Allegato n. 19

Protocollo n. 236/2016/3.4/2016/1

NTT DATA

Global IT Innovator

Analisi del sistema DOCSPA in relazione alla normativa vigente

Documento analisi

Codice: DOCSPA-2015_001_01

Data emissione/ultima modifica: 30-12-2015

Distribuzione: CLIENTI DOCSPA

EVOLUZIONE DEL DOCUMENTO

Versione	Descrizione
01	Prima emissione

INDICE

1 INTRODUZIONE

1.1 Premessa

Il sistema DocsPA è stato realizzato in base ai requisiti richiesti dal Testo Unico in materia di documentazione amministrativa (DPR 445/2000) e alla precedente normativa sul protocollo informatico, il DPR 428/1998 e relative regole tecniche, poi sostituiti dal TUDA che raccoglie le disposizioni legislative e regolamentari contenute nel DLG 28 dicembre 2000, n. 443 e nel DPR 28 dicembre 2000, n. 444. In seguito il Codice dell'Amministrazione Digitale è diventato il principale testo normativo di riferimento (D. Lgs 82/2005). L'introduzione delle nuove funzionalità e le evoluzioni del sistema nel corso degli anni hanno tenuto conto dei nuovi standard e delle nuove Regole Tecniche introdotte nei Decreti del Presidente del Consiglio dei Ministri per l'applicazione del Codice dell'Amministrazione Digitale.

Le ultime Regole Tecniche sulla conservazione e sul protocollo informatico risalgono al DPCM del 3 dicembre 2013 e sono state pubblicate sulla Gazzetta Ufficiale il 12 marzo 2014. Le pubbliche amministrazioni devono adeguare i propri sistemi di gestione informatica dei documenti entro e non oltre 18 mesi dall'entrata in vigore del decreto e pertanto entro e non oltre il 12 ottobre 2015. Sulla Gazzetta Ufficiale del 12 gennaio 2015 sono state pubblicate invece le ultime Regole Tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di conservazione dei documenti informatici delle pubbliche amministrazioni (DPCM 13 Novembre 2014) alle quali le Pubbliche amministrazioni dovranno adeguarsi ancora entro e non oltre diciotto mesi dall'entrata in vigore del decreto e cioè entro e non oltre il 12 agosto del 2016. In uno scenario internazionale invece il Regolamento (UE) n.910/2014 del Parlamento Europeo e del Consiglio del 23 Luglio 2014 pone requisiti in materia di firma elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno che vanno ad abrogare la direttiva 1999/93/CE. Tale regolamento stabilisce le condizioni per il riconoscimento reciproco in ambito di identificazione elettronica e le regole comuni, oltre che per le firme elettroniche, anche per l'autenticazione web. Tale regolamento si applica a decorrere dal 1° luglio 2016.

1.2 Scopo e area di applicazione

Con il presente documento si intende descrivere le funzionalità del sistema DocsPA rispetto alle indicazioni ed ai requisiti di cui alle norme citate in precedenza tra le quali, in particolare il Codice dell'Amministrazione Digitale (CAD) e il Testo Unico in materia di documentazione amministrativa (DPR 445/2000).

2 RISPOSTA DEL SISTEMA DOCSPA ALLA NORMATIVA VIGENTE

2.1 Protocollo informatico

Il DPCM del 3 dicembre 2013 richiede nel dettaglio un adeguamento alle norme in materia di **Protocollo informatico**. Nello specifico alcuni articoli sono riservati al tema delle funzionalità minime di un sistema informatico, altri presentano i requisiti minimi di sicurezza dei sistemi di protocollo informatico e altri ancora pongono le regole per l'annullamento informatico delle registrazioni in forma immodificabile. Attenzione particolare viene poi posta sul formato della segnatura di protocollo. Analizziamo di seguito le funzionalità del sistema DocsPA rispetto ai requisiti previsti dalla normativa sopra citata.

2.1.1 Requisiti minimi di sicurezza dei sistemi di protocollo informatico

Per quanto riguarda i requisiti minimi di sicurezza il sistema DocsPA permette:

- l'univoca identificazione ed autenticazione degli utenti come richiesto dall' Art.7 c.1 lett. a) permettendo infatti nel modulo di amministrazione di censire gli utenti che hanno accesso al

sistema e di associare ad ogni utente un codice proprio ed una password propria che lo identifica univocamente.

- la protezione delle informazioni relative a ciascun utente nei confronti degli altri come previsto dall' Art.7 c.1 lett b), consentendo ad un utente amministratore di gestire i dati e le informazioni relative ai singoli utenti.
- l'accesso alle risorse esclusivamente agli utenti abilitati secondo l' Art.7 c.1 lett c). Nel modulo di amministrazione è possibile abilitare ogni singolo utente a determinate funzioni attraverso la configurazione nell'organigramma di un ruolo di appartenenza e l'amministratore può abilitare o meno l'utente all'accesso nel sistema.
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione (Art.7 c.1 lett d)). Nel modulo di amministrazione del sistema è possibile tener traccia delle azioni di ogni utente attraverso l'abilitazione dei Log. Si può decidere nello specifico di quali azioni tener traccia o meno.

Il sistema DocsPA, in base a quanto richiesto dall' Art.7 c.2, assolve alla funzione di controllo differenziato dell'accesso alle risorse per ciascun utente o gruppo di utenti. Ogni utente può infatti accedere soltanto a determinate risorse in funzione del gruppo di appartenenza.

DocsPA inoltre consente il tracciamento degli eventi di modifica delle informazioni trattate e l'individuazione del suo autore (Art.7 c.3).

La modifica delle informazioni è consentita esclusivamente agli utenti espressamente autorizzati (Art. 7 c.4)

Il sistema DocsPA non consente la modifica del registro giornaliero di protocollo. Inoltre ne può consentire la trasmissione, entro la giornata lavorativa successiva alla sua generazione, ad un sistema di conservazione (Art.7 c.5). DocsPA infatti può facilmente integrarsi tramite WS con sistemi di conservazione (già esistenti o sviluppati *ad hoc*) che gestiscono tale processo, oltre a disporre esso stesso di uno specifico modulo software già integrato per la gestione del processo di conservazione con opportune impostazioni.

Il sistema DocsPA ha implementato funzionalità che prendono in considerazione le misure di sicurezza previste dagli articoli da 31 a 36 e dal disciplinare tecnico di cui all'allegato B del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, come richiesto dall'Art.7 c.6 del DPCM. Si precisa al riguardo che il rispetto di tali misure di sicurezza è legato anche alla sussistenza di fattori e requisiti di sistema e di infrastruttura estranei al sistema DocsPA medesimo e con il quale quest'ultimo potrebbe interfacciarsi (ad es. alcuni requisiti riguardanti l'infrastruttura sulla quale viene installato il sistema DocsPA).

Secondo quanto richiesto nell'Art.34 c.1 del Codice in Materia di Protezione dei Dati Personali, il trattamento dei dati personali effettuato con DocsPA prevede:

- L'autenticazione informatica;
- L'adozione di procedure di gestione delle credenziali di autenticazione (sono gestite, nello specifico, la scadenza della password, il formato della password, l'annullamento della password con necessità di cambiamento al primo accesso. Inoltre la password viene memorizzata sul DB in forma cifrata);

Il sistema DocsPA consente di attribuire un determinata configurazione di riservatezza a particolari tipologie di documenti che sono così accessibili esclusivamente alle persone designate al loro trattamento. Inoltre il sistema DocsPA dispone di un insieme di regole che permettono il controllo sull'accessibilità dei documenti e dati in esso gestiti da parte degli utenti stessi del sistema. Pertanto tutti i dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari possono in tal modo essere preservati dalla visibilità di utenti non autorizzati (Art.34 c.1 lett h).

Relativamente all'Allegato B al codice in Materia di Protezione dei Dati Personali ovvero il disciplinare tecnico in materia di misure minime di sicurezza DocsPA consente quanto segue:

- configurare dei particolari ruoli per gli utenti riservati al trattamento di dati personali dotando gli incaricati di credenziali che consentono il superamento di una procedura di autenticazione relativa ad uno specifico trattamento..

- fornire credenziali di autenticazione che consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato
- assegnare o associare ad ogni incaricato individualmente una o più credenziali per l'autenticazione. impostare l'obbligo di utilizzare una parola chiave, composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; la parola chiave viene impostata per il primo accesso dall'amministratore e obbligatoriamente dovrà essere modificata dall'incaricato al primo utilizzo. Il sistema DocsPA consente di impostare regole per la composizione della parola chiave. L'intervallo temporale oltre il quale è necessario modificare la password si può impostare indipendentemente dalla tipologia del dato trattato.
- Un codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi. Il sistema DocsPA impedisce l'uso dello stesso codice identificativo per utenti differenti e, nel caso in cui più Amministrazioni utilizzino la stessa istanza del sistema, permette di verificare, quando una Amministrazione registra un nuovo utente se questo sia già registrato come utente di un'altra Amministrazione. In questo caso il sistema chiede conferma della volontà di creare un utente comune ad entrambe le Amministrazioni.
- DocsPA, consente di disattivare le credenziali di autenticazione non utilizzate per un periodo che l'amministrazione configurerà di volta in volta, potendo fare eccezione per quelle preventivamente autorizzate per soli scopi di gestione tecnica. Il sistema DocsPA consente di disattivare le credenziali anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali. Il sistema DocsPA, nel caso in cui un utente perda il suo ruolo e quindi le sue funzionalità e le sue autorizzazioni, consente di mantenere l'utente censito ma disabilitato all'accesso.
- Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione. Il sistema DocsPA può essere integrato con sistemi esterni di autenticazione e gestione delle identità e degli accessi (IAM, Shibboleth, ecc…). Inoltre il sistema DocsPA consente di associare ad uno stesso utente profili di autorizzazione differenti, ovvero uno o più ruoli, ciascuno con un proprio specifico profilo funzionale e propri diritti di visibilità sui documenti.
- I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Un utente può accedere al sistema DocsPA solo se precedentemente è stato associato ad uno specifico ruolo in organigramma (non è sufficiente il suo censimento come utente); dalla posizione in organigramma e dal profilo funzionale del ruolo deriva il "profilo di autorizzazione" dell'utente sia in termini di funzionalità che è abilitato ad utilizzare, sia in termini di documenti a cui può avere accesso.
- Per quanto riguarda la frequenza degli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti anche in caso di trattamento di dati sensibili o giudiziari il requisito è legato alla gestione dell'infrastruttura del sistema.
- La protezione dall'accesso abusivo a dati sensibili o giudiziari di cui all'art. 615-ter del codice penale, può essere garantita mediante l'utilizzo di idonei strumenti elettronici di supporto che debbono essere messi a diposizione dalle piattaforme su cui viene istallato DOCSPA. Attraverso le funzioni di tipizzazione dei documenti è possibile separare particolari dati sensibili o giudiziari da altre tipologie di informazioni.

2.1.2 Annullamento delle informazioni registrate in forma immodificabile

Passiamo ad analizzare la risposta del sistema a quanto richiesto dalla normativa in materia dell'annullamento delle informazioni registrate in forma immodificabile.

Nel sistema DocsPA:

- l'annullamento anche di una sola delle informazioni generate o assegnate automaticamente dal sistema e registrate in forma immodificabile è possibile solo con il contestuale annullamento dell'intera registrazione di protocollo come richiesto dall' Art.8 c.1 del DPCM del 3 dicembre 2013.
- L'annullamento anche di un solo campo delle altre informazioni registrate in forma immodificabile, necessario per correggere errori intercorsi in sede di immissione di dati delle altre informazioni, comporta 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. La disposizione di cui al primo periodo si applica per lo stesso campo, od ogni altro, risultato successivamente errato. (Art.8 c.2 del DPCM del 3 dicembre 2013).
- Le informazioni originarie, successivamente annullate, vengono memorizzate secondo le modalità specificate nell'art. 54 del testo unico [DPR 445 del 28 dicembre 2000], come richiesto dall'Art.8 c.3 del DPCM del 3 dicembre 2013, ovvero il numero di protocollo del documento, la data di registrazione di protocollo, il mittente per i documenti ricevuti, il destinatario o i destinatari per i documenti spediti, l'oggetto del documento, la data e il protocollo del documento ricevuto e l'impronta del documento sono annullabili e le informazioni annullate sono memorizzate nella base di dati per essere sottoposte alle elaborazioni previste dalla procedura. La procedura per indicare l'annullamento riporta, secondo i casi, una dicitura o un segno in posizione sempre visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento d'autorizzazione.

2.1.3 Formato della segnatura di protocollo

Per quanto richiesto sul formato della segnatura di protocollo, in DocsPA

- Le informazioni apposte o associate ai documenti informatici, registrati nel registro di protocollo, negli altri registri di cui all'art. 53, comma 5, del testo unico, nei repertori e negli archivi, nonché negli albi, negli elenchi e in ogni raccolta di dati concernente stati, qualità personali e fatti con le modalità descritte nel manuale di gestione, mediante l'operazione di segnatura di cui all'art. 55 del testo unico che ne garantisce l'identificazione univoca e certa, sono espresse nel seguente formato:
  - Codice identificativo dell'amministrazione;
  - Codice identificativo del registro;
  - Data di protocollo;
  - Progressivo di protocollo costituito da almeno sette cifre numeriche. La numerazione è rinnovata ogni anno solare.
  - Codice identificativo dell'area organizzativa omogenea.

  Il sistema DocsPA consente la configurazione del formato della segnatura. L'amministratore del sistema può selezionare i valori da inserire nella segnatura tra quelli elencati, l'anno di protocollazione, l'ora di protocollazione e il tipo di registrazione. La rispondenza della segnatura a quanto previsto dalla normativa dipende pertanto da come viene configurata dall'Amministrazione; in particolare, in DocsPA il codice identificativo dell'area organizzativa omogenea è legato al Registro, è cioè presente se viene utilizzato come codice del registro il codice dell'AOO.

2.2 Formato e modalita' di trasmissione dei documenti informatici tra pubbliche amministrazioni

Il sistema DocsPA permette alle pubbliche amministrazioni di comunicare attraverso la funzione di interoperabilità rispondendo ai requisiti richiesti dall'articolo 10 c.2 del DPCM del 3 dicembre 2013.

Le pubbliche amministrazioni che mediante proprie applicazioni informatiche accedono al sistema, adottano le modalità di interconnessione stabilite nell'ambito delle norme e dei criteri tecnici emanati per

la realizzazione della rete unitaria delle pubbliche amministrazioni. (Art.60 c.1 DPR 445 del 28 dicembre 2000).

Le pubbliche amministrazioni che accedono al sistema grazie all'interoperabilità, secondo quanto richiesto dall'Art.60 c.2 del DPR445/2000, possono ottenere le seguenti informazioni:

a) numero e data di registrazione di protocollo dei documenti, ottenuti attraverso l'indicazione alternativa o congiunta dell'oggetto, della data di spedizione, del mittente, del destinatario;

b) numero e data di registrazione di protocollo del documento ricevuto, ottenuti attraverso l'indicazione della data e del numero di protocollo attribuiti dall'amministrazione al documento spedito.

Il codice identificativo dell'amministrazione, assegnato automaticamente dall'indice IPA in fase di accreditamento, è riportato nei dati della segnatura di protocollo (Art.13 c.1 DPCM 3 dicembre 2013) se viene riportato come codice di AOO.

2.2.1 Modalita' di trasmissione dei documenti informatici mediante l'utilizzo della posta elettronica e in cooperazione applicativa

Lo scambio dei documenti soggetti alla registrazione di protocollo nel sistema DocsPA è effettuato mediante messaggi di posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o messaggi conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC821-822, RFC 2045 e 2049 e successive modificazioni. (Art.16 c.1)

Il Codice dell'Amministrazione Digitale nell'Art.47 stabilisce le norme riguardo alla trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni. Esso richiede che le comunicazioni di documenti tra le pubbliche amministrazioni avvengano mediante l'utilizzo della posta elettronica o in cooperazione applicativa; tali comunicazioni sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza. DocsPA realizza proprio l'interoperabilità tra sistemi di protocollo di amministrazioni differenti mediante il canale della PEC.

Il sistema DocsPA, nella comunicazione tra le pubbliche amministrazioni, supporta l'accertamento della provenienza dei documenti informatici ricevuti per via telematica, secondo quanto previsto dall'Art. 47 c.2 del CAD,

- consentendo l'integrazione con specifici servizi di verifica di validità delle firme digitali o realizzando un'analoga verifica con propri strumenti,

- elaborando automaticamente la segnatura xml dei documenti ricevuti per interoperabilità e mantenendo associato al documento e visibile dall'utente il file xml della segnatura,

- - valorizzando automaticamente il mittente del documento con l'indirizzo mail di provenienza o i dati del corrispondente censito nell'anagrafica del sistema che ha associato tale indirizzo.

2.2.2 Modalita' di registrazione dei documenti informatici

Il sistema DocsPA ad ogni messaggio ricevuto o spedito da un'area organizzativa omogenea di una pubblica amministrazione fa corrispondere un'unica operazione di registrazione di protocollo (Art.18 c.1), con esclusione di interventi intermedi, anche indiretti, da parte dell'operatore, permettendo il completamento dell'intera operazione di modifica o registrazione dei dati come richiesto dal DPR 445/2000 nell'Art.53 c.3.

La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione delle seguenti informazioni (Art.53 c.1 DPR 445/2000):

- il numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile
- data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;

- mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- data e protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

DocsPA consente 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 come richiesto dal DPR 445/2000 nell'Art.53 c.2.

I documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici sono registrati nel sistema DocsPA (Art.53 c.5 DPR 445/2000). Sono comprese le comunicazioni che pervengono o sono inviate dalle caselle di posta elettronica (semplice o certificata).

L'eventuale indicazione dell'ufficio utente, ovvero del soggetto, destinatario del documento, è riportata nella segnatura di protocollo e cioè nel file .xml della segnatura come chiesto nell' Art. 53 c.5 del DPR 445/2000 e come vedremo meglio in seguito.

2.2.3 Impronta del documento informatico

Nell'effettuare l'operazione di registrazione di protocollo dei documenti informatici il sistema DocsPA calcola l'impronta per ciascun documento informatico associato alla registrazione di protocollo utilizzando la funzione crittografica di hash definita nella deliberazione CNIPA 45/2009, recante le regole per il riconoscimento e la verifica del documento informatico, secondo quanto emanato nell' Art.19 del DPCM in materia del protocollo informatico del 3 dicembre 2013.

2.2.4 Segnatura di protocollo dei documenti trasmessi

Nel sistema DocsPA i dati relativi alla segnatura di protocollo di un documento trasmesso da un'area organizzativa omogenea sono associati al documento stesso e contenuti, nel messaggio, in un file, conforme alle specifiche dell'Extensible Markup Language (XML), compatibile con un file XML Schema e/o DTD (Document Type Definition). Nelle attività di manutenzione sono realizzati gli aggiornamenti necessari relativamente agli standard, alle modalità di trasmissione, ai formati e alle definizioni dei tipi di informazioni scambiate tra le amministrazioni pubbliche e associate ai documenti protocollati come richiesto nell' Art.20 del DPCM del 3 dicembre 2013.

Il file .xml contenente i dati relativi alla segnatura di protocollo racchiude inoltre le seguenti informazioni:

- l'oggetto
- il mittente
- il destinatario o i destinatari

come richiesto nell' Art.21 c.1 del DPCM del 3 dicembre 2013.

Nella segnatura di un documento protocollato in uscita da un'Amministrazione possono essere specificate inoltre una o più delle seguenti informazioni incluse anch'esse nello stesso file:

- indicazione della persona o dell'ufficio all'interno della struttura destinataria a cui si presume verrà affidato il trattamento del documento; e/o
- l'indice di classificazione; e/o
- l'identificazione degli allegati,

come indicato nell'art.21 c.2 del DPCM del 3 dicembre 2013, ma non sono gestiti dal sistema dati specifici sull'iter amministrativo a cui è soggetto il documento. Vengono gestiti soltanto i dati legati alla

classificazione e alla fascicolazione del documento, se tali operazioni sono state effettuate nel sistema DocsPA.

È possibile estendere il file .xml della segnatura di protocollo di un documento informatico se due o più amministrazioni stabiliscono di scambiarsi informazioni non previste tra quelle indicate nell'Art.21 c.2 ed elencate precedentemente, includendo informazioni specifiche stabilite di comune accordo, nel rispetto delle indicazioni tecniche stabilite dall'Agid (Art.21 c.3 DPCM del 3 dicembre 2013).

2.2.5 Comunicazioni tra imprese e amministrazioni pubbliche

Il sistema DocsPA si integra con i canali si comunicazione telematica (posta elettronica semplice e posta elettronica certificata) consentendo di gestire direttamente a partire dal sistema le operazioni di ricezione, registrazione e spedizione dei messaggi/documenti scambiati dall'amministrazione con soggetti esterni pubblici e privati come indicato nell' Art.5 bis del Codice di Amministrazione Digitale.

2.3 Documento informatico

2.3.1 Segnatura di protocollo

Il sistema DocsPA permette di associare all'originale del documento la segnatura di protocollo e di apporla sul documento anche attraverso un timbro. Tale apposizione o associazione viene effettuata in forma permanente non modificabile delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile. La segnatura di protocollo contiene le seguenti informazioni previste dal D.P.R. 445/2000 nell'Art.55 c.1:

- Il progressivo di protocollo
- La data di protocollo
- L'identificazione in forma sintetica dell'amministrazione o dell'area organizzativa omogenea.

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo come richiesto sempre dal D.P.R 445/2000 nell'Art.55 c.2.

Mediante una opportuna configurazione del sistema DocsPA è possibile includere nell'operazione di segnatura il codice identificativo dell'ufficio cui il documento è assegnato o il codice dell'ufficio che ha prodotto il documento, l'indice di classificazione del documento e ogni altra informazione utile o necessaria, qualora tali informazioni siano disponibili già al momento della registrazione di protocollo (D.P.R 445/2000 Art.55 c.3).

Con la segnatura in formato .xml è possibile includere tutte le informazioni di registrazione del documento che sono state selezionate dall'Amministrazione all'atto della configurazione. Quando il documento è indirizzato ad altre amministrazioni ed è formato e trasmesso con strumenti informatici, l'amministrazione che riceve il documento informatico può utilizzare le informazioni di registrazione del documento per automatizzare le operazioni di registrazione di protocollo del documento ricevuto (D.P.R. 445/2000 Art.55 c.4)

Il formato e la struttura delle informazioni associate al documento informatico tengono conto di quanto stabilito al c4 del D.P.R. 445/2000.

2.4 Operazioni ed informazioni minime del sistema di gestione informatica dei documenti

Il sistema DocsPA consente di gestire la protocollazione e la fascicolazione, operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni (D.P.R. 445/2000 Art.56 c.1).

2.4.1 Formazione del documento amministrativo informatico

Il documento amministrativo informatico è identificato e trattato nel sistema comprensivo del registro di protocollo e degli altri registri, dei repertori e degli archivi, nonchè degli albi, degli elenchi e di ogni raccolta di dati concernente stati, qualità personali e fatti già realizzati dalle amministrazioni su supporto informatico, in luogo dei registri cartacei con le modalità descritte nel manuale gestione (DPCM 14 novembre 2014, Art.9 c.3)

In DocsPA il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema come richiesto nella normativa nell'art.9 c.5 del DPCM DEL 14 novembre 2014.

In DocsPA è possibile andare incontro alle diverse esigenze delle pubbliche amministrazioni riguardanti i diversi formati da utilizzare. È possibile alle pubbliche amministrazioni utilizzare diversi formati in relazione agli specifici contesti operativi che devono essere esplicitati, motivati e riportati nel manuale di gestione (DPCM 14 novembre 2014, Art.9 c.6).

Al documento amministrativo informatico sono associati, oltre all'insieme minimo, eventuali ulteriori metadati rilevanti ai fini amministrativi, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce (DPCM 14 novembre 2014, Art.9 c.8).

2.4.2 Copie su supporto informatico di documenti amministrativi analogici

Il sistema DocsPA consente di inserire nel documento informatico contenente la copia informatica di un documento amministrativo analogico, formato dalla pubblica amministrazione, ovvero da essa detenuto, l'attestazione di conformità della copia stessa. Il documento informatico così formato può essere sottoscritto con firma digitale o firma elettronica qualificata del funzionario delegato grazie alle funzionalità di firma presenti nel sistema (DPCM 14 novembre 2014, Art.10 c.1).

Il sistema DocsPA consente di produrre l'attestazione di conformità, anche nel caso di uno o più documenti amministrativi informatici. Tale attestazione viene effettuata mediante un'operazione di raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche finalizzate ad accertare la corrispondenza del contenuto dell'originale e della copia, come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia. Il sistema DocsPA consente ove richiesto la sottoscrizione del documento informatico prodotto, con firma digitale o con firma elettronica qualificata del funzionario delegato. (DPCM 14 novembre 2014, Art.10 c.2).

2.5 Procedimento e fascicolo informatico

2.5.1 Procedimento e fascicolo informatico

La normativa richiede che la pubblica amministrazione titolare del procedimento raccolga in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati (CAD Art.41 c.2). Il sistema DocsPA consente la creazione e la gestione di fascicoli elettronici, legati al piano di classificazione dell'archivio, e l'aggregazione in essi di documenti protocollati (prodotti o ricevuti dall'amministrazione) e non protocollati ma comunque registrati nel sistema.

Il fascicolo nel sistema DocsPA è accessibile soltanto ad utenti dell'amministrazione titolare del procedimento.. L'accesso selettivo ai contenuti del fascicolo da parte di altri eventuali soggetti individuati dall'Amministrazione titolare può avvenire tramite interfacce specifiche, quali portali o altri sistemi, e può essere realizzato attraverso apposite API già offerte dal sistema o personalizzate *ad hoc* in funzione del tipo di accesso che deve essere consentito. I documenti aggregati nel fascicolo sono gestiti nella loro formazione, conservazione, trasmissione secondo quanto dettato dalle regole tecniche analizzate nel presente documento. (CAD Art.41 c.2-bis)

Ciascun fascicolo creato e gestito nel sistema è sempre riconducibile alla specifica amministrazione che lo ha creato e che ne cura la gestione, essendo possibile l'utilizzo del sistema solamente a seguito della configurazione di determinati parametri che individuano e descrivono l'ente utilizzatore e gli enti del

sistema. (CAD Art.41 c.2-ter lett.a) Ogni fascicolo creato nel sistema ha inoltre associati determinati metadati che ne costituiscono il "profilo standard", tra questi figurano come obbligatori l'oggetto del procedimento (espresso come descrizione del fascicolo), i dati identificativi del fascicolo (espresso come codice del fascicolo il cui formato è configurabile). Nel sistema DocsPA è possibile associare un fascicolo ad una tipologia documentale. Questo consente di assegnare al fascicolo ulteriori dati e tra questi quelli relativi alle amministrazioni partecipanti al procedimento (trattandosi di oggetto concepito come interno al sistema) e quelli relativi al responsabile del procedimento (che, a seconda delle regole organizzative dell'ente, potrebbe o meno coincidere con l'utente che forma il fascicolo nel sistema e di cui è tenuta traccia). In aggiunta ai metadati indicati, il fascicolo ha associati i documenti che ne fanno parte, visualizzabili come elenco di oggetti contenuti nel fascicolo e da qui direttamente accessibili (CAD Art.41 c.2-ter lett. b, c, d, e, e-bis).

I contenuti del fascicolo possono essere distribuiti in più sottofascicoli i quali possono a loro volta essere organizzati in una gerarchia a più livelli. La visibilità su tali sottofascicoli da parte degli utenti interni al sistema, ovvero appartenenti all'Amministrazione titolare del trattamento del fascicolo, segue quella del fascicolo padre. Tuttavia l'accesso selettivo ai contenuti del fascicolo da parte di altri eventuali soggetti individuati dall'Amministrazione titolare può avvenire tramite interfacce specifiche, quali portali o altri sistemi, e può essere realizzato attraverso apposite API già offerte dal sistema o personalizzate *ad hoc* in funzione del tipo di accesso che deve essere consentito. L'organizzazione dei contenuti in sottofascicoli, garantisce comunque che tutti i documenti di un dato procedimento, aggregati in un fascicolo, siano tra loro collegati grazie a tale aggregazione, accessibili a partire dal fascicolo stesso (CAD Art.41 c.2-quater).

I fascicoli fanno parte del sistema di gestione informatica dei documenti e contengono l' insieme minimo dei metadati indicato nel CAD Art.41 c.2-ter. La classificazione è determinata autonomamente dalle amministrazioni che definiscono adeguati piani per tutti i documenti, compresi quelli non soggetti a registrazioni di protocollo (DPCM 14 novembre 2014 Art.13 c.1).

Attraverso la gestione del fascicolo il sistema DocsPA permette di gestire eventuali aggregazioni documentali informatiche individuate da una chiave di aggregazione come richiesto nell'Art.13 c.2 del DPCM del 14 novembre 2014; ulteriori aggregazioni possono essere realizzate attraverso il salvataggio di ricerche documentali o attraverso particolari funzionalità.

2.5.2 Trasferimento in conservazione

Il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale può generare, in DOCSPA a fronte di opportune integrazioni con sistemi esterni di conservazione per uno o più fascicoli, un pacchetto di versamento che contiene i riferimenti che identificano univocamente i documenti informatici appartenenti al fascicolo con modalità differenti a seconda del servizio di conservazione con cui si integra (DPCM 14 novembre 2014 Art.15 c.1).

2.6 Registri e repertori informatici

2.6.1 Formazione dei registri e repertori informatici

I registri di protocollo e gli altri registri, i repertori, gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti realizzati dalle amministrazioni su supporto informatico in luogo dei registri cartacei sono formati da una generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica (Art.14 c.1 DPCM 14 novembre 2014). Per i repertori in particolare dipende dalla gestione degli enti.

Le pubbliche amministrazioni in DocsPA possono gestire registri particolari informatici, espressamente previsti da norme o regolamenti interni, generati dal concorso di più aree organizzative omogenee con le modalità previste ed espressamente descritte nel manuale di gestione, individuando un'area organizzativa omogenea responsabile (DPCM 14 novembre 2014 Art.14 c.2).

2.6.2 Trasferimento in conservazione dei registri e repertori informatici

Il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale può generare in DOCSPA a fronte di opportune integrazioni con sistemi esterni di conservazione, per uno o più registri o repertori informatici, un pacchetto di versamento che contenga i riferimenti che identificano univocamente i documenti informatici appartenenti all'aggregazione documentale informatica con modalità differenti a seconda del servizio di conservazione con cui si integra (DPCM 14 novembre 2014 Art.15 c.1). DocsPA infatti può facilmente integrarsi tramite WS con sistemi esterni di conservazione (già esistenti o sviluppati *ad hoc*) che gestiscono tale processo, oltre a disporre esso stesso di uno specifico modulo software già integrato per la gestione del processo di conservazione con opportune impostazioni.