i singoli documenti, anche di quelli che partecipano a processi che non sono procedimenti amministrativi[29].
Rispetto al polimorfismo del fascicolo anche informatico, di cui come si è appena visto le organizzazioni pubbliche si devono far carico giacché la fascicolazione è in sé e per sé una funzione di gestione documentale obbligata, la scienza archivistica ha da tempo individuato una casistica completa delle forme possibili[30]:

procedimentali non sono l'unica tipologia di aggregazione documentale che deve essere gestita in un contesto di sistema di gestione documentale al servizio di un'organizzazione pubblica.

[29] Questo obbligo nel modello italiano di gestione documentale per la fascicolazione *tout court*, al di là della specifica fattispecie costituita dal fascicolo relativo al procedimento amministrativo, e che viene in parte evocata anche negli articoli sopra richiamati del «Codice dei beni culturali e del paesaggio», appare meno esplicito nel «Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa». Questo all'art. 52 prescrive che «il sistema di gestione informatica dei documenti … deve … garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione … adottato» e dato che l'art. 64, co. 4, dello stesso «Testo unico» dispone che la classificazione debba essere applicata a tutti i documenti e non solo a quelli sottoposti a registrazione di protocollo, se ne deduce che il sistema di gestione documentale di un'amministrazione pubblica ha l'obbligo di farsi carico dell'organizzazione di tutti i documenti, senza esclusione alcuna. Va però tenuto presente che l'organizzazione documentale non si esaurisce nella mera classificazione, tant'è vero che il legislatore del «Testo unico» indica che quell'operazione deve avvenire «nell'ambito del sistema di classificazione»: come a dire che l'organizzazione documentale si basa sulla classificazione, ma non coincide per intero con essa, giacché, come ha anche sottolineato la scienza archivistica e le tecniche di gestione documentale, l'organizzazione documentale si avvia con la classificazione, ma si completa e si realizza concretamente con l'aggregazione dei documenti, in particolare per fascicoli (per una disamina dei rapporti funzionali complementari tra classificazione e fascicolazione si vedano le pagine che seguono). Dunque lungo questa via interpretativa si perviene ad affermare che anche il «Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa» sembra indicare un obbligo di fascicolazione *tout court*, che va al di là del caso particolare costituito dai fascicoli inerenti ai procedimenti amministrativi in senso stretto.

[30] Una disamina dettagliata delle differenti forme (tipologie) di fascicolo, valevoli tanto per il contesto analogico quanto per il contesto digitale, si ritrova in GIANNI PENZO DORIA, *Il fascicolo*

- il fascicolo di procedimento amministrativo: rappresenta l'agire e l'operato di un'organizzazione pubblica che si svolge attraverso una pluralità di azioni (transazioni) distinte, ma complementari e che finalisticamente concorrono a concludersi con l'emanazione formale di un provvedimento finale;
- il fascicolo di attività: rappresenta l'agire e l'operato di un'organizzazione pubblica che si svolge attraverso una procedura, cioè una sequenza di azioni (transazioni) ripetitive e precisamente definite nelle loro modalità e tempistiche e che non concorrono finalisticamente all'emanazione di un provvedimento finale;
- il fascicolo di affare: rappresenta l'agire e l'operato di un'organizzazione pubblica non procedimentalizzato, né proceduralizzato, giacché le modalità e tempistiche di svolgimento variano per ogni singolo affare;
- il fascicolo di persona fisica o giuridica: rappresenta l'agire e l'operato di un'organizzazione pubblica che si svolge attraverso una molteplicità di procedimenti amministrativi e/o di attività e/o di affari, tra di loro reciprocamente vincolati dal fatto di riferirsi alla medesima persona fisica o persona giuridica.

Tutte queste forme di fascicolazione sono rappresentative di altrettante casistiche di processo, inteso come un insieme di transazioni, tra loro in vario modo interagenti, e che a partire da una serie di condizioni iniziali mirano al raggiungimento di un risultato finale.
La natura del fascicolo informatico – al pari del fascicolo analogico – come rappresentazione, surrogato credibile di un processo e che costituisce la sua ragione funzionale essenziale veicola a cascata tutta una serie di funzioni complementari:

- una funzione gestionale a beneficio dei documenti che costituiscono il fascicolo informatico, perché la conclusione del processo rappresentato dallo stesso fascicolo permette di determinare con certezza lo stato non più attivo dei documenti stessi, consentendo così di impostare le fasi del loro ciclo di vita che si accompagna ad altrettanti trattamenti differenziati (trattamenti per la fase corrente da parte del sistema di gestione documentale, trattamenti per la fase intermedia sempre a carico del sistema di gestione documentale, trattamenti per la fase storica da parte del sistema di conservazione) e di conseguenza le attività di selezione/scarto, calibrate non sul livello granulare del singolo documento, ma sul livello delle aggregazioni fascicolari che realizza per questa via un'economia di scala e una logica di riduzione coerente della complessità;

archivistico: le cinque tipologie e i modelli organizzativi, «Archivi & Computer», XVII/2-3 (2007), p. 22-49.

- una funzione giuridica, giacché il fascicolo informatico in quanto rappresentazione credibile di un processo diviene lo strumento indispensabile per dar conto dell'agire e dell'operato dell'organizzazione pubblica, ponendosi pertanto come lo strumento concreto per l'esercizio del diritto di accesso (normato dalla l. 7 ago. 1990, n. 241) e per un più completo esercizio del diritto di accesso civico (normato dal d.lgs. 14 mar. 2013, n. 33), alla luce degli obblighi di trasparenza a carico del settore pubblico.

Figura 4 – I molteplici ambiti funzionali del fascicolo informatico

2.1.2 L'interazione degli strumenti finalizzati alla fascicolazione

Il modello italiano di gestione documentale, così come formalizzato a livello normativo, prevede specifici strumenti e la loro reciproca interazione, affinché nel contesto della gestione documentale, tanto analogica quanto digitale, la fascicolazione avvenga in forme efficienti ed efficaci, cosicché le aggregazioni di fascicoli siano in grado di adempiere appieno alle ragioni funzionali dettagliate nel precedente paragrafo. Tali strumenti sono:

- il piano di classificazione;
- il piano di fascicolazione, che sarebbe più appropriato denominare piano d'organizzazione;
- il piano di conservazione;
- la mappatura dei procedimenti amministrativi.

La classificazione è normativamente prevista dal «Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa»[31] come una funzione

[31]Alla funzione di classificazione è dedicato, in particolare, l'art. 50, co. 4, l'art. 52, co. 1, let. f), l'art. 56, co. 1, e l'art 64, co. 4.

basilare di un sistema di gestione documentale. La norma prevede, per l'appunto, che alla stessa funzione di classificazione siano sottoposti tutti i documenti comunque gestiti (usati) da un'amministrazione pubblica e non solo quella parte di essi che, tramite la registrazione di protocollo, formalmente escono per invio dalla singola area organizzativa omogenea o entrano per ricezione nella stessa[32]. Questa applicazione generalizzata della classificazione rimanda alla sua ragion d'essere: costituire la prima fase a partire dalla quale un'amministrazione pubblica organizza, in modo unitario e coerente, tutti i propri documenti in un archivio corrente. La classificazione infatti, tramite lo specifico strumento rappresentato dal *piano di classificazione*, permette di suddividere i documenti in rapporto alla funzione che tramite essi la stessa amministrazione pubblica è riuscita a svolgere. A questo livello si tratta di una prima e sommaria organizzazione della documentazione, che però non è ancora la puntuale organizzazione dei documenti in archivio corrente: all'interno di ciascuna suddivisione funzionale i documenti sono raggruppati in quanto semplicemente afferenti alla medesima funzione, ma non sono ancora relazionati in base ai singoli processi che rappresentano le concretizzazioni empiriche di quella data funzione svolta[33]. Perché ciò avvenga è necessario che a ridosso del primo passo – la classificazione – se ne attivi un secondo– la fascicolazione – che permette finalmente all'amministrazione pubblica di pervenire a una completa e concreta organizzazione dell'archivio corrente.

[32] Art. 64, co. 4. Il concetto di *area organizzativa omogenea* è stato introdotto nel nostro ordinamento dall'art. 50, co. 4, dello stesso «Testo unico». Tale concetto designa sostanzialmente l'archivio corrente e pertanto un'amministrazione pubblica, in ragione della sua minore o maggiore complessità organizzativa, può coincidere per interno con un'unica area organizzativa omogenea oppure prevedere più aree organizzative omogenee in rapporto ad altrettante sue articolazioni interne, ciascuna delle quali necessita di un proprio autonomo archivio corrente.

[33] La *funzione* svolta da un'amministrazione pubblica è un concetto essenzialmente astratto, in quanto essa si concretizza solo in un insieme di *processi* che sono quelli realmente portati a termine dalla stessa amministrazione pubblica, nell'esercizio di quella medesima funzione.

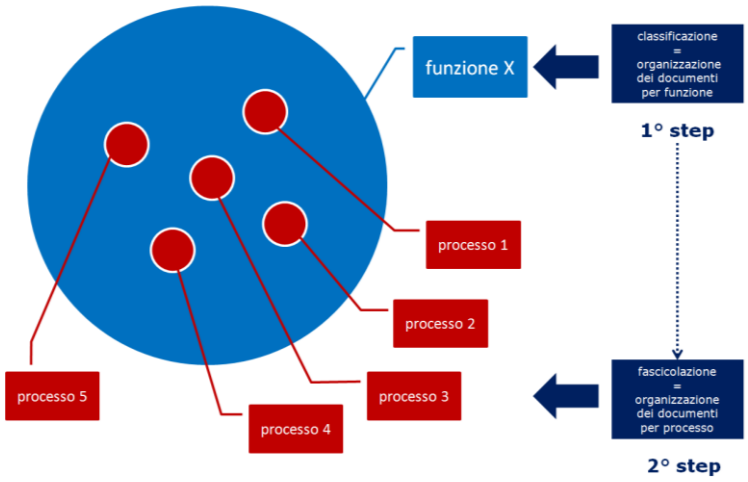


Figura 5 – Complementarietà tra lo step iniziale della classificazione e lo step finale della fascicolazione

Come a dire che la classificazione e la fascicolazione sono strettamente complementari e senza il completamento rappresentato dalla seconda la prima perde gran parte della sua ragion d'essere. Affinché però la classificazione e la fascicolazione possano agevolmente interagire, in un ambito di gestione documentale, come due fasi poste in stretta dipendenza e successione, è necessario che:

- la singola amministrazione pubblica si doti di un particolare strumento, il piano di fascicolazione. Esso ha lo scopo di indicare, in rapporto a ciascuna delle funzioni di dettaglio esplicitate negli ultimi gradi divisionali del piano di classificazione, quali sono le tipologie di fascicoli (modalità aggregative, tempistiche di chiusura, modelli di titolazioni, contenuto documentario standard) che devono essere costituiti per documentare i processi in cui si concretizza l'esercizio di quelle specifica funzione;
- il sistema di gestione documentale includa al proprio interno non solo il piano di classificazione, ma integrato con esso anche il piano di fascicolazione. In questo modo l'utente dello stesso sistema di gestione documentale, a partire dal completamento della classificazione del documento, avrebbe la possibilità di procedere contestualmente alla sua fascicolazione attraverso una sorta di procedura facilitata, in «modalità guidata»: il sistema infatti, in dipendenza dalla voce del piano di classificazione scelta per classificare il documento, prospetterebbe come suggerimenti allo stesso utente le diverse tipologie di fascicolo previste in subordine a quella stessa voce, utente che potrebbe poi da lì procedere ad assegnare il documento a un fascicolo già aperto per una certa tipologia fascicolare o a un fascicolo da aprire ex novo per quella stessa tipologia.

Oggi al contrario il piano di fascicolazione – se adottato dalla singola amministrazione pubblica – è uno strumento che nella maggior parte dei casi non è tracciato dal sistema di gestione documentale, anche se il suo inserimento nello stesso permette di conseguire indubbi vantaggi: in primo luogo, come già evidenziato, mette a disposizione degli utenti dello stesso sistema di gestione documentale una procedura «facilitata» alla fascicolazione; in secondo luogo rende disponibili una serie di procedure automatizzate che nel corso del tempo alleggerirebbero per l'utente le operazioni di fascicolazione (il piano di fascicolazione se tracciato all'interno del sistema di gestione documentale permetterebbe ad esempio, per le tipologie di fascicoli caratterizzate da una sedimentazione tipicamente annuale e da una titolazione seriale, di procedere alla riproposizione automatica per ciascun nuovo anno dei fascicoli afferenti a quelle stesse tipologie).

Va rilevato che, come in precedenza già accennato, la dicitura tradizionale di *piano di fascicolazione* risulta per certi versi non idonea, in quanto non copre per intero le finalità insite nello strumento. Se, infatti, il piano di fascicolazione, abbinato al piano di classificazione, ha lo scopo di dotare l'amministrazione pubblica, o meglio la singola area organizzativa omogenea, di un'organizzazione dei documenti in archivio corrente, è da segnalare che all'interno di un archivio corrente contemporaneo si ritrovano non solo aggregazioni documentali ascrivibili al modello del fascicolo, ma anche aggregazioni documentali definibili come *serie* che a loro volta possono suddividersi in tre fattispecie:

- le serie formate da fascicoli, in quanto a livello di archivio corrente vi è solitamente l'esigenza di raggruppare i fascicoli per macro ambiti di funzioni svolte dall'amministrazione pubblica, in modo tale che gli stessi raggruppamenti possano integralmente rappresentare (documentare) i principali rami di attività in cui si estrinseca l'esistenza della stessa amministrazione. Tali raggruppamenti per serie rendono inoltre più agevoli operazioni dalla forte natura gestionale, perché spostano a un livello più generale l'esecuzione di operazioni che altrimenti dovrebbero essere condotte al livello più granulare rappresentato dal singolo fascicolo (ad esempio trasferimento periodico all'archivio intermedio, controllo e regolazione degli accessi, adempimenti legati alla normativa sulla trasparenza, etc.);

- le serie formate da documenti non fascicolati che afferiscono a dei *repertori*, cioè a modalità particolari di registrazione dedicate a documenti dalla natura fortemente seriale e dunque caratterizzati dalla medesima forma documentaria, anche se da contenuti assai diversificati[34];

[34] Esempio paradigmatico della fattispecie delle serie legate ai repertori è quello costituito dalla serie delle determinazioni prodotte da un'amministrazione pubblica: queste infatti, a prescindere dal loro

- le serie formate da registri (ad esempio la serie dei registri di protocollo).

Pertanto alla denominazione di piano di fascicolazione sarebbe preferibile la dicitura di *piano d'organizzazione* in quanto questo strumento, in dipendenza dal piano di classificazione, dovrebbe guidare non solo la costituzione dei fascicoli, ma anche l'organizzazione dei fascicoli in serie e l'organizzazione delle serie legate a registri o ai repertori: in altre parole l'intera organizzazione dell'archivio corrente su più livelli aggregativi.

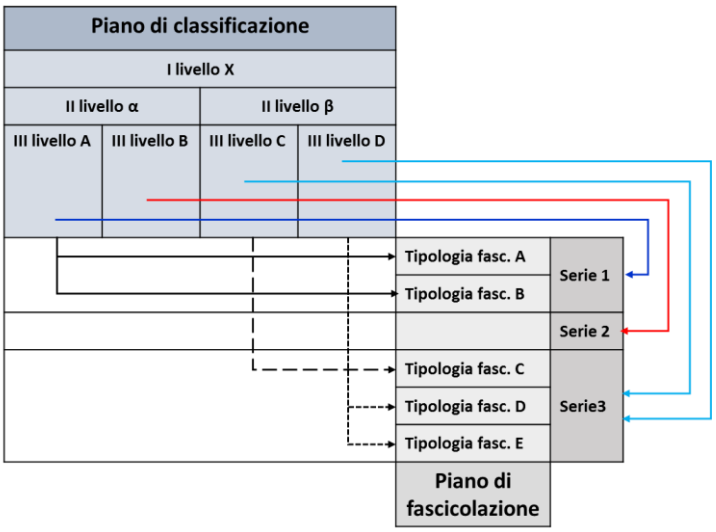


Figura 6 – Integrazione funzionale tra il piano di classificazione e il piano d'organizzazione – esempio 1

contenuto dispositivo, sono sottoposte a una particolare registrazione seriale, nella forma di uno specifico repertorio delle determinazioni, che a sua volta si sedimenta nell'archivio corrente in una serie ad hoc, formata per l'appunto dalle singole determinazioni non fascicolate. Ciò non toglie che in un caso come questo le determinazioni, oltre a formare la serie legata al repertorio, possano nel contempo essere incluse anche nei corrispondenti fascicoli, come provvedimenti finali a chiusura dei relativi procedimenti amministrativi.

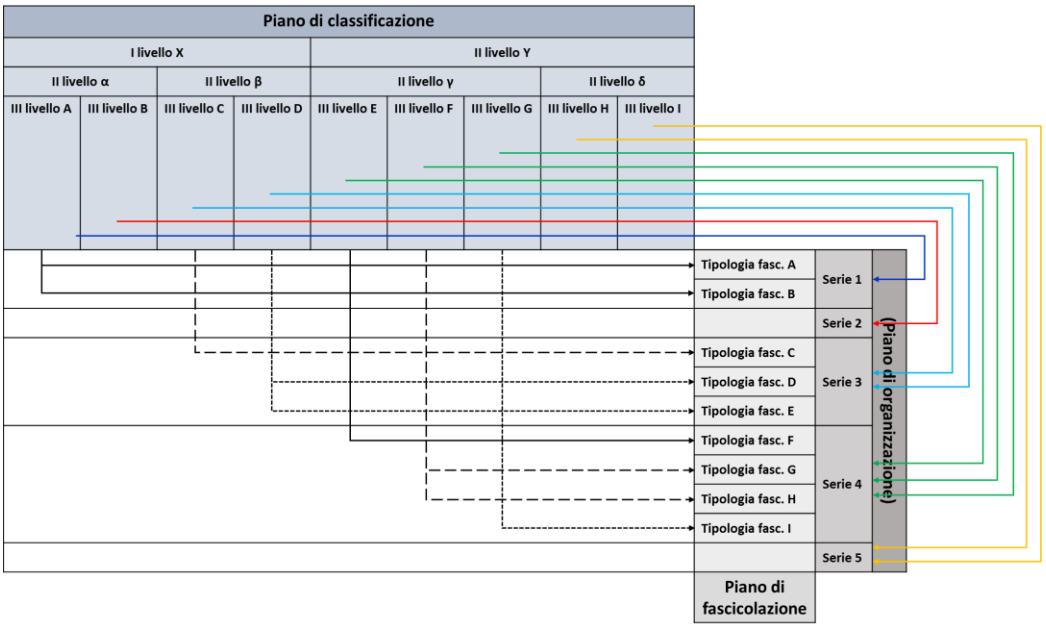


Figura 7 – Integrazione funzionale tra il piano di classificazione e il piano d'organizzazione – esempio 2

Non è un caso d'altronde che nel «Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa» non si citi mai esplicitamente il piano di fascicolazione, ma nel fare riferimento alla classificazione la norma cita contestualmente l'*organizzazione dei documenti* o il suo sinonimo di *archiviazione*[35]: il «Testo unico» sancisce in questo modo che la classificazione è funzionale all'organizzazione dell'archivio corrente, ma non si identifica per intero con essa, essendo necessario anche il complementare apporto di una funzione di archiviazione, intesa come attività regolatrice della sedimentazione di fascicoli e serie.

Va rilevato che se fascicoli e serie sono le aggregazioni documentali base anche in un contesto di archivio corrente digitale, tuttavia all'interno di un sistema di gestione documentale può emergere l'esigenza di gestire delle ulteriori aggregazioni documentali, gerarchicamente intermedie tra i fascicoli e le serie vere e proprie: si tratta di aggregazioni di fascicoli che appunto nulla hanno a che vedere con le serie in senso stretto e che possono

[35] Si fa riferimento rispettivamente all'art. 52 che prescrive che «il sistema di gestione informatica dei documenti … deve … garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione … adottato» e all'art. 50, co. 4, che presenta la seguente formulazione: «ciascuna amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione».

essere suddivise in tre differenti tipologie, a loro volta caratterizzate da distinte finalità e nature:

- aggregazioni di fascicoli che sono oggetto di una precisa pianificazione da parte del sistema di gestione documentale e che pertanto sono previste dal piano di fascicolazione. Esse a loro volta si suddividono in due sottotipologie:
  - una prima sottotipologia rappresentata da quell'aggregazioni di fascicoli che potrebbe essere denominata *iperfascicolo*: si tratta di un'aggregazione di fascicoli di diversa tipologia – sia fascicoli di tipo procedimentale che fascicoli di tipo non procedimentale – e contrassegnati da diverse classificazioni. Tale aggregazione si rende necessaria in quanto complessivamente documenta «entità organiche» in relazione a ragioni normative, a ragioni funzionali o di altro genere (esempi di iperfascicolo sono quelli che comunemente sono denominati «fascicolo di persona» o «fascicolo di fabbricato»);
  - una seconda sottotipologia rappresentata da quell'aggregazione di fascicoli che potrebbe essere denominata *raggruppamento di fascicoli*: si tratta di un'aggregazione di fascicoli contrassegnati da un'identica classificazione, rispetto alla quale rappresentano un'articolazione di maggior dettaglio. Tale aggregazione si rende necessaria in quanto risponde ad esigenze organizzative ed operative dell'organizzazione;
- aggregazioni di fascicoli che sono di natura meramente estemporanea e che dunque non sono, in genere, regolate né dal piano di classificazione né tantomeno dal piano di fascicolazione[36]. Tali aggregazioni possono essere denominate *dossier* (ad esempio il dossier prodotto in vista di un evento, come una mostra, che non rientra tra le attività istituzionali consuete dell'organizzazione).

Affinché la produzione e gestione dei fascicoli anche informatici avvenga in forme efficienti ed efficaci all'interno del sistema di gestione documentale, è necessario che all'interno di questo non solo interagiscano funzionalmente tra loro il piano di classificazione e il piano d'organizzazione come sopra illustrato, ma è anche indispensabile che quest'ultimo si integri sempre dal punto di vista funzionale con altri due strumenti:

- il *piano di conservazione*, previsto originariamente dall'art. 68, co. 1, del «Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa»[37]. Questo strumento ha lo scopo di permette all'organizzazione di

[36] Tali aggregazioni estemporanee dovrebbero, invece, essere oggetto di regolamentazione in merito ai loro tempi di conservazione al fine di evitare, nel lungo periodo, un «appesantimento» del sistema di gestione documentale.

[37] La formulazione dell'art. 68, co. 1, è la seguente: «il servizio per la gestione dei flussi documentali e degli archivi elabora ed aggiorna il piano di conservazione degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e

definire a priori – in base alle proprie esigenze operative o in ragione di quanto disposto dalle norme vigenti – per quanto tempo i documenti debbono essere mantenuti all'interno del sistema di gestione documentale per esigenze correnti o semicorrenti e una volta che sia decorso tale intervallo di tempo se gli stessi documenti debbano essere selezionati per la conservazione a tempo indefinito in un distinto sistema di custodia o piuttosto non debbano essere selezionati per lo scarto. La previsione di tali tempistiche può essere ragionevolmente formulata dalla singola organizzazione tramite una riflessione che sia incentrata soprattutto sulla natura dei propri processi di *business*: infatti, il periodo di mantenimento dei documenti all'interno di un sistema di gestione documentale dipende direttamente dalle scansioni del loro ciclo di vita – fase corrente o attiva, fase semicorrente o semiattiva e fase non più corrente o non più attiva – e il passaggio dall'una all'altra di esse è a sua volta segnato dall'andamento di inizio e conclusione dei processi a cui gli stessi documenti partecipano; allo stesso modo la selezione che deve stabilire, al termine del periodo di mantenimento, se i documenti siano da destinare alla conservazione permanente o allo scarto, può essere programmata secondo logiche coerenti e affidabili solo qualora essa sia il risultato di un'analisi delle tipologie e della natura dei processi rappresentati in modo credibile dai documenti stessi. Tutto ciò porta a concludere che le diverse tempistiche previste dal piano di conservazione dovrebbero essere strutturate secondo una logica per processi e dunque, in ultima analisi, dovrebbero essere funzionalmente calibrate sui diversi tipi di aggregazioni documentali – fascicoli e serie – formalizzate dal piano di organizzazione dell'archivio corrente, in modo tale che all'interno del sistema di gestione documentale non solo sia preventivamente organizzata l'aggregazione dei documenti in fascicoli e/o serie, ma per queste stesse aggregazioni sia programmaticamente impostato il loro periodo di mantenimento e il momento di successiva destinazione alla conservazione permanente o allo scarto[38];

di conservazione permanente dei documenti, nel rispetto delle vigenti disposizioni». Tale formulazione risulta poco precisa, giacché essa induce erroneamente a ritenere che il piano di conservazione debba essere integrato direttamente con il piano di classificazione, invece che con il piano d'organizzazione, cui peraltro non si faceva esplicito riferimento nel Testo unico.

[38] È evidente che in questa visione di gestione documentale l'eventuale scarto non viene operato a livello di singolo documento, ma è realizzato ad un livello aggregativo superiore, dunque a partire dalle aggregazioni documentali – fascicoli o serie – a cui il singolo documento di volta in volta appartiene. Questo «approccio sistemico allo scarto» è d'altro canto perfettamente coerente con il nostro ordinamento giuridico generale, che solo eccezionalmente stabilisce dei periodi obbligatori minimi di mantenimento per singole tipologie di documenti e che con riferimento al solo specifico valore dei documenti in sede giudiziale ha esplicitato con norme di diritto positivo, in particolare nel Codice civile, i termini entro cui si prescrivono i diritti per il cui godimento i documenti stessi possono essere esibiti dalle parti come mezzo probatorio. Pertanto, stante tale impostazione dell'ordinamento giuridico generale, nulla ostacola una definizione da parte delle organizzazioni di piani di conservazione calibrati per processo e o meglio per aggregazioni documentarie, siano esse fascicoli o serie.

- la *mappatura o tabella dei procedimenti amministrativi* svolti da una determinata amministrazione pubblica. Si tratta di uno strumento la cui predisposizione, peraltro già prevista dai primi regolamenti applicativi della legge 241/1990, è stata resa esplicitamente obbligatoria dalla recente normativa in tema di trasparenza sull'agire del comparto pubblico e di lotta alla corruzione. In particolare l'art. 35 del decreto «Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione delle informazioni»[39] dispone, per le amministrazioni pubbliche, l'obbligo di pubblicare una serie di informazioni dettagliate e utili all'identificazione e alla descrizione delle tipologie di procedimenti amministrativi di loro competenza[40]. In aggiunta a tale norma l'art. 3 del CAD stabilisce il diritto da parte di chiunque di poter utilizzare le soluzioni e gli strumenti delle tecnologie dell'informazione e della comunicazione – così come regolate dal Codice stesso – nei rapporti con i soggetti pubblici, anche al fine dell'esercizio del diritto di accesso e per la reale partecipazione al procedimento amministrativo.

L'insieme di queste finalità insite nella mappatura dei procedimenti amministrativi sono effettivamente conseguibili nella misura in cui tale strumento riesca a interagire, dal punto di vista funzionale, con il piano di organizzazione dell'archivio corrente, in particolare con quella sua parte relativa all'organizzazione dei fascicoli. Infatti l'integrazione tra questi due dimensioni operative permette di:

- stabilire un legame puntuale tra le tipologie di procedimenti amministrativi che spettano, in astratto, a un'amministrazione pubblica e i singoli procedimenti effettivamente e storicamente svolti in quanto materialmente documentati da quella loro concreta manifestazione rappresentata dai pertinenti fascicoli;

- fornire ai cittadini degli strumenti efficaci per individuare in concreto le aggregazioni fascicolari rispetto a cui richiedere eventualmente il diritto di accesso e su cui eventualmente far valere la loro partecipazione ai singoli procedimenti amministrativi;

- mettere a disposizione della singola amministrazione pubblica degli strumenti efficaci per la ricerca e il recupero dei fascicoli attinenti a legittime richieste di accesso o che documentano dei procedimenti amministrativi rispetto a cui far valere la partecipazione dei soggetti legittimati;

- individuare, nell'ambito dell'archivio corrente, quelle aggregazioni fascicolari che sono sottoposte a più stringenti obblighi di legge, a seguito della normativa sul

[39] D.lgs. 14 mar. 2013, n. 33.

[40] L'obbligo per le amministrazioni pubbliche a rendere disponibili particolareggiate descrizioni relative ai propri procedimenti amministrativi è ribadito anche da due deliberazioni emanate dall'Autorità nazionale anticorruzione: la deliberazione 24 set. 2013, n. 50, e la deliberazione 1 ago. 2013, n. 71.

diritto di accesso, sul procedimento amministrativo, sulla trasparenza dell'agire pubblico e sulla lotta alla corruzione.

In altri termini l'interazione funzionale tra la tabella dei procedimenti amministrativi e il piano di organizzazione dell'archivio corrente – in particolare di quella sua parte costituita dal piano di fascicolazione – da un lato consente l'esercizio concreto, efficace ed efficiente dell'accesso e della trasparenza[41] e dall'altro permette ai fascicoli di svolgere appieno quella loro funzione giuridica che nella precedente figura 4 è stata indicata come la ragione funzionale derivata delle aggregazioni fascicolari.

[41] È da rilevare che il legislatore, nell'emanare la normativa in tema di trasparenza sull'agire pubblico e di lotta alla corruzione, ha rimarcato in termini esclusivi il riferimento ai soli procedimenti amministrativi, tralasciando pertanto tutti quei processi che oggi si sviluppano all'interno di un'amministrazione pubblica, ma che non risultano in alcun modo procedimentalizzati. Rispetto a tale limite va osservato che una mappatura che si limitasse ai soli procedimenti amministrativi in senso stretto fornirebbe una visione solo parziale sull'agire del comparto pubblico. In aggiunta a ciò poter disporre di uno strumento che censisca tutti i processi che avvengono all'interno di un'organizzazione pubblica – a prescindere che possano o meno qualificarsi come procedimenti amministrativi – costituisce un'imprescindibile base di conoscenza, indispensabile per impostare e mantenere aggiornato nel tempo il piano di organizzazione dell'archivio corrente, in particolare quella sua parte rappresentata dal piano di fascicolazione.

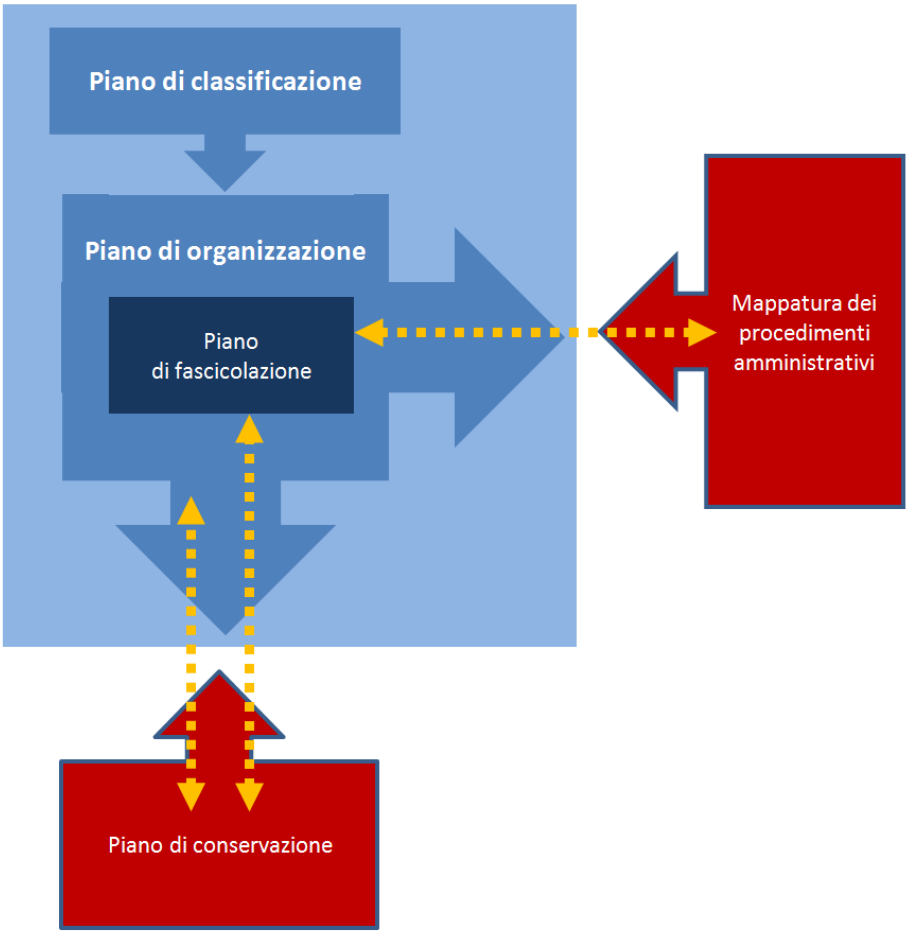
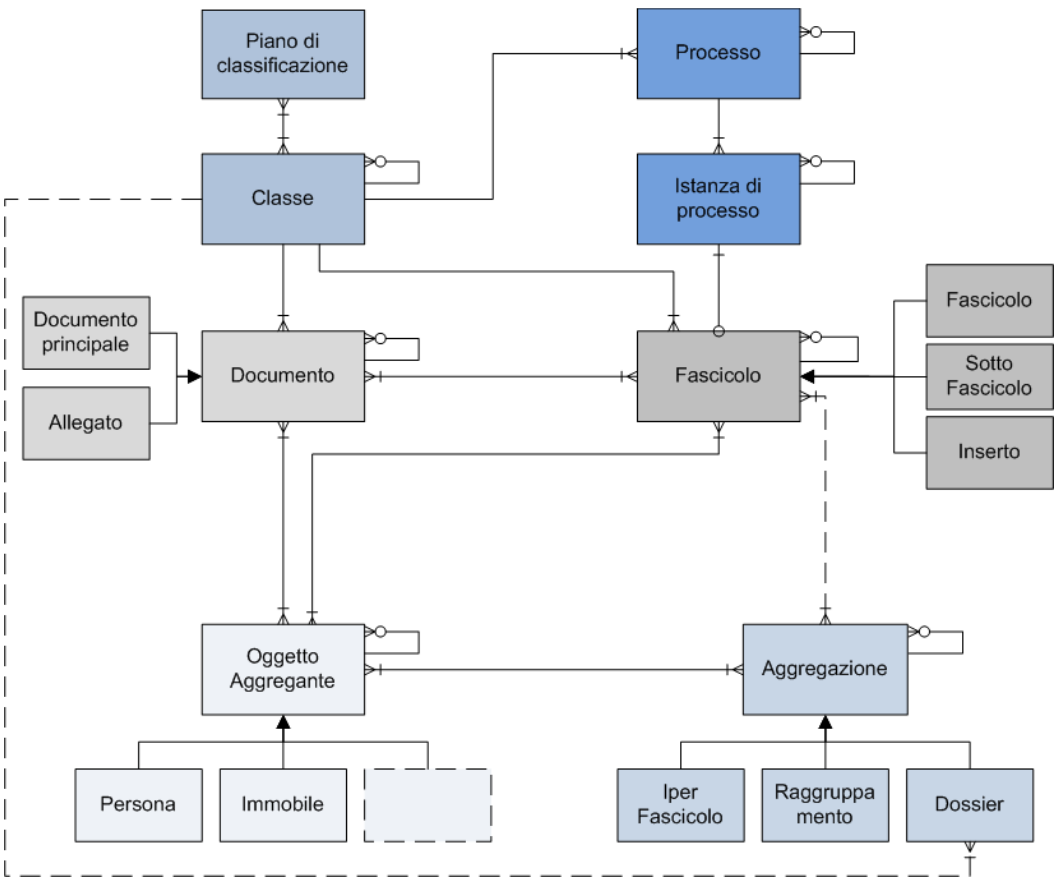


Figura 8 – Interazione degli strumenti per una efficiente ed efficace produzione e gestione dei fascicoli informatici

Allegato 1.2 – Modello E-R

Il seguente diagramma rappresenta, utilizzando la notazione E-R, una possibile formalizzazione dei contenuti esposti nel documento.

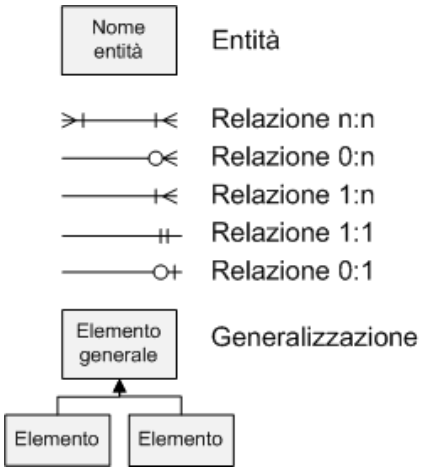
Il modello è focalizzato in particolare sul concetto di fascicolo e sulle sue possibili forme di aggregazione; non include invece, per una scelta di semplificazione, altre entità (ad esempio quelle necessarie a dare conto delle relazioni esistenti tra gli oggetti documentali e la realtà organizzativa all'interno della quale si forma l'archivio) che dovrebbero certamente essere prese in considerazione in una riflessione più estesa sui sistemi documentali.



La revisione della tabella è stata curata da Valeria Sisti (Dedagroup Public Services) e Costantino Landino (Istituto centrale per gli Archivi)

Per la lettura del diagramma rappresentato in notazione «crow.s foot»[42], si riporta anche una leggenda delle relazioni con le rispettive cardinalità.

Le relazioni indicate con la linea spezzata sono suggerite, ma da approfondire.



[42] GORDON C. EVEREST, *Users Do Logical Database Design. CAD/CAM Databases '87 Conference Proceedings, Management Roundtable*, Inc., Boston, MA, 1987 April.

3. Prova d'identità, firma e sigillo elettronico

capitolo a cura di[43]

Una famosissima vignetta pubblicata ai tempi del primo grande sviluppo del web mostrava un cane su una sedia davanti a una scrivania con un personale computer che dice a un altro cane: "Su Internet nessuno sa che sei un cane". Oggi con lo sviluppo dell'Intelligenza Artificiale possiamo integrare questa frase con "su Internet nessuno sa che sei un robot". Queste affermazioni introducono il principio che nel mondo cosiddetto cibernetico l'identità è la base per ogni attività, a maggior ragione se la propria identità digitale è la base per conferire valore legale alle proprie attività istituzionali o amministrative.

In questo capitolo verranno affrontate a vari livelli di approfondimento le tematiche della prova di identità rispetto alla fruizione di documenti informatici (non solo file, ma anche record e quindi anche dati in memoria fisica e logica). Il tema dell'identità deve essere analizzato anche dal punto di vista del regolamento europeo 679/2016 sulla protezione dei dati personali (GDPR) visto che la fruizione e gestione di documenti informatici deve essere conforme anche a queste specifiche regole.

Si parlerà poi della sottoscrizione informatica, del suo valore legale a livello europeo (regolamento UE 910/2014 – eIDAS) associata alla fattispecie operativa del motivo per il quale si firma un documento ovvero la funzione della sottoscrizione. Con il regolamento eIDAS è stato introdotto anche il sigillo elettronico allo scopo di garantire la certezza dell'origine e l'integrità dei dati ai quali il sigillo è applicato.

Il sigillo (come vedremo) è praticamente identico alla firma dal punto di vista tecnologico ma differente sul piano giuridico. Il fatto che nel Codice dell'amministrazione digitale (Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni – CAD) non si parla di sigillo elettronico impone di fare una serie di analisi e valutazioni su questa fattispecie al

[43] Il capitolo nasce dalle riflessioni e dal confronto del gruppo di lavoro coordinato da Giovanni **Manca** (Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale) e composto da Rosamaria **Bertè** (Corte dei conti), Gabriele **Bezzi** (Polo archivistico Emilia-Romagna), Roberto **Carosi** (Dedagroup Public Services), Cristiana **Carratù** (Corte dei conti), Marco **Ceccolini** (Lombardia Informatica), Laura **Flora** (Istituto nazionale di astrofisica), Silvia **Ghiani** (Lepida Spa), Stefano **Ianniello** (Agenzia per l'Italia digitale), Carlo **Lentini** (Inail), Alessandro **Todeschini** (Ministero della giustizia), Brizio **Tommasi** (Consob), Giovanni **Veterini** (Sogei).

fine di profilarne il valore giuridico e l'efficacia probatoria coordinandole a livello nazionale, il tutto considerando che eIDAS come regolamento europeo si pone ad un rango normativo superiore della Legislazione nazionale (nei limiti dei trattati comunitari) e del CAD in particolare.

Per completare le attività, vista anche la gioventù del sigillo elettronico saranno illustrati alcuni casi d'uso di possibile utilizzo del sigillo stesso. Nell'ambito del ciclo di vita di questa pubblicazione, alcuni casi d'uso saranno immediatamente applicabili, altri che saranno indicati come significativamente utili richiederanno un aggiornamento normativo.

Infine saranno indicati anche degli scenari dove l'utilizzo del sigillo elettronico risulterebbe seducente ma poi, in verità, è ampiamente fuori dai scopi o addirittura sbagliato.

3.1 Introduzione

Con la nascita nella metà degli anni '90 della Rete Unitaria della Pubblica Amministrazione – RUPA (Direttiva del Presidente del Consiglio dei Ministri 5 settembre 1995) si è creato il problema di attribuire un valore giuridico ai documenti digitali che vi transitavano.

In tal senso nella Legge 59/97 (articolo 15, comma 2) si conferiva per la prima volta valore giuridico a quello che poi sarebbe diventato il documento informatico.

Per analogia con il mondo cartaceo venne introdotta la firma digitale all'epoca normata tecnicamente nel DPCM 8 febbraio 1999. Poi è arrivata la direttiva 1999/93/CE che ha introdotto la firma elettronica, la firma elettronica avanzata e la firma elettronica qualificata.

Nel recepimento nazionale di questa direttiva è cominciata l'azione ondivaga dei vari Governi che si sono succeduti. In ogni versione della normativa primaria di settore veniva modificato il valore giuridico e l'efficacia probatoria delle sottoscrizioni. Questo oltre vent'anni dopo richiede un aggiornamento sul valore delle firme ovvero del perché si firma e di come la tecnologia stabilita a livello europeo dal regolamento 910/2014 (noto come eIDAS e operativo dal 1 luglio 2016) influenza il significato della sottoscrizione. Nella prassi quotidiana di firma ma si dimentica perché si firma in termini giuridici.

Nella conoscenza comune ci sono dei limiti culturali sul tema quindi, per prima cosa è bene chiarire che la sottoscrizione informatica non è una sottoscrizione in senso letterale perché il documento informatico non mantiene il senso dello spazio.

Quindi la sottoscrizione informatica quando è apposta come digitale (il livello più sicuro dal punto di vista informatico e dal valore giuridico e probatorio più elevato e a più ampio spettro di applicazione) è realmente un numero binario (oggi di 2048 bit) calcolato sulla

base di una serie di operazioni matematiche e crittografiche che in questa sede non si vuole approfondire.

Essendoci a livello comunitario piena equivalenza tra firma digitale/qualificata e sottoscrizione autografa non si può prescindere dal citare Francesco Carnelutti per il quale la firma è il "segno grafico riconducibile al soggetto".

La firma digitale è senz'altro un numero riconducibile al soggetto anche se a documento differente si associa un numero binario differente.
Nel mondo archivistico e diplomatistico ovvero considerando il mondo cartaceo abbiamo la suddivisione degli esperti in sigla, visto, firma e sottoscrizione. Su questo tema e la relazione con il mondo digitale si segnala questo articolo.
Sempre il già citato Carnelutti esplicita le varie funzioni della firma autografa:

- la funzione indicativa che individua e distingue chi appone la firma dagli altri soggetti giuridici;
- la funzione probatoria ovvero la sottoscrizione autografa fa piena prova della provenienza del documento;
- la funzione dichiarativa ovvero l'espressione del consenso del soggetto cui la firma appartiene.

Possiamo anche considerare una funzione informativa applicabile quando la firma ha un ruolo di "presa visione" del documento. Questo scenario dottrinale si deve coordinare con le sottoscrizioni informatiche al fine di comprendere quali legami ci possono essere tra "segni" autografi e evidenze informatiche.

Per un ulteriore approfondimento sul tema si rinvia a questo articolo.

Il sigillo elettronico

Nel mondo digitale a partire dalla data di piena attuazione di eIDAS (1 luglio 2016) è stato introdotto il sigillo elettronico definito come *"dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità dei dati"*. Come è evidente il sigillo elettronico è molto importante nell'ambito dell'identità digitale (origine dei dati) e della firma (integrità dei dati).

Identità e firma

Lo scenario dei social network ha introdotto nuove esigenze sulla natura dell'identità digitale e sul nuovo legame che questa può avere con la sottoscrizione informatica nel suo senso giuridico e tecnico più ampio.

Non è trascurabile anche il ruolo della nuova Carta d'Identità Elettronica (CIE 3.0) e del Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese (SPID) come strumenti personali di autenticazione informatica.

Su questo tema saranno dedicati altri due articoli. Il primo analizzerà quanto stabilito nell'articolo 20, comma 1-bis del vigente Codice dell'amministrazione digitale (CAD). In particolare il tema del documento informatico formato previa identificazione informatica, attraverso un processo avente i requisiti forniti dall'AgID con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore.

Il secondo, sul medesimo tema, proporrà uno scenario tecnologico ai fini delle Linee guida che il vigente CAD stabilisce essere le nuove regole tecniche di riferimento.

Come sinteticamente abbiamo illustrato la relazione tra identità del soggetto e sottoscrizione informatica rappresenta un tema innovativo e complesso.

I social network oltre evidenziare grossi problemi sulla protezione dei dati personali hanno messo in evidenza la rilevanza del rapporto tra la propria identità e i "post" che pubblico in rete.

Negli scenari della pubblica amministrazione questi temi non sono differenti quando scompare il soggetto come entità fisica e il documento è formato ma reso virtuale nel mondo del cloud che come è noto elimina la locazione fisica transazionale riconducendola totalmente a principi logici.

3.2 Il regolamento europeo 910/2014 (eIDAS)

L'analisi, la descrizione e i commenti sulle tematiche di prova di identità e firma trovano la loro normativa primaria di riferimento nel "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" (nel seguito regolamento). Per i suoi contenuti principali questo regolamento viene anche indicato con l'acronimo eIDAS – electronic IDentification Authentication and Signature).

In questa sede è utile fornire un inquadramento generale delle finalità principali del regolamento per poi, in modo graduale, fornire maggiori dettagli sui temi oggetto del presente documento: l'identità digitale, la sottoscrizione informatica e la nuova fattispecie del sigillo elettronico.

Il considerando 2 esplicita la finalità principale del regolamento ovvero fornire "una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche, in

modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'eBusiness e del commercio elettronico, nell'Unione europea".

Questa posizione scaturisce anche dalla consapevolezza che la direttiva 1999/93/CE (abrogata definitivamente il 1 luglio 2016 allo scoccare della data di piena operatività del regolamento) "trattava la firme elettroniche senza fornire un quadro transfrontaliero e transettoriale completo per transazioni elettroniche sicure, affidabili e di facile impiego" (considerando 3).

Per conferire alla norma il necessario rafforzamento il Legislatore comunitario ha scelto lo strumento del regolamento. Come è noto l'articolo 288, par. 2 del Trattato comunitario stabilisce che "il regolamento ha portata generale. Esso è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri".

In modo sintetico e in modo omogeneo con gli obiettivi del documento nel seguito del capitolo tratteremo dei tre temi attinenti al nostro obiettivo. Prima di iniziare l'analisi, qualche breve nota sui termini utilizzati e sull'approfondimento degli argomenti. La versione in lingua inglese di riferimento del testo del regolamento parla di "identification schemes". La traduzione "regimi di identificazione" non è coerente con il linguaggio giuridico e tecnico del settore quindi verrà utilizzata la frase "schemi di identificazione".

Per quanto attiene al sigillo elettronico, considerata la sua totale novità normativa introdotta in sede di regolamento, l'analisi sarà svolta con un maggior approfondimento rispetto alle sottoscrizioni informatiche.

3.2.1 Schemi di identificazione

Il regolamento distingue tra "identificazione elettronica" e "autenticazione elettronica". La normativa italiana tratta il tema nel D.Lgs. 7 marzo 2005, n. 82, Codice dell'amministrazione digitale (nel seguito CAD) riferendosi alla definizione di identità elettronica base per sviluppare il tema e la normativa per il Sistema pubblico per la gestione delle identità digitali di cittadini e imprese (SPID).

L'identificazione elettronica è definita nel regolamento 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 un persona giuridica. L'autenticazione è definita come un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica.

Nella normativa nazionale l'autenticazione viene riferita al documento informatico quindi conviene fare riferimento all'identità digitale definita nel CAD come la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata

attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64 (riferito a SPID). Per concludere lo scenario delle definizioni è indispensabile ricordare che le definizioni del regolamento sono anche le definizioni del CAD per questione di rango normativo ma anche per la esplicita regola del CAD stabilita nell'articolo 1, comma 1-bis.

Dello SPID e della sua armonizzazione con gli schemi di identificazione comunitari parleremo nel seguito. In questo paragrafo illustriamo le regole comunitarie per gli strumenti di identificazione on line, in particolare delle facoltà degli Stati membri di notifica alla Commissione europea di schemi di identificazione. Gli schemi ove accettati e pubblicati dalla Commissione devono essere accettati da tutti gli Stati membri. L'Italia ha già notificato con successo il sistema SPID e si appresta a notificare la Carta d'Identità Elettronica (CIE).

E' opportuno sottolineare che gli Stati membri possono proseguire nell'utilizzo di strumenti di identificazione on line (in Italia la TS-CNS, Tessera Sanitaria – Carta Nazionale dei Servizi) senza che, in alcun modo, il regolamento imponga l'adozione di uno strumento di identificazione on line comune a livello europeo. Il regolamento stabilisce le regole e i requisiti per la notificazione. Non essendo obiettivo del presente documento il dettaglio delle procedure ci si limita a ricordare alcuni principi basilari.

Uno schema di identificazione è ammissibile per la notifica se soddisfa tutti requisiti dell'articolo 7 di eIDAS. Lo Stato membro che notifica è responsabile della parte che rilascia i sistemi di identificazione (nell'ambito dello schema) e della parte che gestisce la procedura di autenticazione.

I dettagli delle regole e in particolare i livelli di sicurezza e le modalità di riconoscimento della persona fisica o giuridica sono stati ripresi in dettaglio nell'ambito di SPID, quindi ne parleremo nel paragrafo ad esso dedicato.

Concludiamo questo paragrafo con il cruciale concetto che gli Stati membri sono tenuti a riconoscere gli schemi di identificazione che altri Stati hanno notificato con successo alla Commissione europea.

Nasce così l'interoperabilità delle identità digitali pur rimanendo a livello nazionale il principio dell'identità personale la cui attribuzione rimane esclusiva dello Stato membro.

3.2.2 Firma elettronica

Nel regolamento non ci sono modifiche significative rispetto al quadro normativo previgente definito dalla direttiva 1999/93/CE.

A parte la modifica della definizione di firma elettronica che è conseguenza di apposite definizioni per l'identificazione informatica gli altri principi sul tema sono sostanzialmente inalterati.

A titolo di esempio possiamo dire che viene confermato il principio di non disconoscimento del documento informatico e delle firme elettroniche, in base al quale non può essere negata dignità e rilevanza giuridica ad una firma elettronica, solo in ragione della sua forma, appunto, elettronica.

Un principio cruciale sotto il profilo dell'efficacia probatoria è stabilito nell'articolo 25, paragrafo 2 del regolamento che prevede l'automatica equiparazione, per gli effetti giuridici, della firma elettronica qualificata alla firma autografa.

Il valore della firma qualificata è stabilito nell'ordinamento nazionale considerato che questi sono differenti e imposizioni comunitarie potrebbero portare squilibri normative nel mercato interno.

Per quanto attiene alla generazione della firma elettronica qualificata, il regolamento stabilisce regole per uniformare gli strumenti di firma elettronica anche al fine della loro diffusione all'interno del territorio dell'Unione Europea.

Gli obiettivi di tali principi sono ben descritti nel Considerando 50 del regolamento:

"Le autorità competenti negli Stati membri utilizza[va]no formati diversi di firme elettroniche avanzate per firmare elettronicamente i loro documenti" bisogna quindi "garantire che almeno alcuni formati di firma elettronica possano essere supportati elettronicamente dagli Stati membri allorché ricevono documenti firmati elettronicamente".

In questa sede il tema è analizzato nel paragrafo 4.3 per naturale analogia con quanto stabilito anche per il sigillo elettronico avanzato.

E' opportuno ricordare che la Firma Elettronica Avanzata (FEA) stabilita nel regolamento ha efficacia diversa da quella nazionale. Il Titolo V del DPCM 22 febbraio 2013 stabilisce i requisiti minimi affinché un particolare prodotto/servizio posso essere una FEA e quindi avere l'efficacia probatoria stabilita nel CAD.

Come conseguenza di questa efficacia si è sviluppato in Italia un significativo mercato di FEA basata sulla sottoscrizione grafometrica ovvero sulla firma apposta ad un documento mediante uno stilo elettronico su una tavoletta digitale tecnologicamente adeguata.

Nonostante lo sviluppo, soprattutto in ambito bancario e assicurativo, di questa tecnologia non è ancora risolto il problema della verifica "generalizzata" della FEA grafometrica. In altre parole la firma apposta con uno specifico prodotto di mercato può essere sottoposta a perizia grafologica solo con la tecnologia associata al prodotto utilizzato per firmare.

Nell'ambito delle attività dell'associazione AIFAG (Associazione Italiana Firma elettronica Avanzata biometrica e grafometrica) si è individuato un percorso di interoperabilità che si descrive di seguito.

Ricordiamo brevemente come si opera quando si firma in modalità grafometrica.

Il sottoscrittore firma il documento (nella quasi totalità dei casi pratici un documento in formato PDF) utilizzando uno stilo attivo o passivo (attivo: alimentato, passivo: non alimentato) su un dispositivo in grado di raccogliere il tratto della sottoscrizione e, in maniera protetta, di connetterlo in modo indissolubile a quanto si vuole sottoscrivere.

Poiché le strutture dati della firma grafometrica prodotte dalle varie soluzioni sono leggibili solo dallo strumento di analisi grafologica dello stesso fornitore è molto utile disporre di strutture dati omogenee prodotte su un tracciato standard per i dati grafometrici, che in tal modo possono essere analizzati da un qualsiasi strumento di analisi in grado di elaborare questo tracciato.

Naturalmente devono essere applicate le regole stabilite nel Provvedimento prescrittivo del Garante per la protezione dei dati personali (n. 513/2014) che impone di rendere disponibili i dati biometrici solo su richiesta dell'Autorità Giudiziaria quando si è in presenza di un contenzioso.

Nel cennato Provvedimento sono fornite le Regole di protezione del dato biometrico e le indicazioni organizzative per un suo trattamento rispettoso della privacy.

Una volta che il dato è estratto dal suo ambiente protetto è possibile elaborarlo in modo "interoperabile".

E' indispensabile generare i dati in un formato standard; a questo scopo è indispensabile produrre i dati biometrici in formato ISO/IEC 19794-7 (2014). Questo è lo standard di riferimento sul tema.

Nel citato standard vengono stabilite le strutture dati e la rappresentazione dei parametri biometrici che caratterizzano la sottoscrizione grafometrica.

Per esempio le coordinate cartesiane X e Y del tratto grafico, il tempo di acquisizione della coordinata e la differenza di tempo calcolata sulla base della frequenza di campionamento del dispositivo di acquisizione dati. Tutti questi dati sono rappresentabili in un modo standard secondo un tracciato record e la rappresentazione dei dati definita in ISO/IEC 19785-1.

Altri dati sono utili per l'analisi in un giudizio anche se non contemplati nello standard ISO/IEC 19794-7. Tra questi i dispositivi utilizzati per la sottoscrizione e l'acquisizione del dato. Questo potrebbe essere utile, ad esempio, per determinare la calibrazione della pressione per un dispositivo che ne consente l'acquisizione.

Negli ultimi mesi si sono verificati alcuni eventi che migliorano lo scenario che si sta analizzando in questa sede. La sicurezza dei sistemi grafometrici è rimasta stabile con alcune punte di eccellenza. La certificazione dei sistemi ai sensi dei Common Criteria (standard di riferimento per la sicurezza di questo tipo di hardware e software) non è mai

decollata per la mancanza di domanda sul tema. Le aziende investono se ci sono obblighi di legge o specifica domanda del marcato e non c'è né l'una, né l'altra cosa.

Molto importante è la pubblicazione da parte degli esperti di AGI (Associazione Grafologica Italiana) del documento "Le buone prassi per l'analisi forense di firme grafometriche" dove si danno fondamentali indicazioni ai periti grafologi per la conduzione professionale della perizia grafologica in ambiente grafometrico.

Sul piano dell'interoperabilità, proseguendo quanto detto in precedenza, lo stato dell'arte del mercato potrebbe essere adeguato se a livello normativo ci fosse l'obbligo di rappresentazione standard delle sottoscrizioni "in chiaro". Per raggiungere questo obiettivo i tempi sono maturi.

AIFAG ha aggregato le varie professionalità, indispensabili per raggiungere l'obiettivo. In testa le aziende produttrici, poi i grafologi, esperti del Notariato e anche le istituzioni con il coinvolgimento di AgID (l'Agenzia per l'Italia Digitale).

L'ultimo sforzo potrebbe concretizzarsi con un gruppo di lavoro coordinato da AgID per la scrittura delle Linee guida previste nell'articolo 61, comma 6 delle Regole tecniche sulle sottoscrizioni informatiche, DPCM 22 febbraio 2013.

6. (…), al fine di favorire la realizzazione di soluzioni di firma elettronica avanzata, l'Agenzia elabora Linee guida sulla base delle quali realizzare soluzioni di firma elettronica avanzata conformi alle presenti regole tecniche.

In tali Linee guida si possono indicare metodi "legali" per decifrare i dati biometrici della firma, per la verifica della stessa a prescindere dallo strumento informatico utilizzato dal perito (oggi l'interoperabilità è puramente teorica) con una visione comune di istituzioni, aziende ed esperti.

Queste linee guida potrebbero anche indicare buone prassi nella rappresentazione della firma "a vista".

In numerosi casi (Es. l'acquisto di una SIM card) la firma riportata sul documento viene deformata e rimpicciolita rendendo scarsamente efficace la perizia in sede giudiziaria.

Raggiunta l'interoperabilità i limiti stabiliti nell'articolo 60 del DPCM 22 febbraio 2013 che stabilisce limiti d'uso della FEA "La firma elettronica avanzata realizzata in conformità con le disposizioni delle presenti regole tecniche, è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore e …" il soggetto proponente la soluzione di FEA (peraltro in contraddizione con i principi del CAD sul tema) possono essere eliminati semplificando e ampliando il mercato di riferimento.

3.2.3 Il sigillo elettronico

Il regolamento introduce il sigillo elettronico come l'insieme dei dati in forma elettronica acclusi, o connessi tramite associazione logica, ad altri dati in forma elettronica, per garantirne la provenienza e l'integrità. Vedremo che il sigillo ha forti analogie con la sottoscrizione informatica (intesa come indicazione sintetica delle varie fattispecie di firme disponibili), infatti il regolamento definisce oltre al sigillo elettronico, il sigillo elettronico avanzato e qualificato. Solo ad una prima lettura, con l'indubbio vantaggio di una immediatezza comunicativa, il sigillo elettronico può essere considerato la firma della persona giuridica. Nella realtà occorre valutare, in coordinamento con l'ordinamento nazionale, (o a livello europeo con i singoli ordinamenti) quanto il sigillo possa essere firma e con quali limiti. In questo paragrafo ricordiamo che per il sigillo elettronico qualificato il regolamento stabilisce che gode della presunzione di integrità dei dati e di correttezza dell'origine dei dati a cui il sigillo è associato. In questo principio vanno individuati e sviluppati gli ambiti di utilizzo del sigillo elettronico qualificato auspicando che il Legislatore italiano lo inserisca in qualche normativa anche tecnica. Qualche dettaglio in più viene analizzato nello specifico paragrafo.

3.2.4 I servizi fiduciari

Il regolamento introduce anche nuovi concetti sul piano dei termini di riferimento. Il più significativo è quello del Trust Service Provider (TSP) che in italiano è stato tradotto Prestatore di Servizi Fiduciari. I servizi fiduciari in base a eIDAS sono servizi elettronici forniti di norma a pagamento (ci si riferisce a servizi offerti dal mercato interno) che consistono nella creazione, la verifica e la convalida delle firme elettroniche, dei sigilli elettronici o validazioni temporali elettroniche, dei servizi elettronici di recapito certificato e dei certificati relativi a tali servizi. Sono servizi fiduciari anche la creazione, la verifica e la convalida dei certificati per l'autenticazione dei siti web, e infine la conservazione delle firme elettroniche, sigilli o certificati relativi a tali servizi.

I servizi fiduciari possono essere qualificati o non qualificati. Quelli qualificati devono soddisfare una serie di requisiti descritti nel regolamento. Il soddisfacimento di tali requisiti è soggetto a verifica da parte dell'ente preposto (In Italia l'Agenzia per l'Italia Digitale – AgID). Ottenuta l'approvazione di AgID o soggetto equivalente nello Stato membro dove si opera, questo ente è iscritto in un apposito elenco di fiducia e può fregiarsi di un marchio definito dalla Commissione.

Lo stato di prestatore di servizi fiduciari qualificati è valido in tutti gli Stati membri e la vigilanza condotta dallo Stato membro che ha iscritto il prestatore nell'elenco di fiducia è svolta all'interno di una "rete di cooperazione" che coinvolge anche ENISA, l'Agenzia europea per la sicurezza ICT.

Come successivamente è stato stabilito anche con il Regolamento europeo sulla protezione dei dati personali (679/2016) la violazione dei dati (data breach) assume un ruolo cruciale soggetto a specifiche attenzioni e controlli.

E' opportuno sottolineare che eIDAS introduce i servizi elettronici di recapito certificato (SERC) analoghi alla nostra Posta Elettronica Certificata (PEC). La validazione temporale elettroniche è portata a livello primario comunitario a fronte di una storia nazionale di norme di rango secondario per le marche temporali e più in generale per i riferimenti temporali opponibili ai terzi.

La conservazione di firme, sigilli e certificati non è confrontabile con la nostra conservazione digitale in quanto il suo scopo è solo quello di assicurare la cosiddetta Long Term Data Preservation (Conservazione dei dati per un lungo periodo) al fine, per esempio, di consentire la verifica di una firma elettronica qualificata o di un sigillo elettronico avanzato dopo la scadenza del certificato utilizzato per la generazione della firma stessa.

3.3 Identità, firme e sigilli nel CAD

Il Sistema Pubblico per l'Identità Digitale (SPID) è operativo da oltre due anni e, senza particolari sussulti, prosegue la sua lenta evoluzione in termini quantitativi di credenziali di accesso distribuite agli utenti e qualitativi, ossia di servizi di rete attivati dalle pubbliche amministrazioni.

Al momento della scrittura sono attivi 8 gestori dell'identità digitale, circa 4.000 amministrazioni hanno attivato i loro servizi per l'accesso anche tramite SPID (nel senso che il sistema SPID è affiancato al PIN/Password e alla Carta Nazionale dei Servizi - CNS) e sono oltre 2.800.000 le credenziali rilasciate agli utenti (ottobre 2018).

Recentemente sono state stabilite le tariffe che i gestori privati devono compensare ai gestori pubblici dell'identità digitale, a norma di legge, per la verifica dell'identità dei soggetti che intendono fruire di questi specifici servizi da soggetti privati. È inoltre stato stabilito nel Codice dell'amministrazione digitale (CAD) che esiste un compenso dovuto per la verifica delle identità ai fini dei servizi resi da pubbliche amministrazioni.

Al fine di fornire sintetica informazione sullo scenario nel quale opera SPID, di seguito, si illustrano le generalità su alcuni aspetti legali, organizzativi e tecnici di questo sistema di autenticazione informatica.

In SPID i soggetti coinvolti sono l'Agenzia per l'Italia Digitale (AgID), i Gestori delle identità digitali (IdP), i gestori degli attributi qualificati (per esempio l'appartenenza a un ordine professionale), i fornitori, pubblici o privati, di servizi e i titolari delle credenziali SPID rilasciate dagli IdP.

Le pubbliche amministrazioni, già all'inizio delle attività nel marzo 2016, hanno iniziato a fornire servizi in rete accessibili tramite SPID. Come già sottolineato, il vigente CAD (in vigore dal 27 gennaio 2018) stabilisce che "Le pubbliche amministrazioni in qualità di fornitori dei servizi, usufruiscono gratuitamente delle verifiche rese disponibili dai gestori di identità digitali e dai gestori di attributi qualificati" (art. 64, comma 3-bis).

Il Piano triennale per l'informatica nella pubblica amministrazione 2017-2019, fissava al 31 marzo 2018 la data entro la quale le pubbliche amministrazioni avrebbero dovuto garantire l'accesso ai propri servizi in rete anche tramite SPID. Un decreto specifico deve tuttavia ancora stabilire la data entro la quale i servizi in rete dovranno essere acceduti esclusivamente tramite SPID.

Un ulteriore passo è stato fatto poi alla fine del 2017, quando AgID ha stabilito con la pubblicazione della Determinazione 366/2017 l'"Approvazione degli schemi di convenzione per l'adesione al Sistema Pubblico dell'identità Digitale (SPID) per i Gestori delle identità digitali e i Fornitori privati di servizi". In questo documento si indicano le tariffe che i fornitori privati di servizi devono agli IdP.

Nonostante il tempo passato e la fortissima attenzione politica e amministrativa (con AgID e il "Team Digitale" guidato dal Commissario straordinario Diego Piacentini) SPID sta procedendo in maniera lenta disomogenea nella pubblica amministrazione (a parte i tradizionali casi di eccellenza) e con scarso successo nel privato.

Nella pubblica amministrazione i problemi sono in linea con altri scenari di "innovazione digitale" già vissuti negli ultimi 15 anni circa. Si tratta dell'approccio all'adempimento secondo il quale l'attività istituzionale è eseguita in maniera acritica e quindi il servizio rimane tale e quale al cartaceo anche se la tecnologia di contorno consentirebbe attività di semplificazione e efficienza operativa.

Naturalmente le grandi amministrazioni, sia centrali che locali, procedono in maniera spedita e in qualche modo anche i servizi resi si ampliano e di conseguenza vengono fruiti dagli utenti.

In senso più generale, spesso, i servizi resi in rete non sono la conseguenza di un adeguato processo di semplificazione del procedimento amministrativo. Talvolta gli stessi servizi non possono essere resi in rete perché su base "fortemente" cartacea.

Gli addetti ai lavori ricordano benissimo che questi scenari sono gli stessi già visti per la Carta Nazionale dei Servizi (CNS) poi associata alla Tessera Sanitaria (TS-CNS) e parzialmente per la Carta d'Identità Elettronica (CIE) che ha una diffusione significativa nell'ambito del terzo ciclo di emissione (CIE 3.0 – alla data oltre 3.900.000 documenti emessi).

Nonostante tutto si percepiscono una serie di iniziative che sono importanti per un decisivo sviluppo di SPID.

La prima è senz'altro la disponibilità di un software libero, reso disponibile per le amministrazioni che devono erogare servizi compatibili con SPID, elaborato dal "Team Digitale" in collaborazione con AgID. Il suo impatto sulla crescita del numero di amministrazioni che hanno attivato SPID non è, al momento, particolarmente significativo.

Rimanendo nell'ambito del software è in fase finale di rilascio una APP che consente di fruire della CIE 3.0 come credenziale personale per SPID utilizzando le caratteristiche contactless di questo dispositivo. Questa APP legge i dati dalla CIE tramite l'interfaccia degli smart phone compatibili (i telefoni ANDROID di ultima generazione) e utilizza l'IdP per la verifica dei dati di accesso al servizio. Il passaggio per l'IdP evita alla pubblica amministrazione lo sviluppo di una specifica interfaccia di accesso per la CIE 3.0 (anche per la TS-CNS il cui futuro è peraltro non chiaramente definito).

Oltre alle questioni software il vero salto di qualità è legato all'individuazione di parametri stabili di finanziamento degli IdP. Questo finanziamento può derivare solamente dal mondo privato, visto che la pubblica amministrazione, come già detto, usufruisce gratuitamente di SPID.

Le attuali tariffe sono piuttosto elevate per volumi di utenza significativi, ma è in corso un dibattito tra gli IdP e le istituzioni per un aggiornamento al ribasso di tali tariffe.

Dalle informazioni in possesso dello scrivente tale ribasso è "importante" e se ratificato da AgID rappresenterebbe una decisa svolta per la diffusione di SPID e la sua cruciale sostenibilità economica.

Lo sviluppo di SPID è anche legato alla effettiva utilità del suo utilizzo. Questo è palesato nella frequente frase pronunciata dai potenziali utilizzatori, "Che cosa ci posso fare?".

Ulteriori iniziative riguardano la possibilità di migrare identità basate su TS-CNS a credenziali SPID e la possibilità per il mondo finanziario di utilizzare queste ultime per i controlli anti riciclaggio, obbligatori nelle transazioni di questa natura.

Le considerazioni finali, visto lo stato dell'arte, sono ancora relative a una situazione interlocutoria. Si è in una fase di crescita stabile delle credenziali rilasciate, ma i numeri globali sono lontani dalle previsioni politiche delle origini.

Numerosi servizi in rete sono fruibili solo in modo parziale con SPID, peraltro altrettanti servizi hanno superato l'esame sia a livello centrale che locale.

Quindi, consolidato lo scenario evolutivo, il passo più importante sarà quello che porterà alla fruizione dell'intero procedimento amministrativo in modalità digitale anche per scenari complessi. In particolare, per l'interazione con l'Anagrafe Nazionale della Popolazione Residente (ANPR) e il possibile utilizzo di SPID per la sottoscrizione qualificata di documenti informatici.

3.3.1 CIE, CNS, SPID

Nell'informatica dei mainframe prima e dei mini computer distribuiti poi l'identità digitale era costituita da un nome utente (username) e da una parola chiave (password) da tenere ben custodita e a mente (al peggio scritta su un post-it incollato al video).

Poi venne Internet, i servizi in rete e la mobilità degli stessi. Le credenziali utente quindi si sono moltiplicate e se avevate un posto di lavoro dove l'accesso sicuro era indispensabile e due conti in banca era certo che in vostro possesso c'erano tre OTP (generatori di password).

In questo contesto si sono sviluppati anche i servizi in rete della PA a partire da quelli previdenziali e fiscali con una ulteriore necessità di PIN (password) specifici per ogni servizio.

A partire dal 1998 si è iniziato a parlare di credenziale unica prima la Carta d'Identità Elettronica (CIE 1.0) e poi con la Carta Nazionale dei Servizi (CNS).

La CIE 1.0 (ma anche la 2.0) è la prima testimonianza del tipico progetto di largo respiro della PA italiana. Il meccanismo è quello del "taglia il nastro" e poi dimentica. Basta un esempio sulla banda ottica installata su questa versione della CIE. Essa è una striscia di materiale "ottico" scrivibile tipo CD WORM. Nei progetti iniziali, oltre a contenere le impronte del titolare, doveva contenere dati sanitari "permanenti", come ad esempio un'ortopanoramica dentale.

Ma la disponibilità di capacità di trasmissione diventa adeguata, quindi i dati sono sui server e si consultano attestando la propria identità con la CIE.

La CIE non decolla mai completamente, costa troppo l'emissione a vista, il sistema anagrafico nazionale nonostante cospicui investimenti non riesce a essere diffuso e stabile e allora…

Vengono finanziati progetti con i fondi UMTS. Il Ministro Lucio Stanca dichiara che non si possono gestire i dati in rete senza una adeguata gestione dell'identità dei cittadini.

Nasce così la CNS che dopo varie vicende diventa Tessera Sanitaria (TS-CNS) e dopo ulteriori vicende è distribuita su base regionale.

Non c'è pace… Il progetto di unificazione CIE e CNS parte; viene redatto un decreto che viene inviato a Bruxelles per la notifica di rito delle regole tecniche. Il provvedimento sul Documento Digitale Unificato (DDU) viene approvato (il termine corretto è comunque non viene disapprovato) ma non diventa operativo.

CIE 3.0 e TS-CNS vanno per strade diverse e indipendenti.

Nel mondo della Rete e dei servizi che imprescindibilmente devono essere erogati tramite essa la visione politica introduce il Sistema Pubblico per la gestione dell'Identità Digitale per cittadini e imprese (SPID).

All'interno di un sistema gestito dall'Agenzia per l'Italia Digitale (AgID) dei soggetti accreditati svolgono il ruolo di gestori dell'identità, altri sono gestori degli attributi qualificati del titolare (per esempio l'appartenenza ad un ordine professionale).

I servizi della PA sono da erogare obbligatoriamente mediante il modello SPID. Le date sono state variate più volte, ma con il Piano Triennale 2017-2019 la scadenza per questo obbligo è stabilita per il 31 marzo 2018. In base ai dati AgID alla fine del 2018 le amministrazioni attive con servizi erogati tramite SPID sono ancora ad un numero di circa 4.000, lontano quindi da un completamento dell'obbligo.

I privati possono erogare servizi basati sul modello SPID e dopo lungo e complesso dibattito tra AgID, Team digitale e gli otto gestori dell'identità digitale attivi si è raggiunto un accordo che ha consentito ad AgID di emanare una determinazione sul tema. L'accoglienza meno che tiepida del mercato alle tariffe proposte e dovute dal fornitore di servizi privato ha portato a dei ripensamenti ed a una riduzione significativa delle tariffe. Si è in attesa di una nuova determinazione AgID sul tema.

Certamente i soggetti privati sono cruciali per il modello di business di SPID. Alla data le credenziali SPID sono rilasciate gratuitamente ai cittadini. Le pubbliche amministrazioni non devono nulla ai gestori dell'identità per il pagamento dei singoli riconoscimenti, ma i soggetti privati sì.

In questo lento e incerto avanzare di SPID è ancora poco chiaro il modello di business del sistema e la modalità mediante la quale SPID sia sostenibile economicamente.

Tanti illustri esperti hanno detto e scritto circa la storia degli oltre 30 mesi di attività per SPID. In questa sede ci si limita a osservare che due grosse impennate di richiesta credenziali si è evidenziata per gli obblighi derivanti da App18 e Carta del Docente.

Contemporaneamente si è attivata l'azione propulsiva delle Camere di Commercio che effettuano gratuitamente le operazioni di registrazione per i gestori dell'identità che aderiscono, liberamente, all'iniziativa.

Ma si va a 1000 identità al mese. Quindi bisogna capire perché.

Per la PA i servizi offerti tramite SPID sono sostanzialmente quelli offerti con PIN o CNS. Pochissimi servizi specificamente sono nati per SPID.

I professionisti utilizzano il PIN e in alcune aree geografiche la CNS e non hanno motivazione reale a passare a SPID. Dovrà essere gestita comunque la transizione di 25 milioni circa di PIN.

Il Codice dell'amministrazione digitale ha reso facoltativo l'accesso ai servizi tramite CIE e CNS. Alcune amministrazioni interpretano la norma come "non sono obbligata a garantire l'accesso tramite le smart card".

Infine risulta carente la linea di indirizzo sull'erogazione di servizi di natura sanitaria tramite SPID. Anche qui la differente velocità regionale crea scompensi territoriali. Gli obiettivi da tenere a mente per lo sviluppo di SPID nel breve periodo sono:

- è obbligatorio (per esempio in ambito servizi NoiPA e con il dispiacere associato alla costrizione per la trasformazione digitale);
- è sconosciuto (fuori dagli addetti ai lavori SPID è ignoto);
- mi serve perché rende il procedimento amministrativo o privato più efficiente per l'utente.

Esempi positivi sono i servizi di home banking, prenotazioni alberghiere e gestione dei viaggi. Non bisogna cedere alle sirene che cantano la circostanza che ottenere e utilizzare le credenziali SPID è "difficile". Il processo deve essere sicuro e allo specifico stato dell'arte. Un livello inferiore crea insicurezza, sfiducia e distacco ovvero il progetto declina e fallisce.

3.3.2 Applicazione dell'art.20, comma 1-bis del CAD

La versione vigente del Codice dell'amministrazione digitale (CAD) in vigore dal 27 gennaio 2018 ha introdotto una nuova fattispecie di formazione del documento informatico nell'articolo 20, comma 1-bis.
In particolare nell'appena citato comma si stabilisce che:

"*Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore(…omissis…)*".

Per completare il quadro sulle novità introdotte sul tema nell'ultimo CAD, dobbiamo citare anche quanto stabilito nel secondo periodo dell'articolo 21, comma 2-bis:

"*Gli atti di cui all'articolo 1350, numero 13), del Codice (civile) redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale ovvero sono formati con le ulteriori modalità di cui all'articolo 20, comma 1-bis, primo periodo*".

Queste norme si commentano allo scopo di fornire evidenza sulla portata di queste novità, evidenziando le criticità associandole a proposte operative tese a meccanismi organizzativi e tecnologici più semplici e coordinati tra di loro.
Il tutto anche con l'indispensabile coordinamento con l'articolo 65 del CAD che tratta di Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica.

Lo schema applicativo che ci propone la norma primaria è il seguente:

1) L'autore del documento è stato identificato in modalità informatica. Questo è avvenuto tramite un processo avente i requisiti fissati da AgID mediante il nuovo meccanismo delle Linee guida che contengono le regole tecniche. La modalità informatica utilizzata per l'identificazione potrebbe essere un PIN, una Carta d'Identità Elettronica (CIE 3.0 è versione che attualmente è in fase di emissione), la Carta Nazionale dei servizi. Il dubbio è comunque risolto nell'articolo 64, comma 2-quater: "*L'accesso ai servizi in rete erogati dalle pubbliche amministrazioni che richiedono identificazione informatica avviene tramite SPID*". Ma il comma 2-nonies stabilisce che l'accesso può avvenire anche tramite CIE o CNS.

2) Preso atto di questo principio sappiamo che AgID dovrà associare a SPID delle modalità di formazione del documento tali da garantire sicurezza, integrità e immodificabilità dello stesso. Per fare delle ipotesi sulla direzione verso la quale si muoverà AgID dobbiamo andare a leggere gli allegati sul glossario e sui formati al DPCM 13 novembre 2014.

3) Nel glossario non c'è la definizione di sicurezza del documento informatico, ma il concetto è espresso nell'allegato dedicato ai formati documentali: *"La sicurezza di un formato dipende da due elementi il grado di modificabilità del contenuto del file e la capacità di essere immune dall'inserimento di codice maligno"*. Il primo concetto rimanda all'immodificabilità quindi per la sicurezza in sé abbiamo solo il secondo.

4) Per quanto attiene all'integrità troviamo la definizione nel glossario:
"Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato".

5) L'allegato con il glossario contiene anche la definizione di immodificabilità:
"Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso".

Questa analisi di dettaglio ci aiuta a definire cosa sarebbe auspicabile stabilire con le specifiche Linee guida di AgID.

Dunque, l'autore è stato identificato tramite SPID e accede con la sua identità in un sistema informatico dove produce la forma e il contenuto del documento informatico.

Applicando le Linee guida AgID adesso deve assicurare la completa formazione garantendo i tre requisiti appena esposti.

Le opzioni sono già stabilite nel DPCM 13 novembre 2104 nell'articolo 3, comma 4.

La presenza di ben 5 opzioni per garantire integrità e immodificabilità non aiuta a definire al meglio il percorso tecnico e organizzativo indispensabile per ottenere applicazioni efficaci ed efficienti.

Inoltre la presenza tra le opzioni della firma digitale (qualificata) ma non della firma elettronica avanzata (applicabile in base al CAD stesso) crea delle disomogeneità tra norme tecniche e rende difficoltoso il coordinamento tra le stesse.

In altre parole possiamo dire che l'unica certezza rimane l'utilizzo di SPID.

Un'altra difficoltà nel coordinamento deriva da quanto stabilito nell'articolo 65, comma 1 del CAD e in particolare nelle lettere a) e b).

Nella lettera a) si fa riferimento alle sottoscrizioni, ma questa nuova fattispecie non è una sottoscrizione visto che è un metodo per formare il documento. Poi nella lettera b) si stabilisce che sono valide le istanze e dichiarazioni presentate alla pubblica amministrazione quando l'istante o il dichiarante è identificato attraverso SPID. Ma sono accettate anche la CIE e la CNS.

E' evidente che il sovrapporsi delle norme non ha portato beneficio alla loro omogeneità e coordinamento. AgID nelle funzioni che gli assegna lo Statuto e l'articolo 71 del CAD dovrà provvedere a disegnare percorsi lineari ed efficaci, razionalizzando l'uso dell'identità digitale, creando un solo percorso valido per l'interazione con la PA.

Inoltre è indispensabile definire i nuovi ruoli della sottoscrizione informatica in coordinamento con l'identità digitale rappresentata da SPID ma anche dalla CIE. Il futuro della CNS è ancora poco chiaro. La circostanza che la notifica a Bruxelles degli schemi di identificazione è stata fatta (con successo) per SPID e entro l'anno sarà attuata anche per la CIE (annuncio di AgID) induce a ipotizzare che la CNS (con la Tessera Sanitaria) può subire una battuta d'arresto.

3.4 Il sigillo elettronico qualificato

In precedenza abbiamo già detto della forte analogia generale tra firma e sigillo elettronico. Questa conseguente apparente similitudine, permane dal punto di vista tecnologico (maggiori dettagli nel paragrafo seguente) ma il profilo funzionale li rende non equivalenti. L'analisi di queste considerazioni può essere facilitata utilizzando ancora una volta la dottrina della prima metà del secolo scorso (F. Carnelutti, Studi sulla sottoscrizione, 1929)

che come già visto in questo documento, individuava le tre principali funzioni della sottoscrizione autografa. Quindi riprendendo e specializzando al sigillo quanto già illustrato nel capitolo introduttivo, riprendiamo le funzioni indicativa, probatoria e dichiarativa.
Relativamente al sigillo elettronico possiamo senz'altro affermare che quest'ultimo svolge la funzione indicativa perché individua e distingue chi genera il sigillo dagli altri soggetti giuridici. Prima conclusione che si può trarre è che il sigillo elettronico rappresenta una tecnica di identificazione della persona giuridica.
Il sigillo è altresì adeguato a svolgere funzioni probatorie, perché per quanto stabilito nell'articolo 35 del regolamento, forma prova della provenienza dei dati, del documento informatico o del bene digitale della persona giuridica alla quale il sigillo si riferisce.
La funzione dichiarativa non è esplicitamente richiamata dal regolamento. Ricordiamo che con essa si assume la paternità del documento e, di fatto, si esprime il consenso relativo al documento.
In [4], pag. 258 si specifica che "la funzione dichiarativa è strettamente connessa alla sussistenza della capacità d'agire in capo alla persona giuridica". E si precisa ulteriormente che "*questa è regolata dalle norme di diritto nazionale di ogni Stato membro, mentre il Regolamento, al fine di evitare conflitti normativi, non detta norme in materia di capacità e rappresentanza*".
La seconda conclusione che possiamo trarre è quindi che il sigillo non svolge "di base" la funzione dichiarativa. Peraltro il regolamento stabilisce esplicitamente che è accettabile anche la firma elettronica qualificata del rappresentante autorizzato della persona giuridica (considerando 58 di eIDAS).
In questo senso la Commissione UE ha chiarito nelle FAQ su eiDAS che il sigillo elettronico:

*"can only be issued to and used by legal persons to ensure origin and integrity of data / documents. An electronic seal is therefore **NOT** an electronic signature of the legal person.*

When a legal entity makes use of electronic seals, it is recommended to set up an internal control mechanism ensuring that only the natural persons entitled to act on behalf of the legal entity can make use of the electronic seals (push the button on behalf of the legal entity).

Electronic seals can be also used by information systems, hence being a powerful tool for supporting secured automated transactions; in this case, again, internal control mechanisms to assure that only authorized uses are allowed should be put in place".

Per concludere questo paragrafo ricordiamo l'importanza del sigillo elettronico qualificato per l'asseverazione dell'integrità di documenti informatici ma anche di beni tutelati dal diritto d'autore come foto digitali ma anche software.
E' anche utile ricordare che non è nota a priori la persona fisica che appone il sigillo o addirittura non esiste la persona fisica perché il sigillo è apposto da sistema informatico.
Il Regolamento determina che la riconducibilità sia fattibile con il considerando 60 dove, in riferimento al sigillo elettronico qualificato, si dice che i prestatori di servizi fiduciari che rilasciano certificati qualificati di sigillo elettronico devono attuare le misure necessarie a identificare la persona fisica che c'è "dietro" la persona giuridica.

Altre indicazioni normative sui sigilli sono disponibili nell'ambito del capitolo sugli utilizzi di quelli qualificati.

3.4.1 Fondamenti tecnologici

La similitudine tra firma e sigillo è evidente quando si descrivono le tecnologie da utilizzare, in conformità agli standard stabiliti dalla Commissione europea. Lo stesso regolamento, stabilendo nell'allegato III il profilo per i certificati per il sigillo elettronico qualificato, evidenzia le analogie con quanto stabilito in allegato II per i certificati per la firma elettronica qualificata.

3.4.2 Gli standard europei sul sigillo elettronico

Gli standard europeo sul sigillo elettronico avanzato e sul certificato digitale per il sigillo elettronico sono pressoché identici a quelli per le firme elettroniche. Il regolamento per sua natura giuridica e principi comunitari è tecnologicamente neutro e sviluppo i suoi effetti tramite atti comunitari secondari denominati Atti di esecuzione o Atti delegati.
Come è noto la prassi consolidata in ambito comunitario è che la normativa è tecnologicamente neutra al fine di evitare squilibri e disomogeneità nel mercato interno. Peraltro già con la direttiva 1999/93/CE si è scelta la via di atti secondari della Commissione che stabiliscono gli obblighi tecnologici facendo riferimento agli standard di classe EN (norme Europee). Questi standard sono sviluppati secondo le regole di settore alle organizzazioni ETSI (nel sottogruppo ESI) e CEN.
Anche per la firma e il sigillo è stata percorsa questa strada che ha portato alla Decisione di esecuzione 2015/1506.
Questa norma secondaria della Commissione europea è dell'8 settembre 2015 e "*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'articolo 27, paragrafo 5, e all'articolo 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 nel mercato interno*".
Nei considerando di questa decisione di esecuzione ne troviamo uno che delinea l'analogia tra firme elettroniche avanzate e sigilli elettronici avanzati, e il numero (6).

"*Le firme elettroniche avanzate e i sigilli elettronici avanzati sono simili dal punto di vista tecnico. Pertanto le norme per i formati delle firme elettroniche avanzate dovrebbero applicarsi mutatis mutandis ai formati per i sigilli elettronici avanzati".*
Gli scopi di questa decisione sono stabiliti nell'articolo 1:
"*Gli Stati membri che richiedono una firma elettronica avanzata o una firma elettronica avanzata basata su un certificato qualificato, secondo quanto disposto dall'articolo 27, paragrafi 1 e 2, del regolamento (UE) n. 910/2014, riconoscono la firma elettronica avanzata XML, CMS o PDF al livello di conformità B, T o LT o tramite contenitore di firma associata, purché tali firme siano conformi alle specifiche tecniche riportate nell'allegato".*

In maniera coordinata con questo articolo questa Decisione stabilisce regole per il sigillo nell'articolo 3. Si noti come questo articolo sia di fatto identico all'articolo 1, fatta eccezione per le parole firma e sigillo.

"*Gli Stati membri che richiedono un sigillo elettronico avanzato o un sigillo elettronico avanzato basato su un certificato qualificato, secondo quanto disposto dall'articolo 37, paragrafi 1 e 2, del regolamento (UE) n. 910/2014, riconoscono la firma elettronica avanzata XML, CMS o PDF al livello di conformità B, T o LT o tramite contenitore con sigillo associato, purché tali sigilli siano conformi alle specifiche tecniche riportate nell'allegato".*
L'allegato a questa Decisione contiene l'elenco delle specifiche tecniche per le firme elettroniche avanzate XML, CMS o PDF e per il contenitore con firma associata e le regole analoghe per i sigilli.
Sia per le firme che per i sigilli esse sono:

Profilo di base XAdES	ETSI TS 103 171 v. 2.1.1.
Profilo di base CAdES	ETSI TS 103 173 v. 2.2.1.
Profilo di base PAdES	ETSI TS 103 172 v. 2.2.2.

Il contenitore con sigillo associato (identica cosa per la firma) soddisfa la specifica ETSI:

Profilo di base del contenitore con sigillo associato	ETSI TS 103 174 v.2.2.1.

L'allegato riporta anche i collegamenti internet dove è possibile reperire i documenti degli standard referenziati.
Il lettore più attento noterà correttamente senz'altro che gli standard indicati nella Decisione non sono di classe EN. In effetti per motivi temporali legati alle procedure ETSI per la pubblicazione di norme con classe EN la Commissione non potuto referenziarli perché non ancora ufficialmente pubblicati.
Qui la Commissione descrive lo stato dell'arte sugli standard per firme e sigilli ovviamente puntualizzando che la Decisione 2015/1506 referenzia la versione precedente degli standard.
Lo state dell'arte tecnico e legale quindi indica che gli standard presenti nella Decisione sono obbligatori, quelli più recenti sono consigliati.
In allegato 1.3 a titolo di esempio viene mostrata la struttura di un certificato di sigillo elettronico.

3.5 Scenari di utilizzo per il sigillo elettronico qualificato

E' utile ribadire ancora una volta che il sigillo elettronico qualificato beneficia di un pieno riconoscimento legale grazie al Regolamento 910/2014 (eIDAS). In questo scenario di regole europee i sigilli elettronici garantiscono l'integrità dei dati, individuano il creatore del sigillo con un elevato livello di certezza e assicurano la validità dell'origine del sigillo (rendendo arduo per il creatore del sigillo il ripudio dell'apposizione del medesimo ai dati).

Vista la totale novità di questa evidenza informatica nell'ordinamento comunitario e nazionale è importante ribadire che il sigillo elettronico (qualificato) è generato da una persona giuridica ovvero, applicando il Regolamento eIDAS, non ha valore legale la generazione di un sigillo elettronico da parte di una persona fisica. Peraltro quest'ultima può generare firme elettroniche.
Risulta sempre valido il concetto che il sigillo elettronico e la firma elettronica sono simili salvo l'applicazione della separazione legale per la persona giuridica e quella fisica.
Le caratteristiche di sicurezza di queste fattispecie sono derivabili dalle tecnologie utilizzate che, come già detto, sono simili.
In particolare l'utilizzo di crittografia a chiave pubblica rende realizzabile l'integrità dei dati ai quali è stato applicato il sigillo ma anche l'origine degli stessi. Il creatore del sigillo è la persona giuridica alla quale è stata univocamente assegnata la chiave privata utilizzata per la generazione del sigillo stesso.
Sempre questi meccanismi crittografici consentono di associare il non ripudio del sigillo apposto ai dati. Sempre in analogia con la sottoscrizione elettronica, il certificato digitale utilizzato per il sigillo consente (al massimo livello di certezza quando il certificato è qualificato) l'identificazione del creatore del sigillo.
Naturalmente l'identità di chi appone il sigillo è nota tramite le regole che si applicano ai prestatori di servizi fiduciari per l'associazione di una persona fisica alla fattispecie giuridica.
Il Regolamento eIDAS ci consente anche di svincolare la generazione del sigillo elettronico dall'operatore umano. Infatti l'apposizione del sigillo può essere effettuata mediante un procedimento automatico. Questa opzione consente, per analogia, di applicare il sigillo in una serie di scenari dove, ad oggi, viene utilizzata la sottoscrizione con procedura automatica (ex articolo 35, comma 3 del nostro CAD). La sottoscrizione con procedura automatica è utilizzata per stabilire l'origine e l'integrità di flussi di dati di elevata numerosità (referti clinici, fatture, particolare contrattualistica, ecc.).
La disponibilità del sigillo è utile perché nella maggioranza dei casi l'operazione deve essere ricondotta ad una persona giuridica e la firma è oggi utilizzata perché ancora non è pienamente operativo il sigillo ovvero per la necessità di aggiornamenti normativi.
Sempre al fine di chiarire i corretti scenari legali e organizzativi del sigillo elettronico è utile ricordare che il sigillo non è di una persona fisica, i dati sigillati non hanno necessariamente una validità giuridica o un senso logico a priori. I dati sigillati non possono garantire la loro riservatezza, quindi devono essere associati ai dati dei meccanismi di cifratura adeguati, meglio prima di apporre il sigillo.
Il sigillo elettronico non sostituisce una marca temporale e non garantisce l'integrità permanente dei dati. Quindi per i sigilli (come per le firme e i rispettivi certificati) è indispensabile realizzare la *Long Term Data Preservation*.
Il dettaglio degli utilizzi pratici del sigillo elettronico (qualificato) è disponibile nei paragrafi dedicati di questo capitolo. Volendo fornire una bussola per aiutare l'orientamento tra le possibili applicazioni possiamo dire quanto segue.
In alcuni casi il sigillo potrebbe essere applicato, ma la normativa vigente non lo consente, quindi dovrebbe essere modificata.

In altri casi il passaggio dalla sottoscrizione elettronica all'apposizione del sigillo non costituisce una semplificazione del procedimento amministrativo, ma solo un'azione di coordinamento e coerenza con le fattispecie giuridiche.
Prima di esaminare alcuni possibili casi d'uso del sigillo elettronico è utile richiamare in modo completo l'articolo 35 del Regolamento eIDAS.

1. A un sigillo elettronico non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per i sigilli elettronici qualificati.

2. Un sigillo elettronico qualificato gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico qualificato è associato.

3. Un sigillo elettronico qualificato basato su un certificato qualificato rilasciato in uno Stato membro è riconosciuto quale sigillo elettronico qualificato in tutti gli altri Stati membri.

I paragrafi 2 e 3 di questo articolo ci forniscono chiari messaggi sulle circostanze a fronte delle quali è indispensabile utilizzare un sigillo qualificato.
In ogni caso sarebbe opportuno utilizzare almeno un sigillo elettronico avanzato, visto che per questa fattispecie sono disponibili delle specifiche tecniche comunitarie (ETSI) anche ai fini dell'interoperabilità trans frontaliera e trans settoriale.

Il sigillo elettronico è la forma digitale del "timbro" su carta, l'apposizione di un sigillo elettronico dovrebbe rendere immediatamente evidente l'origine di un documento elettronico riportando i dati identificativi della persona giuridica, un po' come la carta intestata di una società; ovviamente il suo utilizzo sarà per quei documenti sui quali non è obbligatoria una sottoscrizione autografa nemmeno nel mondo cartaceo: si pensi in ambito commerciale ai documenti informativi o - relativamente alla documentazione giuridicamente rilevante – alla documentazione sulle condizioni generali di contratto che riportano nell'intestazione i dati dell'operatore commerciale e rispetto ai quali si vogliano dare le adeguate garanzie circa la loro provenienza, anche con l'utilizzo di tecniche automatiche di verifica.
L'apposizione di sigilli "sequenziali" può consentire di tracciare le successive modifiche nell'ambito di un ciclo di vita documentale.
In ambito notarile si possono individuare ambiti di utilizzo innovativi.

In altri settori l'utilizzo del sigillo elettronico potrebbe rendere immediatamente individuabili le evidenze informatiche dirette a garantire esclusivamente l'origine e l'integrità dei dati, che debbono avere un uso controllato all'interno della persona giuridica a cui si riferiscono ma non necessariamente personale, ciò rispetto agli strumenti di firma che invece presuppongono un utilizzo personale e diretto e che hanno lo scopo dell'appropriazione giuridica da parte del firmatario e non quello di "congelare" il contenuto del documento.

E' evidente, a questo punto, che possiamo indicare come principali scenari per l'utilizzo del sigillo elettronico (qualificato) la fatturazione elettronica (dove il sigillo è già applicato alle ricevute di accettazione), i procedimenti che coinvolgono flussi elevati di dati, tipicamente in ambito clinico o amministrativo nei casi dove è soddisfatto il requisito della definizione a priori del flusso e dell'omogeneità dei dati. In altre parole in tutti quei casi dove l'esame del contenuto del documento informatico non è cruciale perché non derivato da procedimenti di formazione automatici (Es.: Referti clinici di esami di laboratorio, referti di radiologia).
Il sigillo può essere utilizzato al posto della firma digitale nei procedimenti di formazione del contrassegno elettronico utilizzato nelle procedure di produzione di copie conformi.
Poiché spesso, in modo discorsivo il contrassegno elettronico di cui all'articolo 23-ter, comma 5 del CAD viene associato anche il termine (errato) di sigillo elettronico. I termini "glifo", "timbro digitale" o "contrassegno elettronico" sono invece corretti.
Il CAD al appena appena citato, stabilisce che sulle copie analogiche di documenti amministrativi informatici "*può essere apposto a stampa un contrassegno, sulla base di criteri definiti con linee guida dell'Agenzia per l'Italia Digitale, tramite il quale è possibile ottenere il documento informatico ovvero verificare la corrispondenza dello stesso alla copia analogica*".
Lo strumento è utilizzato per la produzione di copie conformi agli originali e può essere utilizzato per i documenti amministrativi quando l'originale è in formato elettronico.
Il contrassegno, quindi, è una fattispecie differente dal sigillo elettronico che, come sappiamo, serve ad attribuire certezza circa l'origine e l'integrità di un documento originale. In particolare, sul piano giuridico sono chiare le differenze. Il sigillo elettronico individua la persona giuridica che ha prodotto il documento, mentre il contrassegno svolge la funzione di garantire la conformità delle copie analogiche di documenti informatici originali.
Certamente esistono analogie tecnologiche e il glifo può essere senza problemi veicolo di informazioni di integrità del documento informatico al quale è stato apposto il sigillo elettronico che è in modo pressoché certo il documento originale.
Il sigillo elettronico qualificato può sostituire la firma in alcune passaggi della conservazione digitale (Es. la sottoscrizione del Pacchetto di Versamento da parte del responsabile della conservazione). In questo scenario sono indispensabili delle modifiche normative poiché in queste si fa esplicito riferimento alla firma digitale ovvero alla firma elettronica qualificata.
Nel periodo di redazione di questo documento viene ipotizzato l'utilizzo del sigillo anche nelle architetture di blockchain e registri distribuiti. L'ipotesi è seducente ma al momento il mondo della "catena di blocchi" e quello dell'eIDAS, pur presentando similitudini tecnologiche, sono chiaramente differenti sul piano legale e organizzativo.

3.5.1 Conservazione digitale

La conservazione digitale utilizza in vari scenari la sottoscrizione. Questo perché la normativa di riferimento sia secondaria che operativa stabilisce l'utilizzo della firma elettronica qualificata. Il caso più diffuso è quello del pacchetto di archiviazione che deve essere sottoscritto dal responsabile della conservazione. Naturalmente è anche prevista l'eventuale sottoscrizione del rapporto di versamento e del pacchetto di distribuzione.

Nella natura giuridica delle cose e in un'ottica di depersonalizzazione del responsabile della conservazione è senz'altro ragionevole ritenere che questa sottoscrizione possa, senza problemi, diventare l'apposizione di un sigillo elettronico.
In molti scenari questa operazione favorisce anche una "serenità psicologica" nella persona responsabile dell'apposizione del sigillo che (in verità senza alcuna specifica base giuridica) opera con maggiore buona volontà rispetto alle operazioni di sottoscrizione.
La separazione, almeno psicologica, tra persona fisica che appone una sottoscrizione digitale e la persona giuridica che appone il sigillo qualificato può determinare molte situazioni che suggeriscono l'uso del sigillo.
Naturalmente se parliamo di conservazione digitale, bisogna attenersi alla normativa vigente che stabilisce l'uso della firma digitale o della firma elettronica qualificata. Solo la modifica normativa può consentire l'utilizzo del sigillo elettronico.

Infatti la vigente normativa relativa al processo di conservazione (art. 9 DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione) prevede esplicitamente "la sottoscrizione con firma digitale o firma elettronica qualificata" in ogni caso previsto: (rapporto di versamento ("eventuale" punto e) pacchetto di archiviazione (punto f) e pacchetto di distribuzione ("ove prevista" punto g).
Nei primi due casi la firma deve essere del responsabile della conservazione, mentre nell'ultimo caso non è specificato.
Nella realtà il responsabile della conservazione delega tale firma ad altri soggetti.

Appare evidente che nel processo di conservazione il sigillo potrebbe validamente sostituire, in ogni caso previsto, le firme e consentire una maggiore efficienza del processo di conservazione, in quanto la finalità è soprattutto di attestare la provenienza da un sistema di conservazione e l'integrità dei pacchetti o dei rapporti, piuttosto che una dichiarazione di conoscenza o di espressione di una volontà.
Il sigillo dovrebbe essere quello della persona giuridica che detiene il sistema di conservazione e svolge le attività di conservatore.
Il Manuale di conservazione dovrebbe riportare le regole con cui i sigilli vengono apposti (*internal control mechanism),* prevedendo anche azioni automatiche di sistema.

3.5.2 Fatturazione elettronica

Nella fatturazione elettronica il sigillo ha trovato la sua prima applicazione "legale" nella pubblica amministrazione. Infatti le ricevute rilasciate dall'Agenzia delle entrate a fronte dell'invio di fatture elettroniche.
Come direttamente indicato dall'Agenzia delle entrate, l'uso del sigillo apposto dal servizio dell'Agenzia è un'alternativa per chi non è dotato di firma digitale. Serve a garantire l'immodificabilità delle fatture elettroniche destinate a privati:

- se trasmesse tramite Sistema di Interscambio (dal 1 gennaio 2017)
- inviate al servizio di conservazione messo a disposizione dall'Agenzia delle Entrate.

L'Agenzia delle entrate indica che il sigillo è uno strumento che, tra l'altro, permette di rilevare se un documento informatico ha subito modifiche e che è definito dagli artt. 3 e 36 del Regolamento 2014/910/UE "eIDAS" (electronic IDentification Authentication and Signature).
La stessa Agenzia ricorda che, a differenza della firma elettronica, può essere apposto da una persona giuridica.

Di seguito il dump ASN.1 del certificato di sigillo elettronico dell'Agenzia delle entrate.

```
  0 1114: SEQUENCE {
  4  834:   SEQUENCE {
  8    3:     [0] {
 10    1:       INTEGER 2
       :     }
 13    8:     INTEGER 56 57 AC F4 57 DC B2 47
 23   13:     SEQUENCE {
 25    9:       OBJECT IDENTIFIER
       :         sha256WithRSAEncryption (1 2 840 113549 1 1 11)
 36    0:       NULL
       :     }
 38  109:     SEQUENCE {
 40   11:       SET {
 42    9:         SEQUENCE {
 44    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 49    2:           PrintableString 'IT'
       :         }
       :       }
 53   30:       SET {
 55   28:         SEQUENCE {
 57    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 62   21:           PrintableString 'Agenzia delle Entrate'
       :         }
       :       }
 85   27:       SET {
 87   25:         SEQUENCE {
 89    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 94   18:           PrintableString 'Servizi Telematici'
       :         }
       :       }
114   33:       SET {
116   31:         SEQUENCE {
118    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
123   24:           PrintableString 'CA Agenzia delle Entrate'
       :         }
```

```
    :       }
    :     }
149  30:   SEQUENCE {
151  13:     UTCTime 16/11/2016 16:17:05 GMT
166  13:     UTCTime 17/11/2019 16:17:05 GMT
    :     }
181 105:   SEQUENCE {
183  11:     SET {
185   9:       SEQUENCE {
187   3:         OBJECT IDENTIFIER countryName (2 5 4 6)
192   2:         PrintableString 'IT'
    :       }
    :       }
196  30:     SET {
198  28:       SEQUENCE {
200   3:         OBJECT IDENTIFIER organizationName (2 5 4 10)
205  21:         UTF8String 'Agenzia delle Entrate'
    :       }
    :       }
228  26:     SET {
230  24:       SEQUENCE {
232   3:         OBJECT IDENTIFIER '2 5 4 97'
237  17:         UTF8String 'VATIT-06363391001'
    :       }
    :       }
256  30:     SET {
258  28:       SEQUENCE {
260   3:         OBJECT IDENTIFIER commonName (2 5 4 3)
265  21:         UTF8String 'Agenzia delle Entrate'
    :       }
    :       }
    :     }
288 290:   SEQUENCE {
292  13:     SEQUENCE {
294   9:       OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
305   0:       NULL
    :       }
307 271:     BIT STRING, encapsulates {
312 266:       SEQUENCE {
316 257:         INTEGER
    :           00 AB 7C C6 3F 1F 67 88 DB 18 E4 D8 82 DB DA EF
    :           5B 08 81 20 F4 D7 B2 9F 47 8C D6 63 44 1C 9C A2
    :           6D 13 C4 7F 4B 91 81 8E A5 5B 3F A9 92 24 0B 6E
    :           F6 6F C1 D5 93 EE 79 F9 D2 55 A0 69 AB 8A BB CE
```

```
    :          22 B2 09 41 B8 46 B8 80 A4 98 12 0B 07 77 EE 16
    :          61 41 BE F1 48 5D 38 0D A8 7F 07 AA 58 70 3E 5D
    :          DD C5 3B AB 81 BF B5 83 83 F9 E0 86 88 6F 5B AD
    :          62 3A E9 33 3D D9 6E F3 E0 C4 42 C3 29 87 D3 A9
    :          8D 08 3C ED C9 CC 3B 12 16 A8 35 FA 90 8F 19 5C
    :          57 98 CB 9F 18 F9 E9 5D 28 9A 59 5C B8 93 96 78
    :          7C DF 9B BD E2 29 DF 39 51 E6 21 A3 D5 6E 4F CC
    :          2A EC 82 C5 4C 2B 39 72 0A 71 FF ED 20 C0 04 69
    :          48 7A 9C A0 7D D7 E3 82 ED F4 C3 AA 06 09 2B BC
    :          73 B8 FC F5 5E FF 67 50 19 9C E6 C3 0B ED FC AC
    :          DB D3 A9 47 05 C1 B5 9A 8C 0A 32 E9 7C E2 1A FA
    :          7D 27 3B 3F 7F D8 92 C6 77 6C CC AA 4B 49 B3 8C
    :          4B
577   3:         INTEGER 65537
    :        }
    :       }
    :     }
582 256:    [3] {
586 253:     SEQUENCE {
589  31:      SEQUENCE {
591   3:       OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
596  24:       OCTET STRING, encapsulates {
598  22:        SEQUENCE {
600  20:         [0]
    :           EA 44 3F 1F 19 E3 37 3E AB AA 94 82 A5 9F EB FC
    :           16 BA 7F B5
    :          }
    :         }
    :        }
622 170:      SEQUENCE {
625   3:       OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
630 162:       OCTET STRING, encapsulates {
633 159:        SEQUENCE {
636 156:         SEQUENCE {
639 153:          [0] {
642 150:           [0] {
645 147:            [6]
    :             'ldap://cads.entrate.finanze.it/CN=CA%20Agenzia%2'
    :             '0delle%20Entrate,OU=Servizi%20Telematici,O=Agenz'
    :             'ia%20delle%20Entrate,C=it?certificateRevocationL'
    :             'ist'
    :            }
    :           }
    :          }
```

```
    :           }
    :         }
    :       }
795  29:      SEQUENCE {
797   3:       OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
802  22:       OCTET STRING, encapsulates {
804  20:         OCTET STRING
    :           A5 D3 05 3A 49 7E 2A 20 61 CF 21 95 F3 96 E1 FA
    :           6B 11 22 45
    :         }
    :       }
826  14:      SEQUENCE {
828   3:       OBJECT IDENTIFIER keyUsage (2 5 29 15)
833   1:       BOOLEAN TRUE
836   4:       OCTET STRING, encapsulates {
838   2:         BIT STRING 6 unused bits
    :           '10'B (bit 1)
    :         }
    :       }
    :     }
    :   }
842  13:  SEQUENCE {
844   9:    OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
855   0:    NULL
    :   }
857 257:  BIT STRING
    :    A4 34 80 27 4E 12 62 F3 F2 49 21 BF 7D CF AF 3C
    :    F6 E7 ED E8 D8 E4 EB 20 FE 09 7B 2C E5 76 FF 51
    :    E5 6A CA A5 08 D7 1C 8E 15 AA 73 E4 D1 19 FD 1C
    :    7B 27 17 37 E8 05 F2 8E 85 12 07 F7 37 09 B8 2B
    :    9D 2D 30 5E 70 D4 5C 4D AD 2C 22 5F 8A 6F F8 56
    :    59 F0 68 33 76 96 33 F8 1E 60 57 84 41 1E 07 C1
    :    04 1F 47 BC 8F 8D D7 63 44 0C 88 2B 6F 3E EC 6A
    :    BA BD 50 33 7B A9 FD 09 0B 30 0C 14 09 9E 22 BF
    :    1A D2 06 D9 88 A4 54 91 70 5E D7 6D 25 92 D5 98
    :    AF C9 13 FC C9 26 CF 50 08 DE 7A 18 88 59 59 64
    :    D7 69 DE 1D 96 40 6C 46 DC 35 E7 B7 61 E7 56 77
    :    18 6E 21 43 4F 09 FA 34 AD A1 4F DB AB C2 57 B1
    :    D8 BD 7F 33 3A E4 EE 6B D2 AD 75 B8 AC 84 CA F9
    :    57 3A 95 37 88 60 9A 02 2F 05 5C 09 FF 02 08 C8
    :    1E 8F 69 83 1F 11 E7 4E 80 D6 F6 13 12 20 8B BE
    :    8A F4 67 50 25 08 80 F7 7B 0C 0F 9E B0 71 53 DD
    :  }
```

3.5.3 Protocollo e repertori informatici

Nella normativa di riferimento e nelle regole tecniche del protocollo informatico non è previsto, né indicato o consigliato, l'uso di una sottoscrizione elettronica per le operazioni di registrazione.
Certo è che in questo contesto lo scopo principale del sigillo (garantire la certezza dell'origine e l'integrità dei dati) e, come già riportato, la possibilità di svincolarne la generazione dall'operatore umano, mediante un procedimento automatico, appaiono estremante calzanti in un conteso dove la trasmissione e la ricezione di un'alta numerosità di documenti informatici è un elemento fondamentale.
Per poter individuare le applicazioni possibili ed appropriate è utile chiarire alcuni aspetti.

La registrazione informatica di protocollo è un'attività che avviene su documenti formati; certifica esclusivamente l'uscita o l'ingresso degli stessi mediante l'associazione di un numero sequenziale ed una data opponibili a terzi. (Ricordiamo che il registro di protocollo è un atto pubblico di fede previlegiata[44] e che la registrazione di protocollo è una validazione temporale[45]).
Nel DPR 445/2000 l'articolo 55 "Segnatura di protocollo" al comma 1 recita: "La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile".
Ovviamente non è nello scopo di questo documento dare indicazioni sulle modalità con cui gestire un servizio primario come quello del protocollo informatico o della gestione dei documenti informatici in generale, ma è inutile nascondere che l'apposizione della segnatura di protocollo all'originale del documento è la prassi consolidata in ambito analogico ed è quella che per consuetudine si cerca di perseguire, non con poche difficoltà, anche sulla documentazione digitale. La motivazione per la quale purtroppo si insiste con l'apposizione della segnatura di protocollo è che il documento non è inserito in un processo reingegnerizzato in ottica di dematerializzazione ed alla fine viene, spesso inutilmente, stampato.
Si deve sottolineare che con una completa digitalizzazione della documentazione e dei processi, una corretta e piena applicazione delle indicazioni sull'interoperabilità tra sistemi[46] e nel rispetto delle regole tecniche per cui i documenti vanno "identificati e trattati nel sistema di gestione informatica dei documenti"[47], la problematica di

[44] Consiglio di Stato, Sez. IV - 5 ottobre 2010, n. 7309
[45] DPCM 22 febbraio 2013 Art. 41. Riferimenti temporali opponibili ai terzi - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche
[46] La circolare Agid 23 gennaio 2013 n.60 "segnatura protocollo informatico", che descrive le modalità di produzione del file segnatura.xml, soddisfa il requisito normativo del già citato comma 1 del DPR 445/2000 l'articolo 55 circa "[…] l'associazione all'originale del documento, in forma permanente non modificabile […]"
[47] rif DPCM 13 novembre 2014 Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici Art. 9 comma 3

"apposizione" della segnatura di protocollo verrebbe meno, a fronte dell'evidente efficienza dell'"associazione".
In ogni caso questa prassi non è corretta perché l'applicazione di procedure pensate per la carta al digitale è scorretta.
Concentrandoci sulle possibile analogie tra segnatura di protocollo e sigillo elettronico è sicuramente possibile configurare i sistemi in modo che appongano con procedura automatica un sigillo informatico oltre alla segnatura a tutta la documentazione protocollata, ampliando le garanzie di origine ed integrità dei documenti (a titolo di esempio pensiamo ad un cittadino che riceve sulla sua posta elettronica ordinaria la scansione di un documento magari con l'indicazione di firma sostituita a mezzo stampa…).
Peraltro le operazioni di protocollo devono essere considerate separate da quelle di gestione documentale e in questo senso l'apposizione del sigillo come elemento qualificante per la provenienza e l'integrità del documento sigillato deve trovare il corretto equilibrio tra i vari scenari.
Infatti i documenti informatici arrivano al protocollo tramite il sistema della PEC (che in qualche modo possiamo anche associare al principio giuridico del "domicilio digitale") quindi la loro provenienza è nota.
Il documento nel sistema di gestione documentale segue il procedimento definito nel manuale di gestione e il sigillo non sembra essere indispensabile come elemento che fornisce valore aggiunto a tali operazioni. Anche il protocollo in uscita utilizza la casella di PEC dell'Area Organizzativa Omogenea, quindi anche in questo caso il sigillo non fornisce particolari vantaggi.
La natura tecnologica del sigillo elettronico, che come abbiamo visto è pressoché identica a quella della firma non porta vantaggi nemmeno nella gestione dell'integrità del documento, quando le operazioni successive alla sottoscrizione digitale rischiano di alterarne l'integrità.
Da queste premesse si deduce che il protocollo informatico, sul piano tecnologico dovrebbe evitare di modificare il documento oggetto dell'operazione con la conseguenza di non preservarne l'integrità. In ogni caso l'apposizione di un sigillo sul documento protocollato non sembra portare alcun effettivo vantaggio.
Nella gestione documentale il sigillo può essere utilizzato quando non c'è l'obbligo di sottoscrizione da parte della persona fisica e si vuole garantire la provenienza (in senso di responsabilità legale e non di origine di trasmissione del documento) e l'integrità. Cioè è opportuno rimanere nella specificità dello strumento senza sconfinare in altri scenari tecnici e normativi.
Allo stato dell'arte, quindi, è utile discutere del possibile utilizzo del sigillo elettronico negli scenari di protocollo informatico e gestione documentale, ma al momento non si percepiscono reali vantaggi mentre il rischio di confusione tra strumenti "legali" differenti può essere elevato.

3.5.4 Sanità elettronica

La sanità elettronica ha utilizzato le sottoscrizioni elettroniche fino dai primi progetti in Lombardia e in altre Regioni. Gli utilizzi da parte degli operatori sanitari sono stati sempre

molto ampi e diffusi nonostante un costante mugugno nei confronti di queste tecnologie. Il personale sosteneva che l'informatica e la complessità nel procedimento clinico introduceva ritardi rispetto all'attività sanitaria.
La disponibilità del sigillo può presentare numerose opportunità al sistema sanitario digitalizzato, proprio perché la sua natura impersonale ma con la validità legale per attestare la provenienza e l'integrità del dato supera la necessità associare il firmatario alla persona fisica.
Il procedimento amministrativo clinico può essere ricondotto all'organizzazione, al reparto o comunque alla funzione giuridica operativa che valida il dato.
La firma apposta con procedura automatica può senza problemi essere sostituita dall'apposizione di sigilli elettronici qualificati anch'essi apposti con procedura automatica analoga a quella della sottoscrizione.
Questo per la refertazione degli esami di laboratorio, per la nota di diario clinico e per una serie di altra documentazione clinica che possiamo definire di routine.

3.5.5 Altri utilizzi

La circostanza che la sottoscrizione elettronica è fisiologicamente connessa alla sottoscrizione autografa non deve far perdere di vista il fatto che il sigillo elettronico è stabilito nel regolamento eIDAS per "autenticare" documenti informatici, software, server o qualsiasi bene digitale riferibile ad una persona giuridica.
La conferma che questa ipotesi sia valida si ha con la lettura del Considerando 65 del regolamento: "*Oltre ad autenticare il documento rilasciato dalla persona giuridica, i sigilli elettronici possono anche servire ad autenticare qualsiasi bene digitale della persona giuridica stessa, quali codici di software o server".*
A titolo di esempio possiamo ipotizzare che il codice sorgente di un pacchetto software possa essere sigillato elettronicamente al fine di consolidare il contenuto del codice "sigillato" e la sua riferibilità alla persona giuridica che "possiede" il software.
Questo approccio è utile in quegli scenari dove il cliente, a sua tutela, chiede al produttore del software di depositare i sorgenti presso un Notaio. Al pacchetto software (il codice sorgente e la documentazione) può essere apposto un sigillo elettronico qualificato per avere la presunzione legale di integrità e correttezza dell'origine dei dati ai quali il sigillo elettronico qualificato è associato.
Ancora più efficace è lo scenario delle ricevute di accettazione o di consegna nella Posta Elettronica Certificata dove la firma elettronica delle stesse è effettuata da un server.
L'efficacia probatoria di queste ricevute può essere elevata a livello europeo se la firma elettronica è sostituita da un sigillo elettronico avanzato qualificato.
Questo si può evincere anche dall'articolo 44 del regolamento (Requisiti per i servizi elettronici di recapito certificato qualificato). Infatti nella lettera d) del paragrafo 1 si stabilisce che "*l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati".*
Stante l'ordinamento nazionale, in attesa delle decisioni governative sul futuro della PEC anche in termini di possibile convergenza con i citati servizi elettronici di recapito certificato

qualificato, appare opportuno utilizzare i principi del sigillo elettronico per le ricevute del sistema PEC.
Questo utilizzo comporta la modifica delle regole di riferimento utilizzando lo strumento delle Linee Guida emanate da AgID in conformità all'articolo 71 dell'ultima versione del CAD.
Altri utilizzi del sigillo elettronico sono in scenari completamente originali. Il diritto d'autore sulla rete Internet per musica e fotografia; per proprietà intellettuali o per progetti opera dell'ingegno.
Alcuni utilizzi sono possibili già con la semplice applicazione del regolamento eIDAS.
In molti altri scenari è indispensabile, per la certezza del diritto, che il Legislatore nazionale coordini le normative specifiche con il concetto di sigillo elettronico e delle sue tre fattispecie.
Alla data di pubblicazione del presente documento nel CAD non è presente alcun riferimento al sigillo elettronico e alla sua efficacia probatoria in alternativa alla firma come conseguenza di una maggiore coerenza giuridica con questo strumento comunitario.

3.6 Conclusioni

Nel presente documento sono state analizzati gli scenari, anche comunitari per utilizzo della firma e del sigillo elettronico come prova di identità, nel caso del sigillo elettronico di persone giuridiche.
In riferimento alle pubbliche amministrazioni si ipotizza l'utilizzo del sigillo nei seguenti scenari:

- documenti interni all'amministrazione che non necessitano per loro natura della firma di un soggetto perché 'interni' ad un processo e che oggi sono tipicamente cartacei: per dematerializzare detti documenti senza necessariamente introdurre la firma o protocollarli perché non previsto dalla Legge.
- Il sigillo potrebbe essere utilizzato, ma solo nel caso in cui non sia già presente un Sistema di Gestione Documentale che consenta di preservare immodificabilità e integrità dei documenti stessi, come richiesto dalla norma: in questo caso infatti sarebbe il Sistema stesso a garantire sia la provenienza che integrità e immodificabilità; introdurre anche il sigillo secondo me non sarebbe errato ma certamente non economico;
- documenti in uscita che attestano atti e fatti detenuti dall'amministrazione: in tutti i casi in cui l'amministrazione emette dei 'certificati', ovvero certifica un'informazione posseduta, se tale emissione può essere automatizzata, su questa può essere apposto un sigillo al posto di una firma e utilizzare il contrassegno elettronico nel caso di produzione di copie cartacee (certificati anagrafici, attestazioni di avvenuta vaccinazione, ecc.);
- comunicazioni tra PA dove la norma o la natura del documento non prevede espressamente una firma (attività dell'Agenzia delle Entrate, fatturazione elettronica, ricevute generiche dove non serve la persona fisica);

- comunicazioni verso cittadini che non necessitano di firma e per cui non è necessario tenere traccia dell'avvenuto ricevimento: in questo modo il sigillo potrebbe sostituire non solo la firma ma anche l'utilizzo della PEC stessa (comunicazioni delle società di servizi pubblici, ex municipalizzate di interruzione di servizi o cose simili);
- attestazioni particolari dove deve essere attestata la provenienza e l'integrità come, in ambito sanitario, la nota di diario clinico che deve essere riferita al reparto, piuttosto che alla persona fisica che la redige;
- comunicazioni da parte di cittadini o con maggiore frequenza imprese verso la PA dove non sia necessaria l'individuazione del responsabile della comunicazione o perché l'utilizzo è di natura "statistica". Un esempio è quello delle dichiarazioni periodiche che le imprese devono fare in relazione all'inquinamento che producono (Es. report annuale per AIA e AUA).

Nel documento si è più volte evidenziato che molti utilizzi del sigillo elettronico sono possibili solo se la normativa vigente, anche di tipo tecnico/organizzativo ne autorizza l'utilizzo.

E' infatti ben noto che l'esplicito riferimento all'utilizzo di una firma impedisce un più valido utilizzo del sigillo.

Anche nel Codice dell'amministrazione digitale sarebbe utile dedicare qualche comma ai principi di utilizzo del sigillo che sono demandati esclusivamente alla norma comunitaria (eIDAS). Si auspica, infine, che nella normativa tecnica e specificamente nelle previste Linee guida si stabiliscano regole chiare per determinare l'equilibrio di utilizzo tra PEC e servizi elettronici di recapito certificato qualificato (SERCQ), sigillo elettronico, sistemi di protocollo informatico e sistemi di gestione documentale.

In questa sede si ricorda semplicemente che la PEC e i SERCQ sono strumenti di trasporto documentale affidabile, il sigillo e la firma sono connessi nel loro ruolo legale al documento, il protocollo è lo strumento di trasparenza amministrativa e la gestione documentale è strumento organizzativo di efficacia ed efficienza della macchina amministrativa.

Allegato 1.3 - Esempio di profilo di certificato qualificato di sigillo elettronico

Il certificato è stato generato per scopi di test.
Come prassi si pubblica la notazione ASN.1 e dopo di essa qualche commento su alcuni punti cruciali delle informazioni contenute nella struttura base e nelle estensioni.

```
    0 2068: SEQUENCE {
 4 1532:   SEQUENCE {
 8    3:     [0] {
10    1:       INTEGER 2
     :       }
13    8:     INTEGER 48 7A F6 1B 01 47 AE D9
23   13:     SEQUENCE {
25    9:       OBJECT IDENTIFIER
     :         sha256WithRSAEncryption (1 2 840 113549 1 1 11)
36    0:       NULL
     :       }
38  172:     SEQUENCE {
41   11:       SET {
43    9:         SEQUENCE {
45    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
50    2:           PrintableString 'IT'
     :         }
     :       }
54   26:       SET {
56   24:         SEQUENCE {
58    3:           OBJECT IDENTIFIER '2 5 4 97'
63   17:           UTF8String 'VATIT-02780480964'
     :         }
     :       }
82   28:       SET {
84   26:         SEQUENCE {
86    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
91   19:           UTF8String 'Intesi Group S.p.A.'
     :         }
     :       }
112  41:       SET {
114  39:         SEQUENCE {
116   3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
121  32:           UTF8String 'Qualified Trust Service Provider'
     :         }
     :       }
```

```
155  56:      SET {
157  54:       SEQUENCE {
159   3:        OBJECT IDENTIFIER commonName (2 5 4 3)
164  47:        UTF8String
     :          'Intesi Group EU Qualified Electronic Seal CA G2'
     :        }
     :       }
     :     }
213  30:    SEQUENCE {
215  13:     UTCTime 23/11/2017 12:51:42 GMT
230  13:     UTCTime 22/11/2022 12:51:42 GMT
     :     }
245 101:    SEQUENCE {
247  11:     SET {
249   9:      SEQUENCE {
251   3:       OBJECT IDENTIFIER countryName (2 5 4 6)
256   2:       PrintableString 'IT'
     :        }
     :       }
260  26:     SET {
262  24:      SEQUENCE {
264   3:       OBJECT IDENTIFIER '2 5 4 97'
269  17:       UTF8String 'VATIT-12345678901'
     :        }
     :       }
288  28:     SET {
290  26:      SEQUENCE {
292   3:       OBJECT IDENTIFIER organizationName (2 5 4 10)
297  19:       UTF8String 'Intesi Group S.p.A.'
     :        }
     :       }
318  28:     SET {
320  26:      SEQUENCE {
322   3:       OBJECT IDENTIFIER commonName (2 5 4 3)
327  19:       UTF8String 'Intesi Group S.p.A.'
     :        }
     :       }
     :     }
348 290:    SEQUENCE {
352  13:     SEQUENCE {
354   9:      OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
365   0:      NULL
     :       }
367 271:     BIT STRING, encapsulates {
```

```
372  266:       SEQUENCE {
376  257:         INTEGER
     :           00 C6 EE B1 E0 10 14 17 13 33 A4 98 92 5D 73 C8
     :           F2 23 21 53 BB 29 5C 60 16 2C 9F 4A 7D CB E0 97
     :           59 43 89 97 FA F8 78 80 E1 15 C3 75 AF C0 12 73
     :           71 70 9F 44 E8 2C 0B 67 48 B2 32 07 44 E3 77 5F
     :           82 94 26 FE 93 5D 1C F7 00 9F 1A AC 3E E9 77 88
     :           26 B7 57 B1 36 16 A2 7E 44 97 74 65 0D C3 B5 D8
     :           85 9A CA 39 65 59 E1 34 7D 84 1A 3E 3A 8B C2 F9
     :           DC 48 50 ED 01 6D FF 2B 1D D5 13 6E D6 5B 63 2B
     :                 [ Another 129 bytes skipped ]
637    3:         INTEGER 65537
     :         }
     :       }
     :     }
642  894:     [3] {
646  890:       SEQUENCE {
650  124:         SEQUENCE {
652    8:           OBJECT IDENTIFIER authorityInfoAccess (1 3 6 1 5 5 7 1 1)
662  112:           OCTET STRING, encapsulates {
664  110:             SEQUENCE {
666   69:               SEQUENCE {
668    8:                 OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
678   57:                 [6]
     :                  'http://caissuers.time4mind.com/Intesi/qualifieds'
     :                  'ealCA.crt'
     :                 }
737   37:               SEQUENCE {
739    8:                 OBJECT IDENTIFIER ocsp (1 3 6 1 5 5 7 48 1)
749   25:                 [6] 'http://ocsp.time4mind.com'
     :               }
     :             }
     :           }
     :         }
776   29:       SEQUENCE {
778    3:         OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
783   22:         OCTET STRING, encapsulates {
785   20:           OCTET STRING
     :             8E 54 06 C5 CC CD 43 40 D7 B7 C4 36 F2 D1 BC DE
     :             86 55 88 FB
     :           }
     :         }
807   12:       SEQUENCE {
809    3:         OBJECT IDENTIFIER basicConstraints (2 5 29 19)
```

```
814   1:         BOOLEAN TRUE
817   2:         OCTET STRING, encapsulates {
819   0:           SEQUENCE {}
      :           }
      :         }
821  31:       SEQUENCE {
823   3:         OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
828  24:         OCTET STRING, encapsulates {
830  22:           SEQUENCE {
832  20:             [0]
      :               E8 D0 6A 58 54 23 FE C0 09 F6 46 E2 44 FD F2 D4
      :               0A 14 2E 60
      :             }
      :           }
      :         }
854 154:       SEQUENCE {
857   8:         OBJECT IDENTIFIER qcStatements (1 3 6 1 5 5 7 1 3)
867 141:         OCTET STRING, encapsulates {
870 138:           SEQUENCE {
873  21:             SEQUENCE {
875   8:               OBJECT IDENTIFIER '1 3 6 1 5 5 7 11 2'
885   9:               SEQUENCE {
887   7:                 OBJECT IDENTIFIER '0 4 0 194121 1 2'
      :               }
      :             }
896   8:             SEQUENCE {
898   6:               OBJECT IDENTIFIER etsiQcsCompliance (0 4 0 1862 1 1)
      :             }
906  11:             SEQUENCE {
908   6:               OBJECT IDENTIFIER
      :                 etsiQcsRetentionPeriod (0 4 0 1862 1 3)
916   1:               INTEGER 20
      :             }
919   8:             SEQUENCE {
921   6:               OBJECT IDENTIFIER etsiQcsQcSSCD (0 4 0 1862 1 4)
      :             }
929  19:             SEQUENCE {
931   6:               OBJECT IDENTIFIER '0 4 0 1862 1 6'
939   9:               SEQUENCE {
941   7:                 OBJECT IDENTIFIER '0 4 0 1862 1 6 2'
      :               }
      :             }
950  59:             SEQUENCE {
952   6:               OBJECT IDENTIFIER '0 4 0 1862 1 5'
```

```
 960  49:            SEQUENCE {
 962  47:              SEQUENCE {
 964  41:                IA5String
      :                'https://www.intesigroup.com/en/documents/'
1007   2:                PrintableString 'en'
      :              }
      :             }
      :            }
      :           }
      :          }
      :         }
1011 439:       SEQUENCE {
1015   3:        OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
1020 430:         OCTET STRING, encapsulates {
1024 426:          SEQUENCE {
1028   9:           SEQUENCE {
1030   7:             OBJECT IDENTIFIER '0 4 0 194112 1 3'
      :            }
1039 411:            SEQUENCE {
1043  12:             OBJECT IDENTIFIER '1 3 6 1 4 1 48990 1 1 2 1'
1057 393:             SEQUENCE {
1061  53:              SEQUENCE {
1063   8:               OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
1073  41:                IA5String
      :                'https://www.intesigroup.com/en/documents/'
      :              }
1116 334:              SEQUENCE {
1120   8:               OBJECT IDENTIFIER unotice (1 3 6 1 5 5 7 2 2)
1130 320:                SEQUENCE {
1134 316:                  BMPString
      :                'Il presente certificato è valido solo per firme '
      :                'apposte con procedura automatica. The certific
ate may only be used for unattended/automatic digital sig
nature.'
      :              }
      :             }
      :            }
      :           }
      :          }
      :         }
1454  68:       SEQUENCE {
1456   3:        OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
1461  61:         OCTET STRING, encapsulates {
```

```
1463  59:          SEQUENCE {
1465  57:            SEQUENCE {
1467  55:              [0] {
1469  53:                [0] {
1471  51:                  [6]
      :                   'http://crl.time4mind.com/Intesi/qualifiedsealCA.'
      :                   'crl'
      :                  }
      :                 }
      :                }
      :               }
      :              }
      :             }
1524  14:           SEQUENCE {
1526   3:            OBJECT IDENTIFIER keyUsage (2 5 29 15)
1531   1:            BOOLEAN TRUE
1534   4:            OCTET STRING, encapsulates {
1536   2:              BIT STRING 6 unused bits
      :                '10'B (bit 1)
      :              }
      :             }
      :            }
      :           }
      :          }
1540  13:       SEQUENCE {
1542   9:        OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1553   0:        NULL
      :         }
1555 513:       BIT STRING
      :         89 D8 B2 C4 E8 C8 93 C1 E6 8B FB 49 B3 55 53 CE
      :         0A 64 47 47 FC 2E 1C D1 64 37 B4 2B AF 35 EE F9
      :         C4 3A C9 E8 D2 7E CC C1 FF 66 36 7C 72 8A A5 D0
      :         3A 1E 64 01 00 14 E8 B1 A0 89 B9 66 1E 1E AE 0E
      :         C6 A6 2B 7D E8 17 19 D6 6C 31 E4 55 0F CA 22 3D
      :         2E 86 7D 95 10 86 8B 27 D4 20 52 5D 97 D1 96 E1
      :         6A C7 F3 4F 69 60 D2 CA 8A ED 58 97 17 FB 50 70
      :         55 CF F9 0B B3 1E 39 00 46 37 0B A3 78 14 5B 5C
      :               [ Another 384 bytes skipped ]
      :       }
```

Come si può notare il certificato qualificato per il sigillo elettronico è apparentemente identico ad uno per la firma. In verità già la stringa'VATIT-12345678901'che valorizza il campo Organization Identifier (2.5.4.97) identifica una partita IVA italiana (VAT IT) secondo gli standard ETSI.

Il certificato presenta anche l'indicazione che è dedicata all'apposizione di sigilli con procedura automatica.
L'OID 0.4.0.194121.1.2 (in grassetto nel testo descrittivo) dell'estensione che specifica il tipo di certificato qualificato indica che si tratta di un certificato emesso ad una persona giuridica, in indispensabile conformità con lo standard ETSI EN 319 412-1.
L'OID 0.4.0.1862.1.6.2 (anche questo in grassetto) indica che si tratta di un certificato qualificato conforme al regolamento eIDAS per il sigillo qualificato in base allo standard ETSI EN 319-412-5.

Allegato 2.3 - Riferimenti al sigillo elettronico nel regolamento eIDAS

Nel seguito sono riportati tutti i riferimenti al sigillo elettronico nel regolamento europeo 910/2014.

Riferimenti nelle premesse:

(50) Poiché attualmente le autorità competenti negli Stati membri utilizzano formati diversi di firme elettroniche avanzate per firmare elettronicamente i loro documenti, occorre garantire che almeno alcuni formati di firma elettronica possano essere supportati tecnicamente dagli Stati membri allorché ricevono documenti firmati elettronicamente. Analogamente, allorché le autorità competenti negli Stati membri fanno uso di sigilli elettronici, occorre garantire che supportino almeno alcuni formati di ***sigillo elettronico avanzato****.*

(58) Qualora una transazione richieda un ***sigillo elettronico qualificato*** *di una persona giuridica, è opportuno che sia accettabile anche la firma elettronica qualificata del rappresentante autorizzato della persona giuridica.*

(59) È opportuno che i ***sigilli elettronici*** *fungano da prova dell'emissione di un documento elettronico da parte di una determinata persona giuridica, dando la certezza dell'origine e dell'integrità del documento stesso.*

(60) I prestatori di servizi fiduciari che rilasciano certificati qualificati di ***sigilli elettronici*** *dovrebbero attuare le misure necessarie per poter stabilire l'identità della persona giuridica rappresentante la persona fisica cui è fornito il certificato qualificato di* ***sigillo elettronico****, quando tale identificazione è necessaria a livello nazionale nel contesto di procedimenti giudiziari o amministrativi.*

(61) È opportuno che il presente regolamento garantisca la conservazione a lungo termine delle informazioni, al fine di assicurare la validità giuridica delle firme elettroniche e dei ***sigilli elettronici*** *nel lungo periodo, garantendo che possano essere convalidati indipendentemente da futuri mutamenti tecnologici.*

(62) Al fine di garantire la sicurezza della validazione temporale elettronica qualificata, il presente regolamento dovrebbe richiedere l'uso di un ***sigillo elettronico avanzato*** *o di una firma elettronica avanzata o di altri metodi equivalenti. È prevedibile che l'innovazione produca nuove tecnologie in grado di assicurare alla validazione temporale un livello di sicurezza equivalente. Ogni qualvolta venga utilizzato un metodo diverso dal* ***sigillo elettronico avanzato*** *o dalla firma elettronica avanzata, dovrebbe spettare al prestatore di servizi fiduciari qualificato dimostrare, nella relazione di valutazione di conformità, che tale metodo garantisce un livello equivalente di sicurezza e soddisfa gli obblighi previsti nel presente regolamento.*

Nell'articolato del regolamento troviamo quanto segue:

Articolo 3 - Definizioni

24) «creatore di un sigillo», una persona giuridica che crea un sigillo elettronico;

25) «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;

26) «sigillo elettronico avanzato», un sigillo elettronico che soddisfi i requisiti sanciti all'articolo 36;

27) «sigillo elettronico qualificato», 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;

28) «dati per la creazione di un sigillo elettronico», i dati unici utilizzati dal creatore del sigillo elettronico per creare un sigillo elettronico;

29) «certificato di sigillo elettronico», un attestato elettronico che collega i dati di convalida di un sigillo elettronico a una persona giuridica e conferma il nome di tale persona;

30) «certificato qualificato di sigillo elettronico», un certificato di sigillo elettronico che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato III;

31) «dispositivo per la creazione di un sigillo elettronico», un software o hardware configurato utilizzato per creare un sigillo elettronico;

32) «dispositivo per la creazione di un sigillo elettronico qualificato», un dispositivo per la creazione di un sigillo elettronico che soddisfa mutatis mutandis i requisiti di cui all'allegato II;

40) «dati di convalida», dati utilizzati per convalidare una firma elettronica o un sigillo elettronico;

41) «convalida», il processo di verifica e conferma della validità di una firma o di un sigillo elettronico.

Riferimenti al sigillo elettronico si trovano

nell'articolo 24, paragrafo 1, lettera c)

*c) mediante un certificato di una firma elettronica qualificata o di un **sigillo elettronico qualificato** rilasciato a norma della lettera a) o b);*

nell'articolo 33, paragrafo 1, lettera b)

*b) consente alle parti facenti affidamento sulla certificazione di ricevere il risultato del processo di convalida in un modo automatizzato che sia affidabile ed efficiente e rechi la firma elettronica avanzata o **il sigillo elettronico avanzato** del prestatore del servizio di convalida qualificato.*

La sezione 5 di del regolamento eIDAS è completamente dedicata ai sigilli elettronici:

SEZIONE 5

Sigilli elettronici

Articolo 35

Effetti giuridici dei sigilli elettronici

1. A un sigillo elettronico non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per i sigilli elettronici qualificati.

2. Un sigillo elettronico qualificato gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico qualificato è associato.

3. Un sigillo elettronico qualificato basato su un certificato qualificato rilasciato in uno Stato membro è riconosciuto quale sigillo elettronico qualificato in tutti gli altri Stati membri.

Articolo 36

Requisiti dei sigilli elettronici avanzati

Un sigillo elettronico avanzato soddisfa i seguenti requisiti:

a) è connesso unicamente al creatore del sigillo;

b) è idoneo a identificare il creatore del sigillo;

c) è creato mediante dati per la creazione di un sigillo elettronico che il creatore del sigillo elettronico può, con un elevato livello di sicurezza, usare sotto il proprio controllo per creare sigilli elettronici; e

d) è collegato ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

Articolo 37

Sigilli elettronici nei servizi pubblici

1. Se uno Stato membro richiede un sigillo elettronico avanzato per poter utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce i sigilli elettronici avanzati, i sigilli elettronici avanzati basati su un certificato qualificato di sigillo elettronico e i sigilli elettronici qualificati che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.

2. Se uno Stato membro richiede un sigillo elettronico avanzato basato su un certificato qualificato per poter utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce i sigilli elettronici avanzati basati su un certificato qualificato e i sigilli elettronici qualificati che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.

3. Gli Stati membri non richiedono, per l'utilizzo transfrontaliero in un servizio online offerto da un organismo del settore pubblico, un sigillo elettronico dotato di un livello di garanzia di sicurezza più elevato di quello del sigillo elettronico qualificato.

4. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai sigilli elettronici avanzati. Si presume che i requisiti per i sigilli elettronici avanzati di cui ai paragrafi 1 e 2 del presente articolo e all'articolo 36 siano rispettati ove un sigillo elettronico avanzato soddisfi dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.IT L 257/104 Gazzetta ufficiale dell'Unione europea 28.8.2014

5. Entro il 18 settembre 2015, e tenendo conto delle prassi, delle norme e degli atti giuridici dell'Unione vigenti, la Commissione, mediante atti di esecuzione, definisce i formati di riferimento dei sigilli elettronici avanzati o i metodi di riferimento nel caso in cui siano utilizzati formati alternativi. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 38

Certificati qualificati di sigilli elettronici

1. I certificati qualificati di sigilli elettronici soddisfano i requisiti di cui all'allegato III.

2. I certificati qualificati di sigilli elettronici non sono soggetti a requisiti obbligatori oltre ai requisiti di cui all'allegato III.

3. I certificati qualificati di sigilli elettronici possono includere attributi specifici aggiuntivi non obbligatori. Tali attributi non pregiudicano l'interoperabilità e il riconoscimento dei sigilli elettronici qualificati.

4. Qualora un certificato qualificato di un sigillo elettronico sia stato revocato dopo l'iniziale attivazione, esso decade della propria validità dal momento della revoca e la sua situazione non è ripristinata in nessuna circostanza.

5. Fatte salve le condizioni seguenti, gli Stati membri possono fissare norme nazionali in merito alla sospensione temporanea dei certificati qualificati di sigilli elettronici:

a) in caso di temporanea sospensione di un certificato qualificato di sigillo elettronico, il certificato perde la sua validità per il periodo della sospensione;

b) il periodo di sospensione è indicato chiaramente nella banca dati dei certificati e la situazione di sospensione è visibile, durante il periodo di sospensione, dal servizio che fornisce le informazioni sulla situazione del certificato.

6. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai certificati qualificati di sigilli elettronici. Si presume che i requisiti di cui all'allegato III siano stati rispettati ove un certificato qualificato di sigillo elettronico risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 39

Dispositivi per la creazione di un sigillo elettronico qualificato

1. L'articolo 29 si applica mutatis mutandis ai requisiti per i dispositivi per la creazione di un sigillo elettronico qualificato.

2. L'articolo 30 si applica mutatis mutandis alla certificazione dei dispositivi per la creazione di un sigillo elettronico qualificato.

3. L'articolo 31 si applica mutatis mutandis alla pubblicazione di un elenco di dispositivi per la creazione di un sigillo elettronico qualificato certificati.

Articolo 40

Convalida e conservazione dei sigilli elettronici qualificati

Gli articoli 32, 33 e 34 si applicano mutatis mutandis alla convalida e alla conservazione dei sigilli elettronici qualificati.IT 28.8.2014 Gazzetta ufficiale dell'Unione europea L 257/105

Poi il sigillo viene ulteriormente referenziato nell'articolo 42, paragrafo 1, lettera c)

c) è apposta mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente.

Nell'articolo 44, paragrafo 1, lettera d)

d) l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati;

Nell'allegato I lettere g), h)

g) la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato che rilascia il certificato;

h) il luogo in cui il certificato relativo alla firma elettronica avanzata o al sigillo elettronico avanzato di cui alla lettera g) è disponibile gratuil certificati qualificati dei sigilli elettronici contengono:

a) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che il certificato è stato rilasciato quale certificato qualificato di sigillo elettronico;

b) un insieme di dati che rappresenta in modo univoco il prestatore di servizi fiduciari qualificato che rilascia i certificati qualificati e include almeno lo Stato membro in cui tale prestatore è stabilito e

- *per una persona giuridica: il nome e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali,*
- *per una persona fisica: il nome della persona;*

c) almeno il nome del creatore del sigillo e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali;

d) i dati di convalida del sigillo elettronico che corrispondono ai dati per la creazione di un sigillo elettronico;

e) l'indicazione dell'inizio e della fine del periodo di validità del certificato;

f) il codice di identità del certificato che deve essere unico per il prestatore di servizi fiduciari qualificato;

g) la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato che rilascia il certificato;

h) il luogo in cui il certificato relativo alla firma elettronica avanzata o al sigillo elettronico avanzato di cui alla lettera g) è disponibile gratuitamente;

i) l'ubicazione dei servizi a cui ci si può rivolgere per informarsi sulla validità del certificato qualificato;

j) qualora i dati per la creazione di un sigillo elettronico connessi ai dati di convalida del sigillo elettronico siano ubicati in un dispositivo per la creazione di un sigillo elettronico qualificato, un'indicazione appropriata di questo fatto, almeno in una forma adatta al trattamento automatizzato.IT 28.8.2014 Gazzetta ufficiale dell'Unione europea L 257/113.

I protagonisti del Cantiere

Mariella Guercio
Presidente Associazione nazionale archivistica italiana - Anai

Rosa Maria Bertè
Funzionario Servizio Gestione Centro Unico Servizi, Direzione Generale dei Sistemi informativi, Corte dei conti

Alessandro Alfier
Responsabile vicario della conservazione per il Dipartimento dell'amministrazione generale, Ministero dell'Economia e delle Finanze

Gabriele Bezzi
Responsabile presidio funzione archivistica di conservazione e gestione dei rapporti con gli Enti produttori, Polo Archivistico Emilia-Romagna

Marco Argenziano
Ufficio Gestione Documentale, Istituto Nazionale di Geofisica e Vulcanologia

Gaetano Bruno
Business Analyst Agenzia per l'Italia Digitale

Alberto Baffigi
Responsabile dell'Archivio Storico Banca d'Italia

Loredana Bozzi
Direttore Ufficio Digitalizzazione dell'attività amministrativa, Provincia Autonoma di Trento

Elisabetta Belloni
Responsabile Servizio Gestione Documentale, Comune di Bergamo

Roberto Carosi
Public Sector & Utilities, Dedagroup Public Services

Cristiana Carratù
Funzionario Collaboratore amministrativo presso la DGSIA-CUS Corte dei conti

Giancarlo Di Capua
Responsabile Servizio Governo Elettronico, InnovaPuglia S.p.A.

Marco Ceccolini
Responsabile Area Servizi Documentali, Lombardia Informatica

Stefano Di Leo
Direttore Area dematerializzazione atti, gestione flussi documentali e razionalizzazione archivi digitali e cartacei, Direzione Centrale Patrimonio e Archivi, INPS

Dante Ciantra
Dirigente di Strategic Business Unit, Gruppo Filippetti

Laura Flora
Responsabile amministrativo, INAF Osservatorio astronomico di Trieste

Luca Cicinelli
Project Manager, InnovaPuglia

Patrizia Gentili
Responsabile Servizio documentale, Agenzia per l'Italia Digitale

Alessandra Cornero
Responsabile Ufficio gestione documentale, Formez PA

Silvia Ghiani
Responsabile Area Servizi Amministrazione Digitale, Lepida Spa

Barbara Corvisieri
Archivista Tecnologa, ISTAT

Stefano Ianniello
Agenzia per l'Italia Digitale

Costantino Landino
Istituto Centrale per gli Archivi – ICAR Ministero per i Beni e le attività culturali

Cristina Palumbo
Coordinatore Struttura stabile per la gestione dell'archivio e del protocollo e per il coordinamento sull'applicazione del CAD, Regione Autonoma Friuli Venezia Giulia

Carlo Lentini
Consulenza per l'Innovazione tecnologica, INAIL

Daniela Penzo
Responsabile di team - direzione centrale patrimoni archivi INPS

Giovanni Manca
Vice Presidente ANORC - Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale

Ilaria Pescini
Responsabile Archivi e Sistema Documentale, DG Organizzazione e sistemi informativi, Regione Toscana

Maria Teresa Manoni
Dirigente Ufficio Attività Istituzionali, Consiglio regionale del Veneto

Stefania Piersanti
Direzione Generale Archivi Ministero per i beni e le attività culturali

Antonio Massari
Director of Service Line Digital Transformation Solutions, Dedagroup Public Services

Maria Emanuela Pinto
Referente gruppo di lavoro "Archiviazione e Digitalizzazione dei documenti", FNOMCeO

Roberto Monaco
Segretario Nazionale, FNOMCEO

Andrea Presta
Responsabile della conservazione e Coordinatore vicario della gestione documentale - Regione autonoma Friuli Venezia Giulia

Anna Ponti
Tecnico Amministrativo, Università degli Studi dell'Insubria

Armando Tomasi
Direttore Ufficio Beni Archivistici, Librari e Archivio Provinciale, Provincia Autonoma di Trento

Franca Russo
Dirigente Ufficio della Direzione sistema informativo della fiscalità, Dipartimento delle Finanza Ministero dell'Economia e delle Finanze

Brizio Leonardo Tommasi
Responsabile delegato alla gestione dei flussi documentali e archivi e del sistema documentale, CONSOB

Alessandro Salone
Archivista Storico presso Archivio Capitolino Comune di Roma

Silvia Trani
Funzionario archivista di Stato, Archivio Centrale dello Stato

Valeria Sisti
Head of Consulting & Archival Support at Digital Transformation Services, Dedagroup Public Service

Barbara Troiani
Ufficio Demand e processi digitali, INAIL

Giovanna Tedeschi
Responsabile dell'ufficio protocollo-archivio, Consiglio regionale del Veneto

Cristina Valiante
Area Trasformazione Digitale – Servizio Documentali Agenzia per l'Italia digitale

Alessandro Todeschini
Dirigente Servizio Registro generale dei testamenti, sistemi informatici, statistiche e contabilità, Ufficio Centrale degli Archivi Notarili, Ministero della Giustizia

Giovanni Veterini
Project Manager, Sistemi di Document e Workflow management del MEF Sogei

DEDAGROUP PUBLIC SERVICES

Gruppo Filippetti