community network
EMILIA-ROMAGNA

LINEE GUIDA
per la gestione dei flussi documentali

Parte 1-
Comunicazione Esterna

Versione 1.1
5 settembre 2011

Regione Emilia-Romagna

Tracking List

Versione	Data	Redatto da	Modifiche/Integrazioni	Validato da
1.0	10/06/11	Gabriele Bezzi	Giancarlo Covini	
01.01.00	05/09/11	Gabriele Bezzi		

Note

Il testo è stato redatto da Gabriele Bezzi con il contributo dei partecipanti alla Comunità tematica Gestione Documentale.

Abstract

I DESTINATARI delle informazioni e delle raccomandazioni qui contenute sono tutte le Amministrazioni locali della CNER, andando ad investire in primo luogo chi ha dirette responsabilità in materia di gestione documentale e de materializzazione dei procedimenti, ma che, attraverso questi, è auspicabile raggiunga e pervada l'intera struttura organizzativa di ogni Ente.

OBIETTIVO è quello di creare un circuito virtuoso che permetta a tutte le P.A.L. della CNER di muoversi in maniera condivisa, coordinata e con le stesse modalità operative sul tema della comunicazione digitale da e verso l'esterno degli Enti, contribuendo in questo modo alla semplificazione del lavoro del personale interno.

I CONTENTUTI del presente documento riguardano:

- Canali e strumenti di trasmissione dei documenti digitali
- Differenza tra validità del documento e modalità di trasmissione
- Integrazione tra sistemi di comunicazione e di gestione documentale
- Formati dei documenti da trasmettere e ricevere
- Utilizzo della firma elettroniche

Indice

Premessa

Con la redazione di linee guida sui sistemi documentali e sulle forme di comunicazione telematica ci si propone di offrire un documento sintetico di riferimento generale che fissi alcuni principi essenziali per la gestione dei flussi documentali relativi a documenti informatici, indicando da un lato specifici requisiti funzionali per la realizzazione di un corretto sistema di gestione documentale e dall'altro alcuni modelli comportamentali ritenuti *best practice* da proporre per una condivisione e per risolvere in modo univoco una serie di problemi.

Per affrontare questa complessa tematica si è previsto di suddividere le linee guida in due parti.

In questa prima parte ci si concentra sulle modalità di ricezione e spedizione dei documenti, in particolare dal punto di vista dell'interazione tra sistema di gestione documentale e sistemi di comunicazione telematica, riservando alla seconda parte lo sviluppo di linee guida per la circolazione interna dei documenti, la loro archiviazione e conservazione e le specifiche caratteristiche dei sistemi di protocollo all'interno del sistema di gestione documentale.

La comunicazione telematica e la gestione informatica dei documenti è una materia in costante evoluzione, sia sul piano tecnologico che giuridico-amministrativo ed anche di elaborazione di analisi archivistiche e standard internazionali.

La normativa italiana manca ancora di alcuni elementi quali l'aggiornamento delle regole tecniche, attualmente in corso di definizione. In particolare sono già state pubblicate nel sito di DigitPA le prime bozze delle regole tecniche sulla formazione del documento informatico, sui flussi documentali, sul sistema di conservazione sulla consultazione ed estrazione indirizzi PEC, sull'accesso ai dati della PA e sulle firme elettroniche (http://www.digitpa.gov.it/amministrazione_digitale).

Le indicazioni qui riportate potranno quindi essere integrate e aggiornate a seguito in particolare di modifiche normative.

1. Introduzione

L'elaborazione della prima parte delle i linee guida si è sviluppata da un modello di sintesi basato su alcune valutazioni elaborate e condivise all'interno della CT Documentale già nell'ottobre 2009[1].
In particolare punto di partenza e chiave di lettura centrale dell'analisi sono stati la definizione di due concetti fondamentali:

1. **Differenza tra validità del documento e modalità di trasmissione**
2. **Necessità di integrazione tra sistemi di comunicazione e sistemi di gestione documentale**

Si è inoltre valutato che le soluzioni non potevano essere soltanto di tipo tecnologico, ma dovevano coinvolgere fortemente aspetti organizzativi e di definizione di regole comportamentali coerenti all'interno degli enti.
Questi elementi di base da cui si era sviluppata la riflessione hanno trovato conforto e conferma nelle circolari emanate dal Ministro Brunetta nel corso del 2010[2], in particolare la necessità di collegamento tra le caselle di posta certificata e il sistema di protocollo, o più precisamente tra il "sistema di gestione della posta elettronica tipo PEC e quello di gestione del protocollo"[3]
Questa impostazione è stata autorevolmente e definitivamente stabilita dalle modifiche al CAD apportate dal D.Lgs 30 dicembre 2010, n. 235, in particolare all'articolo 40 bis del testo aggiornato del CAD (D.lgs. n. 82/2005) che recita:
" ***Formano comunque oggetto di registrazione di protocollo ai sensi dell'articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le comunicazioni che pervengono o sono inviate dalle caselle di posta elettronica di cui agli articoli 47, commi 1 e 3, 54, comma 2-ter e 57-bis, comma 1, nonché' le istanze e le dichiarazioni di cui all'articolo 65 in conformità' alle regole tecniche di cui all'articolo 71"***

Nel modello di sintesi iniziale di inquadramento generale il gruppo ha preso in considerazione gli aspetti organizzativi individuati soprattutto dal dpr 445/2000 a cornice dell'attuazione del processo di dematerializzazione e gestione del sistema documentale informatico vigenti già dal 1 gennaio 2004.
Si è dato quindi per acquisito l'iter che tutte le amministrazioni hanno percorso o che devono percorrere per rispondere ai requisiti organizzativi minimi necessari, prima di tutto, per l'attivazione dell'interoperabilità di protocollo e della possibilità di trasmissione e ricezione di documenti informatici, nel rispetto di regole generali da applicare e condividere per produrre e scambiare documenti informatici:

[1] Cfr. "Verbale 2 incontro sottogruppo 14 ottobre 2009 sezione sintesi linee guida"
[2] Circolari 18 febbraio 2010 n. 1/2010/DDI, 19 aprile 2010 n. 2/2010/DDI e 3 settembre 2010 n. 12/2010 del DFP
[3] Circolare 19 aprile 2010 n. 2/2010/DDI pag. 2. La circolare afferma che: "E' preferibile adottare prodotti di gestione del protocollo informatico predisposti per il trattamento dei messaggi e degli allegati veicolati via PEC o soluzioni in grado di "collegare" il sistema di gestione della posta elettronica di tipo PEC e quello di gestione del protocollo. (...) si raccomanda di adottare sistemi di gestione documentale che consentano la gestione integrata e la tenuta dei messaggi, degli allegati e delle ricevute nell'ambito della gestione del fascicolo informatico."

- individuazione dell'ambito organizzativo corrispondente all'Area Organizzativa Omogenea (AOO) (art. 50, comma 4 del dpr 445/2000);
- nomina del responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (ex art. 61, comma 2 del dpr445/2000);
- attivazione della casella di Posta elettronica istituzionale certificata (ex art. 15, comma 3 del dpcm 31/10/2000 e art. 47 comma 3 CAD);
- iscrizione all'Indice PA (IPA) (artt. 11 e seguenti Dpcm 31/10/2000)
- acquisizione e distribuzione del sistema di firma digitale presso i soggetti che internamente alle amministrazioni, abbiano potere di firma.

Elementi informativi utili per una migliore comprensione e applicazione di tali prerequisiti sono comunque illustrati nelle presenti linee guida.
Le linee guida, in questa prima parte, sono articolate in capitoli che illustrano le caratteristiche essenziali degli elementi fondamentali per la ricezione e spedizione di documenti informatici, in particolare:

- i sistemi di comunicazione telematica,
- la formazione del documento informatico, nei sui aspetti legati alla sua validità giuridica e alla conservazione,
- i sistemi di registrazione per l'acquisizione dei documenti informatici nel sistema di gestione documentale dell'ente.

Infine si propone un modello di gestione integrata sviluppato sulla base della normativa italiana e dei principi dell'archivistica corredato di tabelle riassuntive di possibili comportamenti operativi.

2. I Sistemi di comunicazione telematica

Il nuovo CAD prevede esplicitamente che le comunicazioni tra pubbliche amministrazioni e, in base alla nuova disposizione inserita con l'art. 5 bis, anche la comunicazione tra imprese e amministrazioni pubbliche relative alla presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti avvenga "esclusivamente" utilizzando le tecnologie dell'informazione e della comunicazione.
Gli strumenti di comunicazione possono essere molteplici, ma si possono distinguere sostanzialmente in diversi sistemi di posta elettronica o di sistemi più evoluti di comunicazione quali la cooperazione applicativa e le comunicazioni on-line effettuate utilizzando applicazioni web appositamente realizzate per lo scambio di informazioni dati e documenti, normalmente collegate a specifiche esigenze o tipi di procedimenti.

Posta elettronica semplice o ordinaria (PEO)

La posta elettronica è un servizio internet di comunicazione e scambio di messaggi di tipo asincrono; mittente e destinatario non devono necessariamente essere collegati contemporaneamente.

Il servizio prevede che un fornitore del servizio di posta elettronica (provider) metta a disposizione:

- dei server nei quali i messaggi inviati e ricevuti sono conservati,
- un'applicazione web tramite la quale l'utente gestisce la propria messaggistica in entrata e in uscita, o in alternativa un'applicazione client che possa essere installata su un PC. Gmail è un esempio di applicazione web, mentre Outlook è un esempio di applicazione client
- sui server del provider devono essere presenti il protocollo (insieme di regole, meccanismi tramite le quali si garantisce il funzionamento del software specifico) SMTP per la spedizione e il protocollo POP o IMAP per la ricezione.

Il provider rilascia a richiesta caselle di posta elettronica gestite tramite il software opportuno previa autenticazione dell'utente.

In generale il riconoscimento del soggetto richiedente é debole; vengono rilasciate una username e una password a fronte della compilazione di una form con alcuni dati anagrafici.

Il mittente di un messaggio di posta elettronica può richiedere, in modo opzionale e sul singolo messaggio, delle ricevute che confermino l'avvenuta consegna della mail spedita.

Gli standard su cui si basano i protocolli SMTP, POP e IMAP garantiscono l'interoperabilità tra i vari provider di posta elettronica. Utenti diversi che utilizzano sw di posta elettronica diversi possono cioè comunicare tra loro.

Questi sistemi di posta non danno nessuna garanzia legalmente riconosciuta di spedizione, consegna e ricezione dei messaggi, soprattutto se lo scambio di messaggi avviene tra provider diversi.

Un messaggio di posta elettronica è costituito da:

- una busta (envelope)
- una sezione di intestazioni (header)
- un corpo del messaggio (body)
- eventuali allegati.

Il formato dei messaggi di e-mail è basato su standard quali RFC 2822 e MIME, che stabiliscono quali informazioni devono e possono essere presenti, e come esse sono organizzate.

Esempio: messaggio in formato RFC 2822

```
Message-ID: <006401c91467$186fb1d0$6602a8c0>
From: "Silvio Salza" <salza@dis.uniroma1.it>
To: "Silvio Salza" <salza@dis.uniroma1.it>
Subject: Sample single part message
Date: Fri, 12 Sep 2008 01:35:37 +0200
@
Organization: =?iso-8859-1?Q?Universit=E0_di_Roma?=
MIME-Version: 1.0
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Message from the University of Rome
```

Messaggio dall'Universit=E0 di Roma

La visualizzazione dipende dai client di e-mail utilizzati, che, in genere, mostrano solo in minima parte le informazioni presenti nell'intestazione.
Le header lines sono una fonte essenziale di informazioni:
– Per la metadatazione del messaggio
– Per l'analisi di autenticità
– Per la corretta interpretazione del contenuto.
Grazie al meccanismo degli *allegati*, il messaggio di posta elettronica può avere una doppia valenza:
A. È un vettore che permette di fissare tempi e dettagli di spedizione e consegna dei documenti che vengono trasmessi come allegati
B. È un documento esso stesso, quando si considera l'informazione contenuta nel corpo del messaggio.
Si segnala infine che i sistemi di posta elettronica pongono limiti fisici di dimensioni dei documenti che possono essere allegati e spediti. Una mail che contiene allegati che superano il limite massimo consentito non viene consegnata al destinatario e il mittente dovrebbe ricevere un messaggio in tal senso dal provider. Il limite sulla dimensione del messaggio nel suo complesso o dei singoli allegati può variare da provider a provider, anche in relazione alle politiche di archiviazione dei messaggi. Ciò può creare problemi nell'invio di documenti amministrativi informatici di grosse dimensioni (ad es: allegati cartografici o immagini scansionate molto pesanti).

Posta Elettronica Certificata (PEC)

La PEC è un tipo particolare di posta elettronica. Anche la PEC é basata sui protocolli standard di comunicazione; SMTP, POP e IMAP.
L'aggettivo "Certificata", introdotto sostanzialmente dalla normativa Italiana, indica che con questo sistema, la comunicazione è garantita da parte del provider: sia per quanto riguarda il l'integrità e la provenienza del messaggio, sia per quanto riguarda le azioni di spedizione e consegna.
Nella normativa Italiana la PEC è equiparata alla notifica a mezzo posta (art. 48 del CAD), ma può anche essere assimilata alla tradizionale raccomandata con ricevuta di ritorno.
Le caselle di PEC vengono fornite da provider iscritti in una lista apposita, come fornitori del servizio di PEC, previa certificazione del servizio da parte del DigitPA.
Nella comunicazione tra due caselle di PEC la garanzia dell'avvenuta spedizione e ricezione e' fornita dalle ricevute di ACCETTAZIONE (rilasciata dal provider del mittente che attesta la presa in carico del messaggio) e di CONSEGNA (rilasciata dal provider ricevente che attesta la consegna del messaggio nella casella del destinatario).
Le ricevute di ACCETTAZIONE e CONSEGNA e la busta di trasporto del messaggio sono firmate digitalmente dal gestore del servizio e pertanto certificano l'integrità del messaggio consegnato, la data e l'ora di spedizione e di consegna.

Tutte le ricevute vengono fornite al mittente come messaggi nella casella di posta del mittente.
Il servizio di PEC fornisce anche, in caso di problemi, ricevute di MANCATA ACCETTAZIONE o di MANCATA CONSEGNA, nelle quali sono riportati i problemi riscontrati che hanno impedito l'accettazione o la consegna (ad es. dimensione eccessiva degli allegati, mancanza di collegamento con il provider ricevente, ecc.).
Nel caso in cui la comunicazione avvenga tra una casella di PEC e una casella di posta elettronica semplice, nell'insieme della comunicazione, viene a mancare la ricevuta di CONSEGNA rilasciata dal gestore della casella del destinatario, quindi manca la conferma legalmente valida di consegna.
I gestori del servizio di PEC mettono a disposizione delle applicazioni web tramite la quale gli utenti possono gestire i loro messaggi.
Le caselle di PEC sono rilasciate a richiesta, senza identificazione diretta del richiedente.
La caratteristica principale dei messaggi di PEC è che sono formati da un messaggio del gestore del sistema firmato digitalmente a cui è allegato l'intero messaggio inviato dal mittente.
Questo messaggio presente anche in forma di file xml, denominato daticert.xml, riporta la data e l'orario di trasmissione del messaggio stesso, che corrisponde a quello presente anche nella ricevuta di ACCETTAZIONE e rappresenta un riferimento temporale opponibile a terzi certificando l'orario esatto di spedizione del messaggio di PEC.

Esempio di messaggio di PEC
Messaggio di posta certificata
Il giorno 24/05/2011 alle ore 15:55:54 (+0200) il messaggio
"Messaggio di prova - All'attenzione di Gabriele Bezzi" e' stato inviato da
"peigiunta@postacert.regione.emilia-romagna.it"
indirizzato a:
PARer@postacert.regione.emilia-romagna.it "posta certificata"
Il messaggio originale è incluso in allegato.
Identificativo del messaggio: opec228.20110524155554.17364.04.1.2@pec.actalis.it

Comunicazione Elettronica Certificata tra Pubblica Amministrazione e Cittadino (CEC PAC)

Questo tipo di posta elettronica, la CEC PAC (istituita con DPCM 6 maggio 2009 in attuazione al DL n.185 del 29/11/2008), ha, tecnicamente, lo stesso tipo di funzionamento della PEC.
Ha la stessa valenza di raccomandata con ricevuta di ritorno.
Offre le stesse garanzie di trasmissione dei messaggi e integrità del messaggio stesso.
Viene rilasciata a privati cittadini e rappresentanti di imprese previo riconoscimento diretto del richiedente che effettua una prima richiesta via web, e conclude il rilascio della casella recandosi personalmente presso un ufficio Postale.
La CEC PAC ha delle limitazioni d'uso: da una casella CEC PAC e' possibile inviare messaggi solo ed esclusivamente a caselle PEC che siano presenti nell'Indice delle Pubbliche Amministrazioni. L'invio di messaggi;

- verso caselle PEC non presenti nell'IPA (ad esempio caselle PEC degli Ordini Professionali, delle Banche o di Enti pubblici che non hanno provveduto ad iscriversi all'IPA)

- caselle di posta elettronica semplice
- altre caselle CEC PAC

è inibito.

La richiesta e attivazione di una casella CEC PAC per un cittadino implica l'elezione della casella quale domicilio esclusivo presso il quale ricevere le comunicazioni da parte della PA.

L'elenco delle caselle CEC PAC sono raccolte in un indice simile a quello degli Enti pubblici, al quale per il momento si puo' accedere solo se in possesso di una casella presente nell'elenco.

Come previsto nel Codice dell'Amministrazione Digitale in vigore da gennaio 2011, DigitPA ha emanato e pubblicato le "Regole tecniche tecniche per la consultazione ed estrazione di indirizzi PEC ed elenchi di indirizzi PEC" di cui all'art. 6 comma 1-bis del CAD, cioè relativi ad indirizzi di cittadini (CEC-PAC) o di professionisti iscritti in albi o di imprese registrate nel registro delle imprese che risultano pubblicate dal 22 aprile 2011 nel sito di DigitPA[4].

Entro il mese di maggio i gestori dovrebbero comunicare le modalità di recupero delle informazioni, che sembrano però non permettere al momento l'estrazione automatica da parte di sistemi di protocollo degli indirizzi con relativi dati come per l'IPA.

Poiché le caselle di CEC PAC sono rilasciate a seguito dell'identificazione (e sottoscrizione autografa di un contratto cartaceo) del richiedente, l'invio di una istanza alla PA tramite una di queste caselle viene considerata valida anche in assenza di ulteriore sottoscrizioni o identificazioni purché l'identificazione del titolare sia attestata dal gestore del sistema nel messaggio o in un suo allegato[5].

Caselle istituzionali e diverse caselle PEC degli Enti

Nell'ambito delle Pubbliche Amministrazione la normativa vigente prevede che ogni Ente, per ogni AOO elegga una casella di PEC come istituzionale; cioè come canale privilegiato per la trasmissione e ricezione di documenti informatici tra amministrazioni e con l'utenza della PA. Come già ricordato tale obbligo era già definito nel DPCM 31 ottobre 2000 all'art. 15 comma 3 che prevedeva:

> *Ciascuna area organizzativa omogenea istituisce una casella di posta elettronica adibita alla protocollazione dei messaggi ricevuti. L'indirizzo di tale casella è riportato nell'indice delle amministrazioni pubbliche.*

Tale norma è stata ribadita dall'art. 47 comma 3 del CAD che recita:

> *Le pubbliche amministrazioni...provvedono ad istituire e pubblicare nell'Indice PA almeno una casella di posta certificata per ciascun registro di protocollo.*

[4] http://www.digitpa.gov.it/notizie/adottate-le-regole-tecniche-la-consultazione-ed-estrazione-di-indirizzi-pec-ed-elenchi-di-in

[5] Art. 65, comma c-bis) del CAD. La norma citata può riferirsi a qualsiasi casella di PEC.

Ai sensi delle definizioni dell'allegato A della Delibera AIPA 28/2001 per casella istituzionale si intende:

la casella di posta elettronica istituita da una AOO, attraverso la quale vengono ricevuti i messaggi protocollati (D.P.C.M. 31 ottobre 2000, articolo 15, comma 3)

Ovviamente, con il termine "protocollati" si intendono messaggi inviati da altri sistemi di protocollo che debbono essere sottoposti a registrazione di protocollo da parte dell'AOO ricevente.

Le stesse definizioni ci ricordano che una AOO (Area Organizzativa Omogenea) è un insieme definito di unità organizzative di una amministrazione, che usufruiscono, in modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali. In particolare, ciascuna AOO mette a disposizione delle unità organizzative clienti il servizio di protocollazione dei documenti in entrata ed in uscita, utilizzando una unica sequenza numerica, rinnovata ad ogni anno solare, propria alla AOO stessa.

La casella istituzionale é uno dei dati che ogni Ente deve fornire al DigitPA da inserire tra i dati dell'Amministrazione all'atto dell'iscrizione nell'Indice delle Pubbliche Amministrazioni (IPA: http://www.indicepa.gov.it).
DigitPA ha recentemente pubblicato una "Guida operativa delle nuove funzionalità dell'Indice delle Pubbliche Amministrazioni" (ver. 1.1 – 16 maggio 2011) scaricabile dalla pagina per le amministrazioni del sito citato.
Secondo tale documento le operazioni e le attività di gestione dell'IPA che vedono direttamente coinvolte le singole amministrazioni, sono le seguenti:

- accreditamento di una amministrazione, secondo l'art. 12 del DPCM 31/12/2000;
- aggiornamento delle informazioni da pubblicare relative all'amministrazione;
- raccolta ed inserimento delle informazioni da pubblicare riguardo alle Unità Organizzative (UO) e alle Aree Organizzative Omogenee (AOO);
- aggiornamento delle informazioni da pubblicare riguardo alle UO e alle AOO;
- rimozione di una amministrazione accreditata
- conservazione dei dati storici;
- consultazione.

La coerenza del processo di accreditamento di un'amministrazione presso l'IPA verrà invece garantita dal Responsabile dell'IPA (ruolo assegnato al DigitPA).
In precedenza CNIPA aveva emanato regole tecniche per consentire l'accesso ai dati dell'IPA da parte degli applicativi di protocollo o per eseguire, in alternativa, l'export periodico dei dati dell'IPA sui data base locali degli Enti.

Poiché lo scopo primario della casella PEC Istituzionale é la comunicazione digitale tra le PA o con cittadini e imprese che hanno dichiarato il proprio indirizzo di PEC , la casella é bene sia integrata con il sistema di protocollo che ne assume la gestione in entrata e in uscita, dei messaggi e delle ricevute. Tutti i messaggi in entrata o in uscita dalla casella istituzionale amministrativamente rilevanti, cioè non "spam" o materiali pubblicitari o inviti a manifestazioni, devono infatti essere

registrati al protocollo e le ricevute prodotte dalla spedizione di un messaggio devono essere collegate alla registrazione del documento che è stato spedito.
Ogni Ente iscritto all'IndicePA deve dichiarare all'atto dell'iscrizione una casella PEC istituzionale legata al registro di protocollo cioè per ciascuna Area Organizzativa Omogenea (AOO).
Ciascun Ente può attivare anche altre caselle PEC, che possono o meno essere dichiarate all'IndicePA; queste caselle NON sono definite Istituzionali, ma debbono ugualmente essere connesse al sistema di protocollo.
Può essere utile per un Ente disporre di caselle PEC diverse per gestire le comunicazioni relative ad alcuni procedimenti cruciali che prevedono lo scambio di comunicazioni con altri Enti Pubblici o con categorie di utenza ben definita e provvista a sua volta di caselle PEC, ma, come già ricordato, tutte le caselle di PEC di un Ente devono essere collegate al sistema di protocollo: questo garantisce una gestione semplificata dei messaggi in entrata e in uscita e sopratutto garantisce che tutti i documenti siano correttamente registrati al protocollo, ai sensi dell'art. 40 bis del CAD ed acquisiti dal sistema di gestione documentale.

Interoperabilità e Cooperazione applicativa[6]

Con i termini interoperabilità e cooperazione applicativa ci si riferisce ad una specifica capacità di due o più sistemi informativi connessi in rete di comunicare, affinché l'applicazione, operante in ciascun sistema, sia in grado di disporre automaticamente, per le proprie finalità applicative, dei dati che sono producibili e/o acquisibili solo attraverso il processo elaborativo delle applicazioni operanti negli altri sistemi informativi.
In particolare, l'interoperabilità attiene alla capacità di due o più sistemi informativi di scambiarsi informazioni e di attivare, a questo scopo, processi elaborativi nelle rispettive applicazioni.
Ciascun sistema informativo può differenziarsi dall'altro per le scelte implementative; linguaggio di programmazione e formato dei dati, ma grazie all'utilizzo di regole, di uno stesso formato di interscambio dei dati e tecniche di comunicazione condivise queste differenze non risultano rilevanti.
L'interoperabilità è quindi la capacità di un sistema o di un prodotto informatico di cooperare e di scambiare informazioni o servizi con altri sistemi o prodotti in maniera più o meno completa e priva di errori, con affidabilità e con ottimizzazione delle risorse.[7]
Obiettivo dell'interoperabilità è dunque facilitare l'interazione fra sistemi differenti, nonché lo scambio e il riutilizzo delle informazioni anche fra sistemi informativi non omogenei (sia per software che per hardware).
Si possono definire in particolare tre aspetti:

[6] In parte rielaborato dal sito: http://www.progettoicar.it/ViewDocument.aspx?catid=b83d99a9-b251-45fd-8308-7768cbc0d864&docid=a110281d-011b-404e-8b04-5772363c76d7

[7] Interoperability: "The ability of one application/system to communicate or work with another." *InterPARES 2 Glossary*

A. l'interoperabilità tecnica, concernente problemi tecnici di collegamento tra sistemi, la definizione delle interfacce, il formato dei dati e i protocolli, comprese le telecomunicazioni;

B. l'interoperabilità semantica, che assicura che il significato esatto delle informazioni scambiate sia comprensibile da qualsiasi altra applicazione, anche non pensata inizialmente per quel determinato scopo;

C. l'interoperabilità gestionale, che modella i processi di lavoro, allineando le architetture dell'informazione con gli obiettivi dell'organizzazione, e aiuta i processi di business nella cooperazione".

Per sviluppare funzioni di interoperabilità sono spesso utilizzate comunicazioni formattate secondo lo standard xml con tracciati noti sia al sistema mittente che al sistema ricevente.

Per Cooperazione Applicativa si intende l'erogazione di servizi informatici a valore aggiunto che utilizzano le funzioni di due o più applicazioni, progettate per erogare servizi singolarmente, appartenenti a sistemi informatici diversi afferenti allo stesso o a differenti Domini.

Esiste l'esigenza del coordinamento dei processi realizzati con il concorso di trattamenti distribuiti tra sistemi informatici di cui sono responsabili soggetti pubblici e privati, al fine di assecondare l'esecuzione di procedimenti amministrativi e la produzione di atti e provvedimenti amministrativi. Il coordinamento e la collaborazione di detti sistemi devono essere corredati dalla capacità di ispezionare in ogni momento lo stato di avanzamento (gli adempimenti amministrativi effettuati e quelli ancora da effettuare) dei processi applicativi e l'origine di ogni atto amministrativo effettuato nell'ambito del processo applicativo, al fine di realizzare concretamente la trasparenza dell'azione amministrativa nel doveroso rispetto delle norme sulla confidenzialità e riservatezza dei dati.

Nella cooperazione applicativa un'applicazione, nel corso del suo processo elaborativo, può far uso di una serie di informazioni elaborate da un'altra applicazione.

Ad esempio: un applicativo che rilascia certificati anagrafici, a cui si accede tramite un portale, tramite la cooperazione applicativa puo' richiedere la protocollazione automatica del certificato da rilasciare trasmettendo al sistema di protocollo i dati necessari per generare una registrazione, tramite un documento in formato xml, strutturato secondo regole concordate che entrambi i sistemi applicativi riconoscono. Il sistema di protocollo riceve il documento in formato xml ed esegue automaticamente il processo di registrazione estraendo i dati necessari dal documento xml ricevuto.

La "***cooperazione applicativa***" è anche espressamente definita all'art. 72 del CAD, nella sezione relativa al Sistema pubblico di connettività (SPC), come:

la parte del sistema pubblico di connettività finalizzata alla interazione tra sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi.

Lo stesso articolo specifica che all'interno del Sistema pubblico di connettività per "***interoperabilità di base***" si intendono:

i servizi per la realizzazione, gestione ed evoluzione di strumenti per lo scambio di documenti informatici fra le pubbliche amministrazioni e tra queste e i cittadini

mentre per ***"interoperabilità evoluta"*** si intendono:

i servizi idonei a favorire la circolazione, lo scambio di dati e informazioni, e l'erogazione fra le pubbliche amministrazioni e tra queste e i cittadini

Per le specifiche funzioni di interoperabilità tra sistemi di protocollo vedi capitolo 4.

Comunicazioni on line

Comunicazioni che avvengono utilizzando applicazioni web appositamente realizzate per lo scambio di informazioni dati e documenti.

Possono configurarsi come veri e propri servizi on-line realizzati dagli Enti per la gestione di specifici procedimenti (ad es. tabelle prezzi, iscrizioni nidi, AIA, ecc.)oppure applicazioni generiche per lo scambio di comunicazioni di varia natura: dalla richiesta di informazioni su eventi, procedimenti e attività' svolte dall'Ente, all'invio dei curricula e altri processi gestiti dall'Ente ma non strutturati.

Esempi di comunicazioni on line sono i servizi esposti dai portali degli Enti.

A questi servizi si accede previa richiesta di credenziali autorizzate dall'ente, tramite una richiesta on line oppure con riconoscimento diretto del soggetto richiedente, e successiva consegna diretta o invio di un supporto contenente le credenziali (smart card, CNS ...) o in busta chiusa con Userid e password o l'invio delle credenziali tramite posta elettronica.

Il sistema FedERa, ad esempio, consentirà agli utenti, con un'unica coppia di credenziale di autenticazione, e registrandosi una sola volta, di accedere a tutti i servizi on line messi a disposizione dai vari enti che aderiscono alla federazione. I cittadini possono perciò fare più cose con le stesse credenziali, e gli enti dal canto loro possono fornire servizi senza la necessità di registrare nuovamente gli utenti.

Le credenziali si potranno ottenere presso qualsiasi amministrazione che aderisce al sistema e quindi, in prospettiva, presso tutti gli enti pubblici dell'Emilia-Romagna.

I processi di registrazione permettono l'acquisizione, da parte del sistema, delle informazioni necessarie alla creazione delle identità digitali utilizzate dal sistema di autenticazione.

In base alla modalità con cui l'utente è identificato il sistema assegnerà uno dei seguenti livelli di affidabilità:

1. alta:

- identificazione "de visu";
- identificazione CIE/CNS;
- identificazione tramite documenti;
  - Registrazione tramite documentazione inviata tramite: fax, posta ordinaria, e-mail con documenti firmati digitalmente
  - Registrazione con autenticazione "indiretta" tramite raccomandata
- identificazione mediante verifica delle credenziali fiscali dell'utente

2. media

- identificazione indiretta tramite cellulare(SIM/USIM);

3. bassa

- utenti non identificati, richiede la sola iscrizione on-line.

Tramite le credenziali il soggetto accede al servizio che può consistere nella compilazione di metadati in una o più form e/o l'upload di documenti veri e propri; firmati digitalmente o meno.

Per sistemi di comunicazione basati su servizi on line la trasmissione dei documenti deve essere realizzata integrando il servizio esposto con il sistema di protocollo dell'ente che recepisce l'istanza inoltrata dal servizio, sviluppando appositi sistemi di interoperabilità.
L'integrazione può essere realizzata a vari livelli;

- tramite cooperazione applicativa; i due sistemi realizzano una comunicazione altamente automatizzata interloquendo tra di loro senza la necessità di alcun intervento umano, trasmettendo in modalità interoperabile tutti i dati necessari per la registrazione di protocollo e per il successivo trattamento dei documenti;
- realizzando componenti software (web services o procedure legate al data base quali store procedure e trigger) che eseguono in modalità automatica o semiautomatica le varie funzioni relative alla registrazione di protocollo. Questo tipo di implementazione realizza l'integrazione con il sistema di protocollo principalmente nella parte di gestione del back office del servizio;
- con un invio alla PEC istituzionale dell'ente; in questo caso l'intervento umano è necessario e l'integrazione viene ricondotta ad una normale comunicazione tramite PEC.

3. La formazione dei documenti

In questa sezione si esamineranno rapidamente alcune caratteristiche dei documenti, quali formati e firme elettroniche nella prospettiva di fornire indicazioni sul trattamento dei documenti ricevuti o da spedire.

La riforma del CAD rende il diritto soggettivo dell'utente all'utilizzo delle nuove tecnologie pieno, immediatamente esigibile ed azionabile davanti al giudice amministrativo. Pertanto ogni cittadino può presentare istanze e dichiarazioni in modalità telematica, mentre le pubbliche amministrazioni, comprese quelle locali hanno l'obbligo di formare gli originali dei documenti amministrativi in modalità esclusivamente informatica. Inoltre la riforma del CAD semplifica le condizioni di validità del documento informatico.

L'idoneità del documento informatico a soddisfare il requisito della forma scritta viene lasciata al libero apprezzamento del giudice sulla base delle caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando che i documenti informatici sottoscritti con firma elettronica avanzata, qualificata o digitale, formate nel rispetto delle regole tecniche da emanare entro il gennaio 2012 con apposito DPCM e che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità soddisfano il requisito della forma scritta e hanno l'efficacia probatoria della

scrittura privata. L'uso obbligatorio della firma elettronica qualificata o digitale per dare validità sostanziale e probatoria rimane solo per le scritture private di cui all'art. 1350 del Codice civile, ovvero i contratti in cui la forma scritta è prevista a pena nullità, quali ad esempio quelli aventi ad oggetto il trasferimenti di beni immobili[8].

Come già in precedenza, i documenti informatici senza alcuna firma elettronica, ai fini probatori hanno il valore delle riproduzioni meccaniche di cui all'articolo 2712 del Codice civile e, cioè, formano piena prova della rappresentazione dei fatti o delle cose in essi contenuti fino a disconoscimento da parte delle persone contro cui sono prodotte, mentre quelli con firma elettronica semplice sul piano probatorio sono liberamente valutabili in giudizio, tenuto conto delle loro caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.
Si ricorda che ai sensi del comma 2 dell'art. 68 del CAD le pubbliche amministrazioni nella predisposizione o nell'acquisizione di programmi informatici debbono adottare soluzioni informatiche che assicurino l'interoperabilità e la cooperazione applicativa e consentano la rappresentazione dei dati e documenti in più formati, di cui almeno uno di tipo aperto, salvo che ricorrano motivate ed eccezionali esigenze.
Per formato aperto, in base al comma 3 del citato articolo, si intende un formato reso pubblico e documentato esaustivamente.
DigitPA dovrebbe, in attuazione del comma 4 dello stesso articolo, realizzare ed aggiornare con cadenza almeno annuale un repertorio dei formati aperti utilizzabili nelle pubbliche amministrazioni e delle modalità di trasferimento dei formati.
Per una corretta formazione della versione definitiva e stabile di un documento bisognerebbe valutare i formati anche rispetto ad altre caratteristiche oltre a quella essenziale dell'apertura, in particolare per garantirne piena validità giuridica in caso di documenti firmati elettronicamente e migliori possibilità di conservazione a lungo termine[9].

Formati

In generale tutti i formati che rispondono alle seguenti caratteristiche possono essere considerati accettabili sia per quanto riguarda l'archivio corrente che per quanto riguarda la conservazione:

- aperti, documentati, non proprietari, trasparenti: si tratta di formati che sono standard "de jure" o standard "de facto", le cui specifiche siano comunque rese pubbliche. Il criterio di trasparenza implica anche una maggiore facilita' nella fruizione del documento tramite un maggior numero di sw anche con semplici funzioni di base (ad esempio un semplice editor di testo come Blocco note). Gli standard "de jure" sono preferibili agli standard "de facto";

[8] Art. 20 comma 1bis e art. 21 comma 2 e 2-bis del CAD. Le regole tecniche sono già in avanzata fase di redazione e una prima bozza è stata pubblicata nel sito di DigitPA (http://www.digitpa.gov.it/amministrazione_digitale: firme elettroniche - bozza regole tecniche)
[9] Per una trattazione più ampia si rimanda alla dispensa: *Requisiti e standard dei formati elettronici per la produzione di documenti informatici* **di Stefano Allegrezza,** Febbraio 2010, resa disponibile per cortesia dell'autore assieme a queste linee guida. Ora è disponibile anche un documento di DigitPA sui formati (allegato 2 alle regole tecniche: http://www.digitpa.gov.it/amministrazione_digitale), che contiene anche informazioni sui formati grafici vettoriali, in particolare sul formato SVG, derivato da XML ritenuto in alcuni paesi, come la Francia, adatto alla conservazione documentale.

nel primo caso un organismo internazionale ha certificato le specifiche del formato, ad esempio: il PDF e' ISO 32000, l' ODF e' ISO 26300;

- robusti; in caso di corruzione e' possibile comunque eseguire un recupero parziale e in ogni caso una minima perdita di bit non ne compromette la comprensione;
- stabili nel tempo; frequenza di modifiche nel tempo delle specifiche del formato, tali da garantire comunque compatibilità all'indietro (utilizzo del documento con versioni obsolete del sw utilizzato per generarlo) e in avanti (utilizzo del documento con versioni più' recenti del sw utilizzato per generarlo) senza sostanziale perdita di informazioni;
- diffusi; quanto piu' il sw che gestisce alcuni formati e' diffuso tanto più sarà stabile nel tempo il formato;
- auto-consistenti; contengono tutte le informazioni necessarie per essere visualizzati in modo corretto e completo;
- non modificabili; il documento non deve poter essere modificabile, almeno non facilmente;
- accessibili; possibilità di accesso alle informazioni del documento da parte di persone diversamente abili (il PDF prodotto tramite scansione non e' un documento accessibile, il PDF prodotto tramite conversione via sw e' un documento accessibile);
- assenza di protezioni; non siano presenti password o vincoli particolari collegati al documento

Tuttavia esiste un'altra serie di considerazioni che riduce ulteriormente il numero dei formati che possono essere considerati pienamente accettabili.

Nei documenti della famiglia MS-Office, in particolare Word (formato DOC) e della famiglia Open office (formato ODT) e' possibile inserire parti variabili (es: campi DATA che si autoaggiornano ogni volta che il documento viene aperto, macro o parti di codice eseguibile che fanno riferimento a banche dati che possono essere modificate o cessate nel tempo e comunque non più disponibili al momento dell'invio in conservazione), file audio e video. La presenza di informazioni che possono modificare il loro valore nel tempo può comprometterne la conservazione dal punto di vista informativo, sia a breve che a lungo termine: non garantiscono infatti l'immodificabilità del documento nel tempo.
Ricordiamo inoltre che ai sensi della attuale normativa il documento informatico non deve contenere macroistruzioni, riferimenti esterni, codici eseguibili od altri elementi tali da attivare funzionalità che possono modificarne il contenuto e che il documento informatico sottoscritto con firma digitale o altro tipo di firma qualificata[10] non ha l'efficacia prevista dall'articolo 2702 del codice civile, cioè della scrittura privata[11].

[10] Per estensione anche con firma elettronica avanzata introdotta dal nuovo CAD.
[11] Art. 3 comma 3 DPCM 30 marzo 2009:
Il documento informatico, sottoscritto con firma digitale o altro tipo di firma elettronica qualificata, non produce gli effetti di cui all'articolo 21, comma 2, del codice, se contiene macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati
Gli effetti di cui all'articolo 21, comma 2 sono appunto l'efficacia prevista dall'art,. 2702 del codice civile. Ricordiamo che ai sensi dell'art. 2702 ,"Efficacia della scrittura privata", la scrittura privata fa piena prova, fino a querela di falso della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta.

Questi formati inoltre possono presentare significative differenze formali nella presentazione del contenuto al momento della visualizzazione tramite sw o versioni diverse da quelle con cui sono stati prodotti e risultano molto facilmente modificabili al momento della visualizzazione e della memorizzazione. In alcuni casi la corretta presentazione è garantita solo dalla versione del sw con cui è stato prodotto, che, nel caso dei formati doc, non è liberamente disponibile. Potrebbero quindi creare problemi di visualizzazione e di apertura al momento del loro ricevimento da parte di altri.

D'altro canto questi formati rispondono sicuramente al criterio della diffusione.

Il nuovo formato di Word, DOCX, è un formato aperto perché la Microsoft ne ha reso pubbliche le specifiche (diventato nel 2008 standard "de jure"; UNI CEI ISO/IEC IS 29500:2008), tuttavia e' un formato ancora poco diffuso che necessita di un software specifico e a pagamento per poterlo visualizzare correttamente (MS-Office 2007). Stessa considerazione vale per tutti i formati della famiglia Office 2007. Questa famiglia di formati non risponde al momento al criterio dell'ampia diffusione, oltre ad avere gli stessi problemi citati per i formati DOC e ODT.

Oltre ai programmi specifici che consentono la visualizzazione del solo tipo di documento supportato, esistono nel web dei sw di visualizzazione generici (viewer), in grado di rendere leggibili diversi formati di file di testo.

Questi sw possono essere scaricati sul PC oppure utilizzabili direttamente dal browser (vedi ad esempio: http://guidami.blogspot.com/2010/12/aprire-online-documenti-microsoft.html e http://www.officeviewers.com/).

Un formato che risponde alle caratteristiche elencate all'inizio del paragrafo e' il formato XML, sviluppato dal consorzio W3C. E' il formato secondo il quale vengono generate dai sistemi di protocollo tutte le ricevute previste per l'interoperabilità: segnatura di protocollo, conferma di ricezione, eccezione, etc... .

Il formato XML, se non accompagnato da un foglio di stile tramite il quale e' possibile visualizzarne il contenuto in modo formattato (se al suo interno sono previste informazioni di formattazione), risulta un elenco di variabili e valori assegnati a queste variabili, risulta quindi molto utilizzato nello scambio di dati tra applicazioni e sistemi. Il file segnatura.xml che si scambiano i sistemi di protocollo interoperabili ne è un esempio: il file segnatura.xml contiene i dati della protocollazione in uscita dal mittente. Il file viene intercettato dal sistema di protocollo del destinatario e i dati presenti vengono utilizzati per precompilare la registrazione in entrata. Un altro esempio di documento informato XML è il tracciato dati che viene scambiato tra le applicazioni in una logica di cooperazione applicativa. Il registro di protocollo, è un ulteriore esempio di documento che può essere realizzato in formato XML.

La presenza di parti variabili può avere effetti negativi anche nella libera valutazione in giudizio dell'idoneità del documento informatico a soddisfare il requisito della forma scritta, ai sensi del comma 1-bis dell'art. 20 del CAD, che prevede che tale valutazione sia effettuata tenendo conto delle caratteristiche oggettive di qualità, sicurezza, integrità ed ***immodificabilità*** del documento informatico.

Ricordiamo che la nuova versione del CAD ha esteso l'efficacia prevista dall'articolo 2702 del codice civile anche ai documenti informatici sottoscritti con firma elettronica avanzata, (art. 21 comma 2) che, formati nel rispetto delle regole tecniche, garantiscano l'identificabilità dell'autore e l'integrità e l'immodificabilità del documento.

In effetti più che un formato propriamente detto XML (eXtensible Markup Language) è un linguaggio di marcatura: un documento XML è scritto in formato testo con tag (marcatori) anch'essi in formato testo, è quindi leggibile con semplici test editor come il Blocco Note o tramite un qualsiasi browser.
Si riportano brevi note, sicuramente non esaustive, relative a formati per immagini o di tipo audio e video.

Formati relativi a file contenenti immagini: TIFF, JPEG e GIF. I formati JPEG e GIF forniscono file di immagini compressi, producendo file di dimensioni ridotte rispetto al TIFF. A causa di questa compressione tuttavia risulta meno robusto del TIFF, cioè'; in caso corruzione del file l'immagine visualizzata risulta più degradata nel caso del formato JPEG che nel caso del formato TIFF. Il formato GIF fornisce immagini di bassa qualità perché supporta un numero inferiore di colori rispetto al JPEG.

Formati relativi a file di tipo audio e video. L'MP3 è il formato audio, basato sullo standard di compressione MPEG I; è quello che risponde al criterio di massima diffusione ma non a quello di robustezza. Il WAV, formato audio non compresso, risponde al criterio di diffusione e robustezza ma produce file di notevoli dimensioni.
Per i formati video le estensioni più diffuse sono: AVI, MP4, WMV.
Per le pubbliche Amministrazioni i formati audio e video possono essere considerati come una produzione numericamente marginale o di nicchia, rispetto alla maggiore quantità di documenti di testo, ma possono rivestire una notevole rilevanza nel caso in cui si stabilisca che la verbalizzazione ufficiale di sedute di organi collegiali possano essere rappresentate dalle registrazioni audio o video delle stesse[12].
Infine si segnala che i formati ZIP, RAR e 7-zip non sono formati di documenti, ma formati di contenitori di documenti, pertanto questi possono contenere documenti (anche strutturati in cartelle) in formati non accettati e questo non risulta immediatamente visibile al ricevente. In particolare se il file compresso e' a sua volta firmato digitalmente, la verifica della firma non consente l'immediata visualizzazione del contenuto informativo.

Conclusioni

Per gli usuali documenti testuali e in altri casi, quali disegni tecnici o riproduzione in immagine di documenti, attualmente il migliore e più semplice formato accettabile, sia per la gestione corrente che per la successiva conservazione, e' il PDF e PDF/A, che offrono anche le migliori garanzie di corretta visualizzazione al momento della loro apertura tramite sw liberamente disponibili.
Il secondo in particolare, specificamente definito per la conservazione (A indica appunto Archive o "Archiving")[13] presenta ottime caratteristiche in quanto auto-consistente e definito da uno

[12]Considerando le diverse definizioni di documento amministrativo succedutisi nel tempo dalla legge 241 del 1990 al DPR 445/2000, tali registrazioni debbono comunque considerarsi documenti amministrativi a pieno titolo.
[13]Standard ISO 19005-1:2005 "Document management – Electronic document file format for long-term preservation – Part. 1: Use of PDF 1.4 (PDF/A-1). Ora pubblicato anche il nuovo standard ISO 19005-2:2011: specifies the use of the Portable

standard internazionale, in particolare ha i font incorporati e non può contenere macroistruzioni, campi variabili o hyperlink attivi. Può essere facilmente prodotto a partire da Open Office, ma può presentare alcune limitazioni per la riproduzione ad esempio di slide, inoltre risulta complesso verificare che si tratti effettivamente di un PDF/A, conforme allo standard.

All'apertura di un documento PDF con Acrobat Reader 9 può apparire in automatico, ad inizio pagina, una barra blu con l'informativa "*il documento viene visualizzato in modalità PDF/A***"**.

Se non appare tale dicitura**,** certamente il formato del documento non è pienamente conforme allo standard PDF/A.

Se appare la dicitura indicata, il formato del documento potrebbe essere conforme allo standard PDF/A, ma la verifica effettiva si ottiene solo tramite prodotti specializzati. Si veda al riguardo il sito **www.pdfa.org** alla sezione "Validate PDF/A".

Tra i prodotti elencati si segnalano:

- Adobe Acrobat 9 Professional, che esegue la verifica di conformità del documento alle specifiche dello standard di formato ISO 19005 definite. La funzione di verifica viene attivata selezionando il link presente nella sezione "Informazioni PDF" del documento stesso. Il risultato della verifica viene fornito come "stato". Informazioni di dettaglio sul documento sono ottenibili quale risultato dell'analisi della funzione "Preflight".
- PdfaPilot di www.callassoftware.com, la cui versione server, per piattaforma Unix, è attualmente utilizzata dal servizio camerale di validazione formato PDF/A, messo a disposizione degli utenti Telemaco per la verifica puntuale (e non massiva) dei documenti in formato PDF/A1-b.

Lo standard PDF/A è suddiviso in due parti. Il PDF/A-1 , l'unico ad oggi approvato, è suddiviso a sua volta in due livelli:

- PDF/A-1a= massimo richiesto dallo standard
- PDF/A-1b= minimo richiesto dallo standard (incluso nel PDF/A-1a).

E' infine da sottolineare che la conversione in formato PDF di un documento, redatto e gestito fino al momento della sua stesura finale tramite un software specifico, quali quelli della suite di Office, o di OpenOffice, è ormai accessibile a tutti, in modalità semplice e gratuita, tramite software free (es: PDF Creator) o tramite i tool di conversione presenti nei menù sia di MS-Office che di Open Office.

Al loro interno le Amministrazioni possono quindi facilmente organizzarsi affinché la produzione dei documenti e la gestione documentale (interna e in uscita) sia basata essenzialmente sul formato PDF o meglio PDF/A.

Formati quali DOC, ODT e RTF possono essere ritenuti accettabili soprattutto perché rispondono al criterio della diffusione (soprattutto nel caso del DOC) e della apertura, ma dovrebbero essere

---

Document Format (PDF) 1.7, as formalized in ISO 32000-1, for preserving the static visual representation of page-based electronic documents over time. ISO 19005-2:2011 is not applicable to

- specific processes for converting paper or electronic documents to the PDF/A format,
- specific technical design, user interface, implementation, or operational details of rendering,
- specific physical methods of storing these documents, such as media and storage conditions,
- required computer hardware and/or operating systems.

limitati all'uso per scambio di modelli modificabili o di bozze di documenti da aggiornare e non per le versioni finali e stabili dei documenti stessi, magari firmati digitalmente. Inoltre ODT ha il vantaggio della gratuità del software che lo produce.
Formati quali quelli dei fogli di calcolo non dovrebbero essere accettati e soprattutto mai firmati elettronicamente, in quanto quasi certamente contengono macroistruzioni, codici eseguibili e possibili riferimenti esterni che possono alterare la rappresentazione dei dati contenuti; per questi formati, nel caso sia necessario trasmettere ad altri o ricevere da altri dati elaborati con fogli di calcolo dovrebbe essere chiesta/suggerita una preventiva conversione in PDF, per garantire la stabilità dei dati stessi e la possibilità di acquisirli come documento stabile e conservabile nel sistema di gestione documentale.
Nel caso di documenti strutturati o necessari per sviluppare funzioni di interoperabilità tra sistemi o per il trasferimento di dati sicuramente il formato attualmente preferibile è XML.
Il formato XML e' un formato pienamente accettabile.
Il formato immagine che offre migliori garanzie ai fini della conservazione e' il TIFF.
Formati audio e video potranno essere accettati se rispondenti alle caratteristiche elencate all'inizio del paragrafo, i formati più' diffusi di questa tipologia sono: MP3, AVI, WMV, MPEG-4.
I formati audio e video tuttavia sono in continua evoluzione; soprattutto i formati video.

Firme elettroniche

Il Codice dell'Amministrazione Digitale aggiornato prevede ora quattro tipologie di sottoscrizione per i documenti elettronici:

- firma elettronica
- firma elettronica avanzata
- firma qualificata
- firma digitale

La firma elettronica non prevede l'uso di un supporto sicuro o meno sul quale risiedono le credenziali della persona. Tipicamente consiste nel possesso di una coppia di chiavi, username e password, memorizzate su una banca dati (data base, LDAP, etc..), utilizzate per eseguire un'autenticazione debole.

La firma elettronica avanzata prevede l'uso di un dispositivo sul quale il proprietario ha “il controllo esclusivo” il quale e' stato rilasciato previa identificazione della persona. In questo modo i dati presenti sul dispositivo sono sempre riconducibili al firmatario. Non sono definite le specifiche del dispositivo che può essere, ad esempio; una smart card che contiene un certificato di sola autenticazione (cioè non qualificato) oppure i dispositivi elettronici (token) di tipo One Time Password dei servizi di Home Bancking, o ancora dispositivi basati sul riconoscimento dei dati biometrici della persona. In tutti gli esempi le credenziali e i dati anagrafici identificativi del proprietario/utilizzatore del dispositivo sono univocamente collegati alla persona tramite il dispositivo. Le nuove regole tecniche dovrebbero chiarire quali dispositivi possono essere

considerati generatori di firme elettroniche avanzate anche in riferimento alle modalità per consentire di rilevare se i dati ai quali la firma si riferisce siano stati successivamente modificati.

La firma elettronica qualificata prevede l'uso di un certificato qualificato (cioe' un certificato aderente alle specifiche dell'ETSI: European Telecomunication Stamdard Institute) presente su un dispositivo sicuro che lega direttamente il proprietario al certificato. Questo tipo di firma pur non specificando nessuna tecnologia particolare, ne' per il supporto ne' per il certificato, stabilisce che il processo di firma si basa su un certificato qualificato.

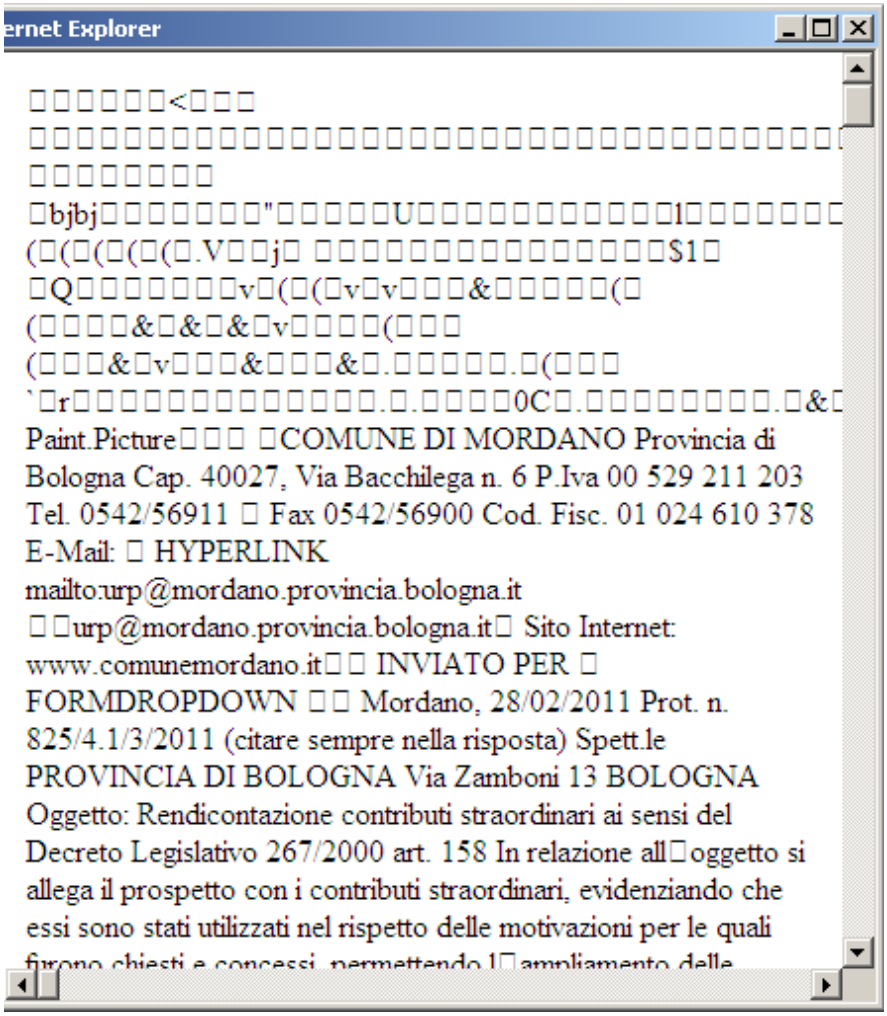
La firma digitale, nella nuova definizione del CAD prevede l'uso di un certificato qualificato ma non specifica l'uso di un dispositivo sicuro.
In questo caso viene specificato il tipo di tecnologia sulla quale si basa il processo di sottoscrizione; quella della coppia di chiavi asimmetriche o a chiave pubblica. Per garantire la titolarità del certificato e' stato stilato un elenco di certificatori accreditati presso il DigitPA. I Certificatori rilasciano certificati di firma, tipicamente su smart card, previo riconoscimento "de visu" del richiedente e sottoscrizione autografa di un contratto cartaceo secondo quanto previsto nel DPCM 30 marzo 2009. Si tratta di una firma elettronica avanzata basata su una specifica tecnologia formalizzata dalla normativa Italiana. Questo particolare tipo di firma garantisce: l'identità' del firmatario, quindi la provenienza del documento dal firmatario stesso e l'integrità del documento.
La normativa relativa alle modalità' di apposizione di una firma digitale a un documento elettronico e' stata modificata alla fine di luglio 2010. La Delibera 45 CNIPA del 21 maggio 2009 (e la Determinazione n. 69 DIGITPA del 28 luglio 2010 che ne modifica alcune parti) contiene il dettaglio delle modifiche approvate.
Tra le modifiche introdotte la determinazione prevede la sostituzione dell'algoritmo utilizzato per la generazione dell'impronta (digest) del documento che viene inclusa nella busta P7M nel processo di firma.
Prima di tale data l'algoritmo per il calcolo dell'hash utilizzato era SHA-1 (impronta a 160 bit), con la determinazione viene introdotto l'algoritmo SHA-256 (impronta a 256 bit).
Il nuovo tipo di firma è definito **CAdES**: formato di busta crittografica definito nella norma ETSI TS 101 733 V1.7.4 basata a sua volta sulle specifiche RFC 3852 e RFC 2634 e successive modificazioni
A fronte dell'aggiornamento delle regole tecniche i fornitori di certificati di firma hanno dovuto aggiornare i software per consentire l'uso dei certificati emessi secondo le nuove regole. Tuttavia i certificati emessi secondo le vecchi regole, non scaduti, non sono stati ritirati o sostituiti. Pertanto il sw deve garantire compatibilità sia con i certificati emessi prima di luglio 2010 sia con quelli emessi dopo luglio 2010.
Dalla pubblicazione sulla Gazzetta Ufficiale della Determinazione 69/2010 Infocamere (uno dei certificatori presenti nell'elenco di quelli accreditati presso DIGITPA) ha rilasciato diverse release della versione 4 dell'applicativo DIKE, per l'apposizione e la verifica di firme digitali, (la versione 3. non e' più supportata), fino ad arrivare alla versione 5.

Tutte le versioni 4. garantiscono la compatibilità con i certificati emessi prima di luglio 2010, sia per l'apposizione della firma che per la verifica. Questa versione del sw in tutte le sue release prevede l'aggiornamento automatico alla versione 5. previa conferma dell'utente.
L'adeguamento alle nuove regole tecniche sulla firma digitale deve essere fatto anche per gli applicativi di protocollo che per la verifica delle firme digitali utilizzano componenti realizzati ad hoc per lo scopo. Questi devono mantenere la compatibilità per la verifica di documenti firmati con certificati rilasciati prima dell'emanazione delle nuove regole tecniche.

La doppia estensione

I documenti firmati digitalmente tramite il sistema attualmente più diffuso hanno estensione P7M.
In generale hanno una doppia estensione; l'estensione P7M e' preceduta da quella relativa al formato del documento originale oggetto del processo di firma.
La maggior parte dei sistemi operativi e delle applicazioni si basa proprio sull'estensione del file per identificare l'applicazione utile alla sua visualizzazione, la mancanza della prima estensione in un file firmato può creare problemi.
L' applicativo DIKE, per l'apposizione e la verifica di firme digitali, realizzato da Infocamere, nel caso in cui la prima estensione del documento del quale si vuole verificare la firma risulti mancante, chiede all'utente di selezionare l'applicazione con la quale visualizzare il contenuto del documento.
La scelta, per l'utente, non e' semplice proprio perché la sintassi del nome del documento non da' indicazioni sull'applicazione da selezionare.
Situazioni ancora più complesse possono essere quelle degli applicativi protocollo che integrano moduli di verifica della firma e visualizzazione dei documenti il cui codice e' realizzato utilizzando librerie di vario genere; proprietarie del sistema operativo oppure dell'ambiente di sviluppo o ancora open source reperibili in rete. In fase di realizzazione questa situazione potrebbe non essere stata prevista.

E' buona norma quindi indicare sempre entrambe le estensioni del documento firmato digitalmente per non complicarne inutilmente la ricezione.
Di seguito e' mostrato il tentativo di apertura di un documento firmato digitalmente che ha la sola estensione P7M; manca cioè l'estensione relativa al documento originale (in questo caso PDF), tramite un generico viewer da un applicativo di Protocollo :



In questo caso il viewer utilizzato non supporta il formato del documento per cui il testo non e' visualizzato correttamente. Se il documento avesse avuto la corretta estensione l'applicativo avrebbe utilizzato il viewer adatto.

Vale la pena ricordare che esiste ed e' pienamente valida anche la firma con tecnologia PDF (Deliberazione DIGITPA 45/2009 art. 21 comma 15) definita **PAdES**: formato di busta crittografica definito nella norma ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modificazioni (standard del PDF).
In questo caso il documento avrà come unica estensione il PDF. Il documento originale può' ssere esclusivamente un PDF.
Il contenuto informativo del documento e' pienamente visibile tramite Acrobat Reader, ma per avere le necessarie informazioni sulla firma occorre installare Acrobat Reader 8.0 oppure 9.0 e un componente aggiuntivo; entrambi scaricabili gratuitamente dal sito di ADOBE.
La verifica di una firma eseguita con tecnologia PDF può essere eseguita anche tramite il software DIKE.

Per firmare digitalmente un documento con tecnologia PDF occorre acquistare Adobe Acrobat 9.0

Esiste un ulteriore processo particolare di firma per i file in formato XML (**XAdES**). Anche questo processo di firma e' pienamente valida (Deliberazione DIGITPA 45/2009 artt. 21 c. 16, 22, 23). Consente di firmare interi file o parti di questi. Un file firmato con tecnologia XML può essere visualizzato tramite un browser, ma le informazioni relative alla firma non risultano immediatamente leggibili, non viene eseguita la verifica e non ne viene data evidenza con un risultato. Per eseguire la verifica di una firma apposta con tecnologia XML può essere utilizzato il sw DIKE.

Conclusioni

Da quanto si è detto precedentemente si possono quindi evidenziare i seguenti elementi:

- verificare che tutti i documenti firmati, in uscita, mantengano la doppia estensione; del formato originale e il P7M assunto dopo il processo di firma-digitale. Richiedere che tutti i documenti firmati, esclusi quelli firmati con tecnologia PDF o XML che non assumono in nessun caso la seconda estensione, in entrata abbiano la doppia estensione nel nome del documento;
- verificare l'adeguamento alle nuove regole tecniche del sw di verifica della firma digitale integrato con gli applicativi, in particolare con l'applicativo di protocollo. In caso di esito negativo eseguire un' ulteriore verifica del documento tramite un sw esterno quale ad esempio DIKE;
- I documenti PDF firmati digitalmente possono essere visualizzati tramite Acrobat Reader (dalla versione 8. in poi), indipendentemente dal processo di firma utilizzato. La visualizzazione all'interno del Reader da' informazioni non attendibili e non complete sul processo di firma se il documento e' stato esplicitamente firmato con tecnologia PDF nel caso in cui non sia stato installato lo specifico add-on Acrobat. La visualizzazione di un documento firmato non con la tecnologia PDF (PKCS7 ora CAdES e' la tecnologia alternativa normalmente implementata dai certificatori accreditati) non da' alcuna informazione sul processo e la validità della firma.

4. La registrazione dei documenti

La registrazione è un modo per formalizzare l'acquisizione di un documento in un sistema documentale.
Tutti i documenti dai quali possano nascere diritti, doveri o legittime aspettative di terzi e tutti i documenti informatici vanno registrati.
La registrazione viene effettuata attraverso due modalità:

1. registrazione di protocollo
2. registrazione particolare.

I documenti ricevuti e spediti, indipendentemente dal supporto e dal mezzo di trasmissione, ad eccezione di quelli specificatamente indicati nell'art 53 comma 5 del DPR 445/2000, sono soggetti a registrazione obbligatoria di protocollo.
Anche delibere e determinazioni digitali, pur se sottoposte a registrazione su apposito registro, possono essere registrate nel registro di protocollo, in ottemperanza a quanto previsto dalla normativa vigente e in quanto tale registrazione in base alle attuali norme , per le sue caratteristiche, costituisce validazione temporale, in quanto la data di registrazione contenuta nelle segnatura di protocollo è un riferimento temporale opponibile a terzi.

Registrazione di protocollo

Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici[14].
Il protocollo è un sistema di certificazione e registrazione della corrispondenza attraverso il quale le amministrazioni pubbliche registrano soprattutto il transito dei documenti tra l'esterno e l'interno; è cioè lo strumento che rileva lo scambio di un documento tra due sistemi documentali inserendo al contempo il documento nel sistema documentale ricevente tramite una registrazione, cioè l'atto di assegnazione di una identificazione univoca, rappresentata da una numerazione sequenziale collegata alla memorizzazione di informazioni descrittive del documento (profilo, metadati) che lo identificano in modo univoco[15].

---

[14] La natura giuridica di atto pubblico del registro di protocollo è stata affermata dalla giurisprudenza con numerose sentenze anche della Corte suprema di Cassazione, ad es.. terza Sezione penale, n. 1571 del 23 maggio 1966, che ha stabilito che il registro di protocollo è un "atto pubblico originario, che fa fede della tempestività del ricevimento e della spedizione di un atto del privato o della pubblica amministrazione, indipendentemente dalla regolarità dell'atto stesso", ma anche Cassazione penale sez. V 6 ottobre 1987 oppure Consiglio di Stato , 1993, I, 838.

[15] Le informazioni obbligatorie della registrazione di protocollo sono definite dall'art. 53 comma 1del DPR 445/2000 e sono le seguenti:

- data di registrazione, assegnata automaticamente dal sistema
- numero di protocollo, generato automaticamente dal sistema
- mittente per il documento in arrivo / destinatario per il documento in uscita
- oggetto del documento

L'effettuazione di una registrazione di protocollo ha una funzione giuridica in termini di attestazione della produzione/ricezione e dell'autenticità del documento e corrisponde alla assunzione di alcune responsabilità da parte delle amministrazioni:

• *per i documenti ricevuti* certifica l'ingresso del documento nel sistema documentale a partire da una certa data e ne sottintende il suo trattamento, ma non ne garantisce la regolarità e la piena validità ai fini procedimentali. Questo significa che, nel caso di documenti ricevuti, l'amministrazione non può negare, a fronte della richiesta di esibizione del contenuto di una registrazione, che il documento sia esistito, ma può comunque valutare che il documento ricevuto non sia idoneo a produrre ulteriori effetti;

• *per i documenti prodotti* la stessa amministrazione può provare che un suo documento è stato registrato e, nel caso di spedizione automatica anche spedito ad una certa data. Questa stessa data costituisce, come è ovvio, anche il termine cronologico di riferimento per la formazione del documento stesso.

Il ruolo della registrazione di protocollo è stato enormemente enfatizzato dalla entrata in vigore della normativa sul procedimento amministrativo (l. 241/1990) che obbliga le amministrazioni ad esplicitare la tempistica delle fasi e delle attività amministrative in relazione ai vari procedimenti, stabilendo in primo luogo la data di avvio e il recepimento dell'istanza.

Il quadro normativo, che prevede che dal 1 gennaio 2004 l'unica registrazione di protocollo giuridicamente rilevante sia quella effettuata da un sistema informatico nel rispetto delle norme del DPR 445/2000, colloca il sistema di protocollo informatico in stretta relazione con altri sistemi quali:

- Sistemi di gestione documentale
- Sistemi per l'archiviazione e la conservazione dei documenti
- Sistemi di workflow per l'esecuzione automatica e il tracciamento dei flussi di lavoro (processi)
- Sistemi di posta elettronica e per la gestione della firma elettronica dei documenti.

Il protocollo classico (sistema di registrazione e certificazione della corrispondenza) va visto pertanto in stretta connessione con tutte quelle soluzioni tese al superamento del tradizionale scambio di informazioni cartacee e più in generale finalizzate alla trasparenza dell'azione amministrativa e all'automazione dei processi.

Nella seconda parte delle linee guida verranno esaminati più in dettaglio le caratteristiche dei sistemi di registrazione di protocollo con particolare riferimento alle loro funzioni in rapporto alla circolazione interna dei documenti e ai sistemi di gestione, archiviazione e conservazione.

Segnatura di protocollo

Contemporaneamente alla operazione di registrazione di protocollo va effettuata l'operazione di segnatura di protocollo che consiste nell'apposizione o associazione all'originale del documento,

---

- data e numero del protocollo del documento ricevuto, se disponibili
- impronta del documento informatico generata impiegando la funzione di HASH (sequenza di bit che identificano in maniera univoca il documento)

in forma permanente e non modificabile delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile, collegandolo alla sua registrazione.
La segnatura deve contenere obbligatoriamente il numero progressivo e la data di protocollo e l'identificazione in forma sintetica dell'amministrazione o dell'AOO.[16]
Può inoltre includere, qualora tali informazioni siano disponibili al momento della registrazione di protocollo, un codice identificativo dell'ufficio che ha prodotto il documento o a cui il documento è stato assegnato, l'indice di classificazione, l'identificazione del fascicolo di appartenenza e ogni altra informazione utile o necessaria per una corretta gestione del documento stesso.
Nel caso di un documento trasmesso con strumenti informatici, la segnatura di protocollo che deve essere associata al documento stesso può includere tutte le informazioni di registrazione del documento. L'Amministrazione che riceve il documento informatico dotato di segnatura di protocollo può utilizzare tali informazioni per automatizzare le operazioni di registrazione di protocollo del documento ricevuto mediante le funzioni di interoperabilità
Tutti i documenti informatici devono avere quindi un file di segnatura, costruito secondo le modalità previste dalla normativa, che dovrà essere sottoposto, insieme al documento, al processo di conservazione.
Nella segnatura o in lettere di trasmissione potrebbero essere inseriti anche elementi di controllo, quali l'impronta, sugli allegati informatici. In particolare già nella circolare AIPA n. 28 del 7 maggio 2001era prevista la possibilità di inviare all'interno della segnatura di protocollo anche l'impronta di documenti informatici che ad esempio per motivi di eccessiva dimensione non possono essere inviati telematicamente, ma esclusivamente su supporto fisico (ad esempio CD o DVD)come riferimento per consentire la verifica dei documenti messi a disposizione del destinatario esternamente al messaggio spedito e registrato al protocollo.

Interoperabilità e segnatura informatica di protocollo

L'interoperabilità di protocollo è finalizzata ad offrire un servizio di certificazione relativo alla ricezione e al trattamento al protocollo di documenti scambiati tra due pubbliche amministrazioni, in realtà due Aree Organizzative Omogenee (AOO). In questo modo due sistemi di protocollo informatico possono trattare in maniera automatica l'uno le informazioni trasmesse dall'altro, consentendo quindi lo scambio di documenti digitali tra amministrazioni e permettendone in certi casi la protocollazione automatica.
L'interoperabilità infatti, come già ricordato è la capacità di un sistema o di un prodotto informatico di cooperare e di scambiare, con affidabilità, informazioni o servizi con altri sistemi o prodotti. Obiettivo dell'interoperabilità è dunque facilitare l'interazione fra sistemi differenti, nonché lo scambio e il riutilizzo delle informazioni anche fra sistemi informativi non omogenei dal punto di vista tecnologico, evidenziando tra questi un elevato grado di sinergia.
Si definisce interoperabilità la capacità di un sistema informatico di interagire con altri sistemi informatici, in uno stesso ambito, in modalità automatica o semi-automatica.

[16] ART. 55 del DPR 445/2000, che descrive compiutamente la operazione di segnatura di protocollo.

Nel caso dei sistemi di protocollo informatico l'interoperabilità e' realizzata tramite lo scambio di informazioni utilizzando una messaggistica basata sul formato XML.
La circolare AIPA n. 28 del 7 maggio 2001, definisce le regole tecniche secondo le quali costruire la messaggistica xml per l'interoperabilità dei sistemi di protocollo della pubblica amministrazione.
Il mezzo di trasporto previsto per lo scambio della messaggistica di interoperabilità tra i sistemi di protocollo e' la posta elettronica, in particolare la casella di posta elettronica istituzionale certificata, ma possono essere utilizzati anche sistemi di cooperazione applicativa e comunicaioni on-line
Per rendere note soprattutto ai sistemi di protocollo gli elementi informativi identificativi delle PA viene istituito un Indice delle Pubbliche Amministrazioni (IPA) che contiene tutte le PA con alcuni **dati necessari** al funzionamento del paradigma dell'interoperabilità**'**, più altri descrittivi della struttura dell'Ente stesso:

- **all'atto dell'iscrizione ad ogni ente viene rilasciato un codice Ente univoco**
- **ogni ente deve dichiarare almeno un'Area Organizzativa Omogenea; AOO**
- **a ciascuna AOO deve corrispondere un indirizzo di PEC**
- deve essere dichiarato il responsabile di ciascuna AOO
- può essere indicata la struttura organizzativa dell'ente
- possono essere dichiarate ulteriori caselle di PEC riferite a particolari strutture organizzative

I dati dichiarati dagli Enti al momento della richiesta di inserimento nell'indice sono resi pubblici, per la loro consultazione, tramite protocollo LDAP (DPCM 31 ottobre 2000, Articoli; 11, 12, 13 e 14).
Per l'iscrizione dell'Ente nell'indice consultare il sito:
http://www.indicepa.gov.it/pla-comepubblicare.php

Il paradigma dell'interoperabilità deve essere implementato nei sistemi di protocollo, che devono essere in grado di generare la corretta messaggistica xml in caso di protocollo in uscita ed essere in grado di interpretare quella in entrata.
A fronte di una protocollazione in uscita il sistema mittente compone una mail che comprende:

- un documento principale di norma firmato digitalmente
- un numero qualsiasi di documenti allegati
- un file denominato Segnatura.xml che contiene i dati relativi alla registrazione di protocollo.

Nel file denominato Segnatura.xml sono incluse;

- informazioni di tipo archivistico alcune delle quali obbligatorie; numero e data della registrazione al protocollo del mittente, codici identificativi dell'amministrazione mittente e indirizzo PEC. Altre informazioni quali ad esempio titolario e fascicolo sono opzionali
- informazioni relative alla struttura del messaggio; distinzione tra documento principale e relativi allegati, richiesta di una conferma di protocollazione avvenuta
- informazioni utili al sistema ricevente per il trattamento del documento; tipo di procedimento a cui si riferisce, struttura dell'amministrazione ricevente a cui va inoltrato.

La struttura del file segnatura.xml e' definita nel documento di riferimento segnatura.dtd.

In questo documento sono indicati:

- i tipi di dati (numerici o alfanumerici ed eventuali dimensioni),
- la loro molteplicità (in segnatura.xml può essere presente; nessuno, uno o molti dati dello stesso tipo),
- se sono opzionali o obbligatori,
- la posizione all'interno di segnatura.xml in cui ciascun dato deve essere inserito (struttura a sezioni del file),
- la struttura delle singole sezioni e quali di queste sono obbligatorie, quali opzionali.

Il file segnatura.xml e' il componente fondamentale dell'interoperabilità'; in base alla completezza dei dati in esso contenuti il sistema di protocollo ricevente e' in grado di automatizzare la registrazione in entrata del messaggio ricevuto.

L'interoperabilità prevede la possibilità che le amministrazioni si scambino altri messaggi in formato xml.

Se richiesto dal sistema mittente, il sistema del destinatario deve generare e inviare un messaggio contenente un file xml denominato **Conferma.xml** che contiene i dati relativi alla registrazione in entrata del messaggio ricevuto.

Una volta registrato in entrata il documento viene inoltrato all'ufficio specifico per il suo trattamento nell'ambito di un procedimento. La trasmissione del documento ad un ufficio specifico può far si che il sistema di protocollo generi un ulteriore messaggio, denominato **Aggiornamento.xml**, che contiene informazioni circa lo smistamento all'ufficio competente.

Nel caso in cui, in un secondo momento sia necessario annullare la registrazione al protocollo di un documento in entrata, il sistema di protocollo può generare un messaggio denominato **Annullamento.xml**, questo contiene il numero di protocollo annullato con la motivazione dell'annullamento.

Nel caso in cui il destinatario del documento abbia dei problemi nella protocollazione in entrata: la segnatura.xml non e' conforme o non correttamente generata, i documenti allegati risultano corrotti, il sistema informatico ricevente può generare un messaggio in cui viene rilevata l'eccezione riscontrata (**Eccezione.xml**).

La generazione e invio di questa messaggistica xml e' generalmente implementata nei sistemi di protocollo come un automatismo; a fronte di uno specifico evento che si verifica nella gestione di un documento viene inviato uno di questi messaggi.

Nel caso del messaggio **Eccezione.xml** può essere utile lasciare un margine di valutazione all'operatore nella compilazione della motivazione e nell'invio del messaggio.

E' infatti possibile prevedere un numero limitato di eventi a fronte dei quali il sistema genera e invia un messaggio di eccezione automaticamente, ma le situazioni reali, di fronte alle quali l'operatore può decidere di rifiutare la registrazione di un documento in entrata, possono risultare molte di più' e molto più varie di quanto previsto.

La struttura di questi messaggi xml e' definita nel documento Segnatura.dtd come quella del file Segnatura.xml.

I nomi dei file xml previsti dall'interoperabilità sono nomi riservati, cioè da considerarsi fissi e non modificabili.

L'interoperabilità cosi' descritta può essere pienamente realizzata esclusivamente tra le PA che adottano sistemi di registrazione di protocollo.
Nelle comunicazioni digitali tra PA e privati (cittadini e imprese), anche quando queste avvengono tramite i sistemi di PEC della PA e un sistema di posta elettronica (anche nel caso in cui si tratti di CEC-PAC o PEC) del privato, i principi dell'interoperabilità non potranno essere completamente soddisfatti.
E' bene, tuttavia, che la PA inserisca sempre il file Segnatura.xml nelle comunicazioni in uscita verso i privati poiché questo risulta l'unico modo giuridicamente valido per il ricevente di accedere a dati quali; il numero progressivo del registro di protocollo, data di registrazione e i dati relativi alla PA mittente. Dati che spesso gli viene chiesto di citare nelle successive comunicazioni.
E' bene comunque che tali informazioni vengano anche riportate nel corpo del messaggio di posta elettronica con cui il documento viene spedito, utilizzando anche testi predisposti automaticamente dal sistema di protocollo.
Qualsiasi sistema di comunicazione utilizzato deve garantire la corretta formazione e trasmissione del file segnatura.xml, eventualmente opportunamente adattato per acquisire i dati dei cittadini o delle imprese come mittenti (es. SegnaturaCittadino.xml del progetto Docarea) e la corretta formazione dei documenti con formati idonei.

5. Integrazione tra sistemi di comunicazione e sistemi di protocollo

L'introduzione dei documenti informatici richiede non solo la capacità di produrli tramite sistemi di *office automation* in formati idonei e sottoscriverli se necessario con firma elettronica, avanzata, digitale o qualificata, ma anche la capacità di riceverli e trasmetterli attraverso un servizio di posta elettronica certificata o un canale web, registrandoli opportunamente, archiviandoli e rendendoli disponibili agli uffici cui compete la trattazione, governando i flussi documentali e garantendo l'affidabilità, l'integrità e l'autenticità.

Per eseguire queste operazioni è necessaria una stretta integrazione funzionale tra sistemi di comunicazione e sistemi di protocollo che stabilisca un collegamento per trasferire automaticamente dai sistemi di trasmissione ai sistemi di registrazione i documenti ricevuti o viceversa per quelli da trasmettere. Tale integrazione permette quindi di utilizzare a pieno le funzioni di interoperabilità.

Numerosi e importanti sono i vantaggi dell'integrazione:

- consentire la registrazione con la maggior quantità di dati (elementi) già forniti dal mittente (o da fornire al destinatario se altra PA) semplificando così le operazioni di registrazione
- evitare ogni possibile dispersione dei documenti: l'acquisizione diretta e automatica o semi automatica sul sistema di gestione dei documenti dei messaggi ricevuti attraverso gli indirizzi di PEC evita ogni possibile dispersione dei documenti negli hd dei singoli utenti che abbiano accesso a queste caselle o la necessità di conservare i documenti all'interno dei

server delle caselle di PEC e obbliga alla loro archiviazione nel sistema di gestione documentale dell'ente al momento della registrazione permettendo poi la trattazione da parte degli uffici competenti.

- La capacità del sistema di gestione documentale e in particolare del sistema di protocollo informatico di formare automaticamente i messaggi di pec in uscita direttamente e immediatamente a seguito della registrazione permette di decentrare la protocollazione e spedizione di documenti informatici nelle unità che li producono senza essere costretti ad attivare per ognuna di esse una casella di pec.
- Per trasmettere un documento informatico ad un soggetto esterno si dovrà semplicemente eseguire le operazioni di registrazione di protocollo in uscita, comprensive delle indicazioni di classificazione e fascicolazione, acquisendo i documenti informatici nel sistema di gestione dei documenti ed effettuando dallo stesso sistema di protocollo al termine della fase di registrazione anche la spedizione in modo automatico o semi automatico all'indirizzo elettronico del destinatario, noto al sistema e inserito già tra i dati di registrazione.

Il protocollo deve prevedere l'integrazione funzionale con il sistema di posta elettronica certificata, utilizzando apposite librerie per integrare le funzionalità dei protocolli SMTP e POP o IMAP a seconda che il messaggio sia in entrata o in uscita, per poter accedere sia in ricezione che in spedizione alla casella di posta certificata istituzionale ed eventualmente ad altre caselle di posta certificata che saranno definite per i vari settori dell'Ente.

Si intende in tal modo, permettere l'accesso alle caselle di posta certificata solo dall'applicazione protocollo per evitare che queste diventino l'equivalente di caselle "normali" e quindi utilizzate per messaggi non istituzionali.

Il sistema di registrazione di protocollo integrato ed interoperabile con il sistema di posta certificata deve prevedere le seguenti funzionalità:

- il sistema di posta certificata invia/rende disponibili i documenti giunti attraverso le caselle di posta certificata al sistema di protocollo
- il sistema di gestione informatica dei documenti comunica verso l'esterno dell'ente avvalendosi del servizio di posta certificata, generando messaggi da quest'ultimo interpretabili e conformi a quanto stabilito dalla normativa vigente in tema di interoperabilità dei sistemi di protocollo
- il sistema di protocollo prevede l'associazione automatica alla registrazione del protocollo relativa al documento spedito delle ricevute del sistema di posta certificata
- per quanto riguarda i vari messaggi generati dal mail server di posta certificata (ricezione, consegna, anomalia di trasporto, etc.), tutti sottoscritti digitalmente dal server, devono essere collegati al documento spedito, ma non necessariamente protocollati.

Il sistema di protocollo deve essere in grado di riconoscere automaticamente i messaggi di interoperabilità di ritorno in entrata, collegandoli alla registrazione di protocollo di partenza.

Ad ogni messaggio di posta elettronica ricevuto da una area organizzativa omogenea corrisponde una unica operazione di registrazione di protocollo. La registrazione si può riferire sia al corpo del messaggio sia uno o più file ad esso allegati[17].

Tra i dati relativi alla segnatura ed alla registrazione di protocollo del documento principale, va inserito il numero e la descrizione degli allegati.

Dai messaggi di posta elettronica certificata in entrata debbono essere recuperati ed inseriti nel sistema di gestione documentale tramite la registrazione di protocollo il maggior numero di informazioni e nella forma più completa possibile. In particolare vanno acquisiti i messaggi e-mail in un formato che mantenga le informazioni dell'intestazione (header)[18] e il messaggio firmato di posta elettronica certificata (daticert.xml) oltre ovviamente il messaggio e i documenti trasmessi dal mittente.

Il sistema di interoperabilità (messaggistica di eccezione e conferma) ove possibile dovrebbe essere sviluppato al massimo anche nei confronti delle imprese e dei cittadini, definendo una serie di messaggi che possano informare il mittente della avvenuta registrazione di protocollo oppure dei problemi del suo messaggio, quali ad esempio problemi di lettura del documento inviato (formato illeggibile o documento corrotto), eventuali problemi di verifica firma, ecc.

Come già sottolineato è bene che la PA inserisca sempre il file Segnatura.xml nelle comunicazioni in uscita verso i privati poiché questo risulta l'unico modo giuridicamente valido per il ricevente di accedere a dati quali; il numero progressivo del registro di protocollo, data di registrazione e i dati relativi alla PA mittente. Dati che spesso gli viene chiesto di citare nelle successive comunicazioni.

E' bene comunque che tali informazioni vengano anche riportate nel corpo del messaggio di posta elettronica con cui il documento viene spedito, utilizzando anche testi predisposti automaticamente dal sistema di protocollo.

Qualsiasi sistema di comunicazione utilizzato deve comunque garantire la corretta formazione e trasmissione del file segnatura.xml, eventualmente opportunamente adattato per acquisire i dati dei cittadini o delle imprese come mittenti (es. SegnaturaCittadino.xml del progetto Docarea) e la corretta formazione dei documenti con formati idonei.

Si evidenzia infatti la necessità di informare e "istruire" gli utenti esterni dell'Ente, in particolare sui formati accettati per i documenti in ingresso dandone evidenza sul sito dell'Ente con una pagina informativa generale collegata, ad esempio, all'indirizzo di posta certificata istituzionale, dando istruzioni dettagliate sull'uso corretto della stessa: "come fare" per spedire un documento alla PA: spedizione via MAIL (PEC), caselle a cui scrivere, formati da usare, modelli da recuperare, tipi di firma e loro spiegazione (vedi esempi allegati).

E' necessario:

- inserire l'informazione sui formati accettati dall'Ente nelle pagine relative ai procedimenti amministrativi e nei bandi di concorso.

---

17 DPCM 31/10/2000 Art.15 comma 2

18 Anche lo standard europeo MOREQ2 prevede tale raccomandazione al primo punto della gestione delle e-Mail (punto 6.3.1) pag. 73

- Inserire nelle pagine informative link tramite i quali gli utenti possono scaricare sw open source per eseguire la conversione in formato PDF dei documenti che devono inviare (es: http://www.pdfforge.org/pdfcreator).

Inoltre bisogna definire un apparato regolamentare: regolamenti, bandi, manuale di gestione, pubblicati ed eventualmente sintetizzati in forme chiare e comprensibili e facilmente visibili nei siti istituzionali, che specifichi e chiarisca le procedure di trasmissione e ricezione di documenti informatici.

Sarebbe necessario anche sviluppare sistemi che compilino in automatico messaggi informativi in fase di spedizione dei documenti o notifiche di eventuali errori o problemi in fase di ricezione dei documenti, con informazioni su come risolverli (ad es. documento in formato illeggibile, si prega di rinviare il documento in formato .pdf; il messaggio è giunto corrotto si prega di rinviarlo).

E' bene ricordare, sia nella composizione di una mail in uscita che nelle istruzioni per l'invio di documenti alla PA, i limiti sulle dimensioni dei documenti allegati posti dai sistemi di posta elettronica sia ordinaria che, soprattutto, certificata. Sarebbe utile esplicitare tali limiti nelle istruzioni, sia per l'interno che per l'esterno fornendo anche soluzioni per l'invio di documenti di grosse dimensioni (allegati cartografci e simili), tramite eventualmente l'invio di supporti fisici (CD o DVD), chiaramente descritti nella lettera di trasmissione, magari riportando l'impronta dei documenti informatici inviati separatamente, secondo il modello già previsto per i riferimenti esterni nella segnatura di protocollo[19].

Nel caso invece di comunicazione on-line i sistemi e le informazioni nei portali, essendo specificamente pensati e proposti all'utenza dovrebbero obbligare a utilizzare solo determinati formati con le necessarie sottoscrizioni, predeterminando anche le dimensioni e l'organizzazione dei documenti da inserire e trasmettere, non consentendo errori in tal senso.

Un ultimo punto da esaminare nei messaggi in entrata è la validità giuridica e amministrativa dei documenti inviati, in particolare relativamente alla verifica della provenienza effettiva da colui che si dichiara autore del documento, a e a chi può competere tale valutazione.

Le recenti modifiche al CAD hanno portato la necessità di rivalutare alcune precedenti certezze, quale quella dell'obbligo di spedizione e ricezione esclusivamente di documenti firmati digitalmente. Alla luce dell'attuale sistema appare necessario che i sistemi di registrazione di protocollo non prevedano vincoli automatici che obblighino l'invio o la ricezione di soli documenti firmati digitalmente, ma possano ricevere ed eventualmente inviare documenti con diversi tipi di firma o perfino non firmati. Infatti i sistemi di protocollo dovrebbero essere improntati al principio dell'avalutatività, cioè della possibilità di registrare tutti i documenti ricevuti indipendentemente dalla regolarità del documento stesso. Ovviamente nel caso di trasmissione di documenti firmati digitalmente debbono essere effettuate le opportune verifiche di validità delle firme (integrità, certificati revocati o scaduti).

L'ente che spedisce dovrebbe garantire la corretta formazione del documento anche da un punto di vista giuridico ed amministrativo, mentre dovrebbe essere il responsabile del

[19] Vedi pag. 23.

procedimento a valutare la correttezza e piena validità dei documenti ricevuti, proponendo eventualmente soluzioni in sanatoria.

Si ricorda che le istanze e le dichiarazioni presentate alle pubbliche amministrazioni sono valide se sottoscritte con firma digitale, ovvero quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi o anche con altri strumenti che consentano l'individuazione del soggetto che richiede il servizio, nei limiti di quanto stabilito da ciascuna amministrazione. Inoltre sono valide anche le istanze inviate telematicamente corredate da copia fotostatica del documento d'identità[20].

L'art. 65 del CAD in particolare il comma 1 lettera c) richiama espressamente le modalità di cui all'articolo 38, comma 3 del DPR 445/2000, che, nel testo vigente, modificato dal D.Lgs 30 dicembre 2010, n. 235, recita: "***La copia dell'istanza sottoscritta dall'interessato e la copia del documento di identità possono essere inviate per via telematica***", quindi si può valutare pienamente accettabile l'invio tramite mail, o meglio PEC, alla casella di posta certificata istituzionale di copia per immagine dell'originale analogico dell'istanza (istanza sottoscritta con firma autografa scansionata) corredata dalla copia per immagine del documento d'identità.

Per l'ente ricevente il documento può essere trattato come documento informatico.

Con lo stesso D.lgs. 30 dicembre 2010, n. 235 è stato modificato anche il comma 2 dell'art. 38, che opera un richiamo all'art. 65 del CAD per la validità delle istanze e delle dichiarazioni inviate alla pubblica amministrazione e che ora specifica: ***" ivi comprese le domande per la partecipazione a concorsi per l'assunzione, a qualsiasi titolo, in tutte le pubbliche amministrazioni, o per l'iscrizione in albi, registri o elenchi tenuti presso le pubbliche amministrazioni".***

L'articolo 65 del CAD contiene anche il nuovo comma c) bis che chiarisce che le istanze e le dichiarazioni sono valide, cioè di fatto ne può essere riconosciuta validamente la provenienza e l'attribuzione ad un autore certo, nel caso siano "t***rasmesse dall'autore mediante la propria casella di posta elettronica certificata purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con regole adottate ai sensi dell'articolo 71, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato. In tale caso la trasmissione costituisce dichiarazione vincolante"*** dell'indirizzo come espressa accettazione dell'invio a tale indirizzo, tramite PEC , da parte delle pubbliche amministrazioni, degli atti e dei provvedimenti che lo riguardano. Il comma conclude con una clausola di salvaguardia per l'uso di specifici sistemi di trasmissione telematica nel settore tributario.

E' da notare che in assenza di regole tecniche che definiscano le modalità di identificazione del titolare per via telematica, l'unica identificazione certa da parte del gestore di PEC può essere solo quella de visu ora prevista per la CEC-PAC. Per la piena applicabilità di tale comma rimangono però da definire anche le modalità di attestazione da parte del gestore dell'effettiva identificazione del titolare della casella di posta elettronica, attualmente non presenti nei messaggi di PEC o di CEC-PAC. Tali elementi poi dovrebbero essere mantenuti e conservati dall'amministrazione ricevente per successive esibizioni dei documenti.

[20] Art 65 CAD.

Tra pubbliche amministrazioni le comunicazioni dovrebbero avvenire mediante l'utilizzo della posta elettronica o in cooperazione applicativa e sono valide ai fini del procedimento amministrativo una volta verificata la provenienza, mediante la presenza di una firma digitale o della segnatura di protocollo o trasmessi per PEC.

Nel caso di documenti non firmati trasmessi tramite semplice e-mail si può provvedere a registrarli a protocollo se ritenuto necessario dal responsabile del procedimento, nel caso in cui sia possibile verificare la provenienza e la rispondenza del contenuto rispetto a quanto atteso. Le tabelle in allegato forniscono un elenco di possibili casi di valutazione.

Allegati

Nome	Breve descrizione	Data ultimo agg.to	Disponibilità
1) Uso della PEC	Esempi di comunicazioni da pubblicare nei si ti sull'uso della PEC (esempi tratti dalla Provincia di Ravenna e dalla Provincia di Modena)	01/06/2011	Versione 1.1
2) Tabelle di riepilogo	Possibili casi di trattamento dei messaggi in ingresso	05/09/11	Versione 1.1
3) Normativa di riferimento			Versione 1.1
4) Glossario condiviso			

Allegato 1 - Uso della PEC

Esempi di comunicazioni sull'uso della PEC

Provincia di Ravenna:
PEC - Posta Elettronica Certificata

La **Posta Elettronica Certificata (PEC)** è un sistema di posta elettronica che permette di inviare e ricevere comunicazioni e documentazione elettronica, con valenza legale paragonabile a quella della raccomandata con ricevuta di ritorno.
Solo la comunicazione tra due caselle P.E.C. garantisce l'emissione della ricevuta di avvenuto inoltro e ricezione.
Per comunicare in forma digitale con imprese, privati e pubbliche amministrazioni, la Provincia di Ravenna si è dotata dal 2006 di una casella di posta elettronica certificata iscritta all'IPA:

- provra@cert.provincia.ra.it

Questo indirizzo va utilizzato se si ha la necessità di ottenere ricevuta di avvenuta consegna del messaggio (per i mittenti dotati di casella di posta certificata) e di inoltrare documentazione formale (preferibilmente in formato pdf, pdf/a, rtf, tiff) da far acquisire al protocollo provinciale.
In particolare, verranno accettate:

- comunicazioni provenienti da caselle PEC di Pubbliche Amministrazioni con o senza file di segnatura;
- comunicazioni provenienti da caselle PEC di privati cittadini, rilasciate ai sensi del DPCM 6 maggio 2009 "Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini";
- comunicazioni provenienti da caselle PEC di privati rilasciate da gestori accreditati presso DigitPA (CNIPA);
- comunicazioni provenienti da caselle di posta elettronica collegate a protocolli informatici;
- comunicazioni provenienti da caselle di posta elettronica, anche non certificata, con allegato almeno un documento firmato digitalmente.

Le comunicazioni provenienti da caselle non certificate e prive di firma digitale potrebbero non essere acquisite, salvo che l'ufficio responsabile del Procedimento non ritenga opportuno procedere.
Per la semplice richiesta di informazioni sull'Ente e i suoi servizi e per qualsiasi segnalazione si può utilizzare l'indirizzo urp@mail.provincia.ra.it

Provincia di Modena:
Posta Elettronica Certificata (PEC)

La Posta Elettronica Certificata (PEC) è lo strumento per attivare lo scambio telematico di documenti fra gli enti pubblici e i cittadini e per ottenere l'evidenza dell'avvenuta consegna al destinatario dei messaggi.

Un messaggio spedito da una casella di PEC ad un'altra casella di PEC ha il valore legale di una raccomandata con ricevuta di ritorno e rispetto a quest'ultima presenta diversi vantaggi tra i quali i costi più ridotti, la semplicità di gestione e riproduzione dei documenti digitali, la facilità con cui si inviano copie multiple dei documenti.

Nel caso si spedisca un messaggio da una casella di PEC ad una casella di posta normale non si avrà nessuna ricevuta di avvenuta consegna ma solo una ricevuta di invio (ed il fatto che il documento sia stato spedito sarà l'unico fatto certificato, mentre nessuna certezza ci sarà sulla consegna del documento al destinatario).

Se invece si spedisce da una casella di posta normale ad una di posta certificata, il mittente non avrà in restituzione nessun messaggio di conferma, non avrà certezze sull'arrivo del suo documento e la sua spedizione non avrà nessun valore legale.

Al fine di comunicare in forma digitale con imprese, privati e pubbliche amministrazioni, la Provincia di Modena mette a disposizione l'indirizzo provinciadimodena@cert.provincia.modena.it cui inoltrare istanze, richieste e comunicazioni.

Per la semplice richiesta di informazioni sull'Ente e i suoi servizi, si può utilizzare l'indirizzo info@provincia.modena.it

Allegato 2 - Tabelle di riepilogo

Casi di trattamento messaggi in ingresso

A) Tabella di riepilogo possibili casi di trattamento messaggi in ingresso ricevuti dalla casella istituzionale o da altre caselle PEC collegate al protocollo

Tipologia documenti	**Canali di trasmissione/ sistemi di comunicazione di invio del messaggio**	**Accettazione e Registrazione di protocollo**	**Note**	**Validità giuridico/amministrativa**	**Validità probatoria**
Messaggio con Documento firmato con firma digitale o qualificata	PEI interoperabilità; PEC; CEC-PAC; PEO Comunicazioni on line	Si, sempre	Associare alla registrazione di protocollo tutti gli elementi del messaggio: Documento informatico (doc principale) e altri allegati Corpo del messaggio segnatura. xml daticert.xml	si	Scrittura privata
Messaggio con Documento firmato con firma avanzata scambiato tra PA	PEI interoperabilità PEC	Sì, sempre	Ipotesi possibile nei casi di scambio di documenti in procedimenti amministrativi inerenti, definiti da accordi specifici	Sì (nb. se documento prodotto da PA solo se l'atto ha rilevanza interna al procedimento amministrativo)	Valore scrittura privata solo contenenti atti a rilevanza interna al procedimento amministrativo. Altrimenti liberamente valutabile
Documento digitale firmato con firma avanzata da servizio on line	Comunicazioni on-line	Sì, sempre	Sì, sempre	Si (per casi es. procedura turismo che non siano istanze o dichiarazioni ai sensi dell'articolo 65 CAD)	Valore scrittura privata se conformi ai requisiti previsti dall'art. 21 comma 4 del CAD, cioè che

					garantiscano identificabilità dell'autore, integrità e immodificabilità
Documento digitale firmato con firma avanzata da cittadino				No	Liberamente valutabile
Messaggio con Documento non firmato o con firma elettronica inviato da cittadini o imprese o messaggio semplice con contenuto amministrativo rilevante	PEC o CEC - PAC	Si, sempre	Eventuale richiesta firma	Si se regolarizzato Necessaria richiesta di regolarizzazione e acquisizione firma digitale fino al momento in cui verrà data piena attuazione al comma c. bis dell'art. 65 del CAD	Liberamente valutabile
Messaggio con Documento non firmato o con firma elettronica inviato da cittadini o imprese o messaggio semplice con contenuto amministrativo rilevante	PEO	A valutazione del responsabile del procedimento o in accordo con il responsabile di protocollo	Per evitare di decidere caso per caso si può operativamente ipotizzare anche una registrazione per tutte le mail con contenuti rilevanti che pervengono a indirizzi istituzionali (PEI o PEC)	Liberamente valutabile Eventuale/necessaria richiesta di regolarizzazione	Liberamente valutabile
Messaggio con Documento costituito da copia immagine di documento firmato autografamente e allegati + scansione Carta di identità	PEO PEC o CEC PAC	Sì, sempre	Sì	Sì	Sì

Documento allegato non leggibile dal sistema	PEI interoperabilità; PEC; CEC-PAC; PEO	No, con notifica di errore		No	Liberamente valutabile
Documento firmato non leggibile perché corrotto	PEI interoperabilità; PEC; CEC-PAC; PEO	No, con notifica di errore		No	No
Messaggio semplice riferito a bandi che richiedono compilazione moduli	PEC; CEC-PAC; PEO	No, con notifica di errore		No	Liberamente valutabile
Messaggio per richiesta informale a carattere informativo	PEC; CEC-PAC; PEO	Si con inoltro interno all'unità competente ed eventuale registrazione di protocollo	Si può nei sistemi che lo prevedono effettuare una registrazione del tipo NP	no	Liberamente valutabile

B) Tabella di riepilogo possibili casi di trattamento messaggi in ingresso ricevuti da caselle di utenti non istituzionali e non collegate al protocollo

Tipologia documenti	Canali di trasmissione/ sistemi di comunicazione di invio del messaggio	Accettazione e Registrazione di protocollo	Note	Validità giuridico/ amm.va	Validità probatoria
Messaggio con Documento firmato con firma digitale o qualificata e contenuto amministrativo rilevante	PEC; CEC-PAC; PEO	Si, su responsabilità del ricevente. La registrazione di protocollo può avvenire direttamente da parte del ricevente o tramite invio ad una casella istituzionale oppure richiedendo al mittente una nuovo invio alla casella istituzionale	Associare alla registrazione di protocollo tutti gli elementi del messaggio: Documento informatico (doc principale) ev. altri allegati Corpo del messaggio segnatura. xml daticert.xml	si	Scrittura privata
Messaggio con Documento non firmato o con firma elettronica inviato da cittadini o imprese o messaggio semplice con contenuto amministrativo rilevante	PEO PEC CEC-PAC	A valutazione del responsabile del procedimento in accordo con il responsabile di protocollo	Eventuale o necessaria richiesta di regolarizzazione: firma digitale ed invio a casella istituzionale	Liberamente valutabile	Liberamente valutabile
Documento firmato non leggibile perché corrotto	PEC; CEC-PAC; PEO	No, con notifica di errore		No	No
Messaggio semplice riferito a bandi che richiedono compilazione moduli	PEC; CEC-PAC; PEO	No, con notifica di errore	Segnalare a cura del ricevente corretta modalità di invio	No	Liberamente valutabile
Messaggio per richiesta informale a carattere informativo	PEC; CEC-PAC; PEO	Si senza registrazione di protocollo	Se il destinatario è competente per la risposta può agire direttamente	no	Liberamente valutabile

Allegato 3 - Normativa di riferimento in materia d flussi documentali

Elenco delle principali norme in vigore distinte tra norme principali, DPCM e delibere o circolari CNIPA (ora DigitPA)

Normativa principale				
L. 214/1990 (G.U. 18 agosto 1990, n. 192)	*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*	Modificata e integrata con L. 11 febbraio 2005, n. 15; L. 80/2005; D. Legge 14 marzo 2005, n. 35; L. 2 aprile 2007, n. 40; L. 18 giugno 2009, n. 69; D. Legge 31 maggio 2010, n. 78; D.Lgs 2 luglio 2010, n. 104; D. Lgs. 13 maggio 2011, n. 70	Riconosce la centralità di un corretto sistema di gestione dei documenti, requisito per ulteriori processi innovativi. Le Pubbliche amministrazioni sono tenute ad individuare, per ciascun provvedimento, l'unità organizzativa responsabile dell'istruttoria e di ogni altro adempimento procedurale e a proporre, all'interno di ciascuna di esse, il responsabile del procedimento. Legge 241/90 con modifiche e integrazioni: http://www.altalex.com/index.php?idnot=550	Procedimento amministrativo Diritto di accesso
DPR 445/2000(G.U. 20 febbraio 2001, n. 42)	Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa	Entrata in vigore: 7.3.2001 Aggiornamenti all'atto 15/02/2002 DECRETO LEGISLATIVO 23 gennaio 2002, n. 10 (in G.U. 15/02/2002, n.39) 20/01/2003 LEGGE 16 gennaio 2003, n. 3 (in SO n.5, relativo alla G.U. 20/01/2003, n.15) .	Disciplina la formazione, il rilascio, la tenuta e la conservazione, la gestione, la trasmissione di atti e documenti da parte di organi della pubblica amministrazione, nonché predispone criteri per la gestione dei flussi documentali. L'art. 50 dispone che entro il 1	Conservazione sostitutiva; Digitalizzazione documenti; Gestione digitale dei flussi documentali; Dematerializzazio

		13/02/2003 DECRETO DEL PRESIDENTE DELLA REPUBBLICA 14 novembre 2002, n. 313 (in SO n.22, relativo alla G.U. 13/02/2003, n.36) 17/06/2003 DECRETO DEL PRESIDENTE DELLA REPUBBLICA 07 aprile 2003, n. 137 (in G.U. 17/06/2003, n.138) 03/07/2003 Errata Corrige (in G.U. 03/07/2003, n.152) , nel modificare l'art. 1, comma 1 del D.P.R. 7 aprile 2003, n. 137 (in G.U. 17/06/2003, n. 138), ha conseguentemente disposto la modifica dell'art. 1, comma 1, lettere q) e cc). 29/07/2003 DECRETO LEGISLATIVO 30 giugno 2003, n. 196 (in SO n.123, relativo alla G.U. 29/07/2003, n.174)) . 28/04/2005 DECRETO DEL PRESIDENTE DELLA REPUBBLICA 11 febbraio 2005, n. 68 (in G.U. 28/04/2005, n.97) . 16/05/2005 DECRETO LEGISLATIVO 07 marzo 2005, n. 82 (in SO n.93, relativo alla G.U. 16/05/2005, n.112) . 10/01/2011 DECRETO LEGISLATIVO 30 dicembre 2010, n. 235 (in SO n.8, relativo alla G.U. 10/01/2011, n.6) . 13/05/2011 DECRETO-LEGGE 13 maggio 2011, n. 70 (in G.U. 13/05/2011, n.110) , convertito con modificazioni dalla L. 12 luglio 2011, n. 106.	gennaio 2004 tutte le pubbliche amministrazioni attivino almeno il “nucleo minimo” per digitalizzare la gestione dei documenti. Stabilisce che ogni amministrazione individui al proprio interno delle Aree Organizzative Omogenee, assicurandone criteri uniformi di classificazione e archiviazione, nonché di comunicazione interne fra esse, ai fini della gestione unica o coordinata dei documenti.	ne

D. Lgs. 7 Marzo 2005, n.62 (G.U. 16 maggio 2005, n. 112)	Codice dell'amministrazione digitale	In vigore da 1 gennaio 2006 Aggiornamenti: D.Lgs 4 aprile 2006, n. 159; L. 18 giugno 2009, n. 69; L. 3 agosto 2009, n. 102; D.Lgs. 30 dicembre 2010, n. 235.	Il Codice (CAD) obbliga tutte le amministrazioni a produrre e gestire i documenti con sistemi informatici. Fornisce definizioni e termini di utilizzo della gestione informatica dei documenti, delle firme elettroniche e introduce la valutazione del rapporto tra costi e benefici della dematerializzazione dei documenti della pubblica amministrazione	Conservazione sostitutiva, Digitalizzazione documenti, Gestione digitale dei flussi documentali Dematerializzazione
DPCM				
DPCM 30 marzo 2009 (G.U. 6 giugno 2009, n. 129)	*Regole tecniche in materia di generazione, apposizione, verifica delle firme digitali e validazione temporale per il riconoscimento e la verifica*		In corso di modifica	Firma digitale
DPCM 31 ottobre 2000 (G.U. 21 novembre 2000, n. 272)	Regole tecniche per il protocollo informatico		Scambio telematico dei dati di registrazione e l'accesso in rete ai sistemi di protocollo mediante la rete unitaria della pubblica amministrazione, le regole tecniche sull'interoperabilità. Stabilisce la creazione del Manuale di Gestione che descrive il sistema di gestione di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio	Protocollo; Interoperabilità; Gestione digitale dei flussi documentali

Delibere CNIPA/DigitPA				
Determinazione DigitPA 28 luglio 2010, n. 69	*Modifiche alla Deliberazione 21 maggio 2009 n. 45 del CNIPA*			Firma digitale
Circolare CNIPA 21 maggio 2009, n.45 (G.U. 22 luglio 2009, n. 168)	*Regole tecniche per il riconoscimento e la verifica del documento informatico*	Modificata da Determinazione DigitPA n.69 del 28 luglio 2010		Firma digitale
Deliberazione CNIPA 19 febbraio 2004, n. 11 (G.U. 19 febbraio 2004, n. 42)	*Regole guida per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti originali*		*Suddivide i documenti in informatici e analogici; Prevede la possibilità di conservare su un qualsiasi tipo di supporto (oltre a quelli a tecnologia laser) i documenti analogici e informatici attraverso l'apposizione del riferimento temporale e della firma digitale.*	*Conservazione sostitutiva; Digitalizzazione dei documenti; Gestione digitale dei flussi documentali; Dematerializzazione*
Circolare AIPA 7 maggio 2001, n. AIPA/CR/28 (G.U. 21 novembre 2001, n. 272)	Standard, modalità di trasmissione, formato e definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati	Art. 18, comma 2, DPCM 31 ottobre 2000	Schema della segnatura.xml	Interoperabilità protocollo informatico

Allegato 4 - Glossario e acronimi

Introduzione

In tema di gestione documentale la redazione di un glossario completo potrebbe contenere numerosi lemmi.
In questa prima fase ci si limita alla definizione di alcuni termini utilizzati nelle linee guida facendo riferimento alle definizioni fornite dalla normativa italiana e dagli standard di riferimento o da progetti internazionali nella loro traduzione italiana. Per ogni definizione la fonte di riferimento è citata in forma sintetica tra parentesi quadre.
Nel caso in cui non siano presenti definizioni in tali fonti si è fatto riferimento alla tradizione archivistica italiana, in particolare al glossario edito nel volume di Paola Carucci *Le fonti archivistiche: ordinamento e conservazione,* NIS 1983 e in parte disponibile nel sito ufficiale del Ministero per i Beni e le Attività Culturali – Direzione Generale degli Archivi http://www.archivi.beniculturali.it/tools/DGA-glossario/. [CARUCCI].
Si può presentare il caso in cui lo stesso termine possa avere utilizzo e definizioni diverse. In tal caso vengono indicate le diverse definizioni numerate.
Termini contenuti nelle definizioni a loro volta definiti nel presente glossario sono riportati in *corsivo.*

Terminologia chiave: glossario e definizioni

accesso: Diritto, possibilità, mezzi per ricercare, trovare o usare informazioni [UNI ISO 15489-1:2006]

acquisizione: (sistemi di *gestione documentale*): *Registrazione, classificazione,* aggiunta di *metadati* e memorizzazione di un *documento d'archivio* [MOREQ][21]

affare: Complesso di documenti prodotti (spediti, ricevuti, allegati, ecc.) da un ente relativi alla trattazione di un oggetto specifico di sua competenza: detto anche pratica [CARUCCI]

affidabilità: La capacita' di un documento di rappresentare i fatti di cui tratta. [INTERPARES]

archivio:
1: Complesso di documenti prodotti o comunque acquisiti da un ente durante lo svolgimento della propria attività[22] [CARUCCI]
2: Istituto nel quale vengono concentrati archivi di varia provenienza che ha per fine istituzionale la conservazione permanente dei documenti destinati alla pubblica consultazione [CARUCCI][23]

[21] Si tratta della traduzione del termine inglese usato da MOREQ2 ***capture.*** Si rimanda anche a tale definizione in particolare nella specifica accezione utilizzata da MOREQ2 che fa riferimento ad almeno uno dei processi utilizzati per inserire un *documento d'archivio (record)* in un ERMS: *Registrazione, classificazione,* aggiunta di *metadati* e protezione dell'*integrità* del documento (freezing the contents of the source document)
[22] I documenti che compongono l'*archivio* corrispondono alla definizione di *documento d'archivio (record).*

archivio corrente: Fase dell'archivio/parte di documentazione relativa agli *affari* in corso; in questa fase i documenti sono usati prevalentemente per finalità pratico-amministrative [CARUCCI]

archivio di deposito: Fase dell'archivio/parte di documentazione relativa ad *affari* esauriti, non più occorrente quindi alla trattazione degli affari in corso, ma non ancora destinata istituzionalmente alla conservazione permanente e alla libera consultazione da parte del pubblico; in questa fase tende a diminuire l'utilizzazione dei documenti da parte dell'ente che li ha prodotti ed aumentare la richiesta di utilizzazione da parte dei ricercatori [CARUCCI]

archivio storico: Fase dell'archivio/parte di documentazione relativa agli affari esauriti, destinata- previa operazioni di scarto – alla conservazione permanente per garantirne in forma adeguata la consultazione al pubblico per finalità di studio o non di studio[CARUCCI]. La normativa italiana prevede che appartengono a questa fase i documenti relativi agli affari esauriti da oltre quaranta anni [DLGS 42/2004 art. 30]

area organizzativa omogenea (AOO): un insieme di funzioni e di strutture, individuate dall'amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario [DPCM 31 ottobre 2001 art. 2, comma 1, lettera n)] In particolare ciascuna AOO mette a disposizione delle unità organizzative clienti il servizio di protocollazione dei documenti, utilizzando un unica sequenza numerica, rinnovata ad ogni anno solare, propria alla AOO stessa [glossario Indice PA]

autenticità: Proprietà del documento di essere ciò che dichiara di essere senza aver subito alterazioni o modifiche [INTERPARES]

autorità archivistica, amministrazione archivistica, istituto archivistico, programma archivistico: Struttura o programma che ha la responsabilità di selezionare, acquisire e conservare i documenti destinati alla conservazione permanente, renderli disponibili e autorizzare la distruzione degli altri [UNI ISO 15489-1:2006](vedi anche *polo archivistico*)

casella istituzionale: la casella di posta elettronica [ora certificata] istituita da una AOO, attraverso la quale vengono ricevuti i *messaggi protocollati*, come previsto dal DPCM 31 ottobre 2000, art. 15, comma 3 [Circolare AIPA n. 28/2001, allegato A art. 1]

casella di posta elettronica certificata: la casella di posta elettronica posta all'interno di un dominio di posta elettronica certificata ed alla quale è associata una funzione che rilascia ricevute di avvenuta consegna al ricevimento di messaggi di posta elettronica certificata [DM 2/11/2005, art. 1]

[23] In questa definizione può essere ricompresa anche la definizione di archivio data da OAIS: organizzazione che mira a conservare informazioni per l'accesso e l'uso da parte di una comunità di riferimento, ovvero struttura organizzata di persone e sistemi che accetti la responsabilità di conservare informazioni e renderle disponibili per una comunità di riferimento.

classificazione: Identificazione e organizzazione in modo sistematico delle attività e/o dei relativi documenti in categorie strutturate logicamente e rappresentate in un piano di classificazione secondo principi condivisi, metodi e regole procedurali [UNI ISO 15489-1:2006]24

cooperazione applicativa: la parte del sistema pubblico di connettività finalizzata all'interazione tra i sistemi informatici della pubbliche amministrazioni per garantire l'integrazione dei *metadati,* delle informazioni e dei procedimenti ammnistrativi [D.Lgs. 82/2005 art. 72 lettera e)]

conservazione: L'ordinata *custodia* di documenti informatici in modo da assicurarne l'*integrità*, l'*affidabilità* e la consultabilità nel tempo, anche attraverso idonei strumenti di ricerca [Deliberazione AIPA n. 51/2000, art. 2] ovvero Processi e operazioni necessari a garantire nel tempo la permanenza di documenti autentici nei loro aspetti fisici e intellettuali [UNI ISO 15489-1:2006]

conservazione a lungo termine: L'azione di mantenimento delle informazioni a *lungo termine,* in una forma corretta e comprensibile in maniera autonoma [OAIS]

conservazione sostitutiva: Processo effettuato con le modalità di cui agli articoli 3 e 4 della Deliberazione CNIPA 19 febbraio 2004 (n. 11/2004) [Deliberazione CNIPA n. 11/2004, art.1 lettera i)]

conservazione sostitutiva di documenti informatici: processo di memorizzazione su supporti idonei che termina con l'apposizione sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte di documenti o insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta il regolare svolgimento del processo [Deliberazione CNIPA n. 11/2004, art.3]

custodia: La responsabilità di prendersi cura della documentazione, che deriva dal suo possesso materiale. La custodia non sempre comprende la proprietà giuridica o il diritto al controllo sull'accesso ai documenti. [ISAD]

documento: (document). Informazioni memorizzate a prescindere dal supporto o dalle caratteristiche (vedi anche *documento d'archivio o archivistico*) [ISAD].

documento amministrativo: Ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa [D.PR. 445/2000, art. 1 lettera a)]

documento d'archivio o archivistico, (record): Informazioni prodotte, ricevute e conservate a fini probatori e informativi da una persona fisica o giuridica per soddisfare obblighi legali o per lo svolgimento delle proprie attività [UNI ISO 15489-1:2006]; ovvero: Informazioni memorizzate su qualsiasi supporto o *tipologia documentaria*, prodotte o ricevute e conservate da un ente o da una persona nello svolgimento delle proprie attività o nella condotta dei propri affari [ISAD] ovvero

[24] Nella tradizione archivistica il piano di classificazione è articolato in livelli gerarchicamente ordinati in relazione alle funzioni e alle modalità operative degli enti e denominato *Titolario.* (vedi anche *sistema di classificazione*)

Un *documento* creato o ricevuto e messo da parte (set aside) nel corso di una attività pratica [INTERPARES glossary dec. 2004].

documento informatico: La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti [D. Lgs. n. 82/2005, art 1 lettera. p)] .

firma elettronica: l'insieme dei dati in forma elettronica allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica [D.lgs 82/2005 art. 1 lettera q)]

firma elettronica avanzata: insieme dei dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modficati [D.lgs 82/2005 art. 1 lettera q-bis)]

firma elettronica qualificata: un particolare tipo di *firma elettronica avanzata* che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma [D.lgs 82/2005 art. 1 lettera r)]

firma digitale: un particolare tipo di *firma elettronica avanzata* che sia basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici [D.lgs 82/2005 art. 1 lettera s)][25]

formato: modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico [Glossario DigitPA]

funzione di hash*:* Una funzione matematica (algoritmo) che genera, a partire da una generica sequenza di simboli binari (bit), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire la sequenza di simboli binari (bit) originaria e generare impronte uguali a partire da sequenze di bit differenti [DPCM 30 marzo 2009, art. 1 lettera g)]

gestione documentale: vedi ***gestione informatica dei documenti***

gestione informatica dei documenti: L'insieme della attività finalizzate alla *registrazione e segnatura di protocollo,* nonché alla *classificazione,* organizzazione, assegnazione, reperimento e *conservazione* dei *documenti amministrativi* formati o acquisiti dalle amministrazioni nell'ambito del *sistema di classificazione* d'archivio adottato, effettuato mediante sistemi informatici [D.Lgs. 82/2005 art. 1 lettera u)]

[25] Per le ulteriori definizioni dei termini, quali certificato qualificato, chiave privata e chiave pubblica si rimanda alle definizioni del CAD [D.Lgs. 82/2005 art. 1 lettere f), h) e i)]

immodificabilità: caratteristica che rende il contenuto del documento informatico non alterabile durante l'intero ciclo di gestione e conservazione del documento stesso [Glossario DigitPA]

impronta di una sequenza di simboli binari (bit): la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna *funzione di hash*. [DPCM 30 marzo 2009, art. 1 lettera h)]

integrità: proprietà del documento di essere completo e inalterato in tutti i suoi elementi essenziali [INTERPARES]; insieme delle caratteristiche di un *documento informatico* che ne dichiarano la qualità di essere completo e inalterato nei suoi elementi essenziali [Glossario DigitPA]

interoperabilità: capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi [Glossario DigitPA]

leggibilità: insieme delle caratteristiche in base alle quali le informazioni contenute in un *documento informatico* sono fruibili durante l'intero ciclo di gestione e conservazione del documento stesso [Glossario DigitPA]

lungo termine : un intervallo di tempo sufficientemente ampio da dover considerare l'impatto prodotto sulle informazioni conservate in un deposito dai cambiamenti delle tecnologie (incluso l'utilizzo di nuovi supporti e formati di dati) e della comunità di utenti. Tale periodo si estende indefinitamente nel futuro [OAIS]

metadati: dati che descrivono il contesto, il contenuto e la struttura dei documenti e la loro gestione nel tempo [UNI ISO 15489-1:2006]

messaggio protocollato: un messaggio di posta elettronica inviato da una AOO mittente per il quale esiste una corrispondente registrazione di protocollo [Circolare AIPA n. 28/2001, allegato A art. 1]

polo archivistico: Istituto o struttura, dotato di personalità giuridica, autonomia funzionale e personale proprio, dedicato alla conservazione di archivi di deposito/storici per più soggetti produttori.

posta elettronica:
1 - un sistema elettronico di trasmissione di documenti informatici [DPR 68/2005, art. 1]
2 – messaggi contenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente fino a che il ricevente non ne ha preso conoscenza [D.lgs. 196/2003 (Codice in materia di protezione dei dati personali) art. 4]

posta elettronica certificata (PEC): ogni sistema di posta elettronica nel quale è fornito al mittente documentazione attestante l'invio e la consegna di documenti informatici [DPR 68/2005, art. 1]

registrazione: Atto di assegnazione dell'identificazione univoca al documento al momento dell'immissione nel sistema [UNI ISO 15489-1:2006]

segnatura di protocollo*:* l'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso. [D.PR. 445/2000, art. 55 comma 1]

segnatura informatica: l'insieme delle informazioni archivistiche di protocollo, codificate in formato XML ed incluse in un messaggio protocollato, come previsto dall'art. 18, comma 1, del DPCM 31 ottobre 2000 [Circolare AIPA n. 28/2001, allegato A art. 1]

sistema di classificazione: strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata [DPCM 31 ottobre 2000, art. 2 lettera h)] (vedi anche *titolario)*

tipologia documentaria (form): una classe di documenti definita sulla base di comuni caratteristiche materiali (per esempio acquarello, disegno) e/o intellettuali (per esempio: diario, libro giornale, registro contabile, minutario).

titolario*:* un sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle competenze dell'Amministrazione, al quale deve ricondursi la molteplicità dei documenti prodotti, per consentirne la sedimentazione secondo un ordine logico che rispecchi storicamente lo sviluppo dell'attività svolta. Ovvero: quadro o *sistema di classificazione* articolato in categorie e eventualmente in ulteriori sotto-ripartizioni, in base al quale i documenti dell'*archivio corrente* vengono raggruppati secondo un ordine logico [Carucci]

Glossario degli acronimi utilizzati

AOO – Area Organizzativa Omogenea
CAD – Codice dell'Amministrazione Digitale: D.lgs. 82/2005 e successive modificazioni
CEC-PAC – Comunicazione Elettronica Certificata tra Pubblica Amministrazione e Cittadino
CIE - Carta d'Identità Elettronica
CNS – Carta Nazionale dei Servizi
INTERPARES - The International Research on Permanent Authentic Records in Electronic Systems
IPA – Indice delle Pubbliche Amministrazioni
ISAD - International Standard Archival Description
ISO- International Organization for standardization
OAIS - Open Archival Information Sistem
PEC – Posta Elettronica Certificata
PEO – Posta Elettronica Ordinaria o semplice