GIULIANOVA, 5, 7, 12 SETTEMBRE 2017

SALA BUOZZI

FORMAZIONE PERSONALE DIPENDENTE

DEMATERIALIZZAZIONE DEI PROCEDIMENTI AMMINISTRATIVI PARTE I

COMUNE DI GIULIANOVA
AREA I – Ufficio Sistemi Informativi
Dott. Gabriele MASSIMIANI

ABSTRACT PRESENTAZIONE

1) Definizione e caratteristiche del documento informatico
2) Il ciclo di vita del documento informatico: formazione, gestione e conservazione
3) Il valore giuridico di un documento informatico
4) La formazione del documento informatico
5) Le tipologie di firme elettroniche

DEMATERIALIZZAZIONE DEI FLUSSI DOCUMENTALI

Per "dematerializzazione" si intende la sostituzione dei supporti tradizionali della documentazione amministrativa in favore del documento informatico

La dematerializzazione dei documenti amm.vi non rappresenta solo un percorso volto al raggiungimento di livelli di maggior efficienza, efficacia, trasparenza, semplificazione e partecipazione, ma anche un preciso ed improrogabile precetto normativo

Il Codice dell'Amministrazione Digitale (CAD) - D.Lgs. 82/2005 e s.m.i.
Art. 40 - Formazione di documenti informatici:

"*Le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71*"

La norma richiamata stabilisce un preciso obbligo:
i documenti delle PA devono essere prodotti esclusivamente in modalità informatica

TRASMISSIONE DEI DOCUMENTI

Per la trasmissione dei documenti il CAD (D.Lgs. 82/2005 e s.m.i.) ha stabilito:

"*La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le PA avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le PA adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese*" (art. 5-bis, c. 1 del CAD)

"*I documenti trasmessi da chiunque ad una PA con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale*...omissis…." (art. 45, c. 1 del CAD)

Il CAD quindi ha stabilito che:

i documenti delle PA possono essere trasmessi alle imprese ed ai cittadini che hanno dichiarato il loro indirizzo (domicilio digitale - PEC) esclusivamente con strumenti informatici tipicamente via e-mail o PEC

Le operazioni di registrazione e segnatura di protocollo di un documento devono essere effettuate esclusivamente in modalità informatica

IL DOCUMENTO INFORMATICO: DEFINIZIONE

Il nuovo CAD (D.Lgs. 82/2005 e s.m.i. aggiornato dal D.Lgs. 179/2016) definisce il documento informatico come:

"*Il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*"

Il Regolamento europeo n. 910/2014 eIDAS (electronic IDentification Authentication and Signature) che regolamenta la materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato europeo interno, definisce il
documento elettronico: Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva

IL DOCUMENTO INFORMATICO: CARATTERISTICHE

Il documento informatico per la sua forma elettronica (rappresentazione informatica – sequenza di bit) può essere formato, acquisito, sottoscritto, trasmesso e conservato

ACCADEMIA DI BELLE ARTI
BOLOGNA

MODULO RICHIESTA RICONOSCIMENTO CREDITI
A.A. 2009/10
Consegnare presso le buchette dei rispettivi Dipartimenti
entro e non oltre il 3 dicembre 2009

□ **ARTI VISIVE**
□ **ARTI APPLICATE**
□ **COMUNICAZIONE E DIDATTICA DELL'ARTE**

Al Direttore
dell'Accademia di Belle Arti
di Bologna

Il sottoscritto/a .....iscritto per l'Anno Accademico...../..... al Corso di Diploma in .....del □ Triennio - □ Biennio, in conformità al protocollo n. 5127 del 8/11/2004.

CHIEDE

Riconoscimento dei seguenti esami svolti presso .....:

1).....voto .....data .....crediti.....
2).....voto .....data .....crediti.....
3).....voto .....data .....crediti.....
4).....voto .....data .....crediti.....
5).....voto .....data .....crediti.....
6).....voto .....data .....crediti.....

Si allega documentazione degli esami sostenuti.

Luogo, data

Firma

Via Belle Arti, 54 – 40126 BOLOGNA – Tel. 051 4226411 – Fax 051 253032
C.F. 80088230370

01111010 01111010 01101111 00100000 01100100 01100101
01101100 00100000 01100011 01100001 01101101 01101101
01101001 01101110 00100000 01100100 01101001 00100000
01101110 01101111 01110011 01110100 01110010 01100001
00100000 01110110 01101001 01110100 01100001 00001011
01101101 01101001 00100000 01110010 01101001 01110100
01110010 01101111 01110110 01100001 01101001 00100000
01110000 01100101 01110010 00100000 01110101 01101110
01100001 00100000 01110011 01100101 01101100 01110110
01100001 00100000 01101111 01110011 01100011 01110101
01110010 01100001 00101100 00001011 01100011 01101000
11101001 00100000 01101100 01001110 01100101 01101100
00100000 01101101 01100101 01111010 01111010 01101111
00100000 01100100 01100101 01101100 00100000 01100011
01100001 01101101 01101101 01101001 01101110 00100000
01100100 01101001 00100000 01101110 01101111 01110011
01110100 01110010 01100001 00100000 01110110 01101001
01110100 01100001 00001011 01101101 01101001 00100000
01110010 01101001 01110100 01110010 01101111 01110110
01100001 01101001 00100000 01110000 01100101 01110010
00100000 01110101 01101110 01100001 00100000 01110011
01100101 01101100 01110110 01100001 00100000 01101111
01110011 01100011 01110101 01110010 01100001 00101100
00001011 01100011 01101000 11101001 00100000 01101100
01001110 01100101 01101100 00100000 01101101 01100101
01111010 01111010 01101111 00100000 01100100 01100101
01101100 00100000 01100011 01100001 01101101 01101101
01101001 01101110 00100000 01100100 01101001 00100000
01101110 01101111 01110011 01110100 01110010 01100001
00100000 01110110 01101001 01110100 01100001 00001011
01101101 01101001 00100000 01110010 01101001 01110100
01110010 01101111 01110110 01100001 01101001 00100000
01110000 01100101 01110010 00100000 01110101 01101110
01100001 00100000 01110011 01100101 01101100 01110110
01100001 00100000 01101111 01110011 01100011 01110101
01110010 01100001 00101100 00001011 01100011 01101000
11101001 00100000 01101100

CICLO DI VITA DEL DOCUMENTO INFORMATICO

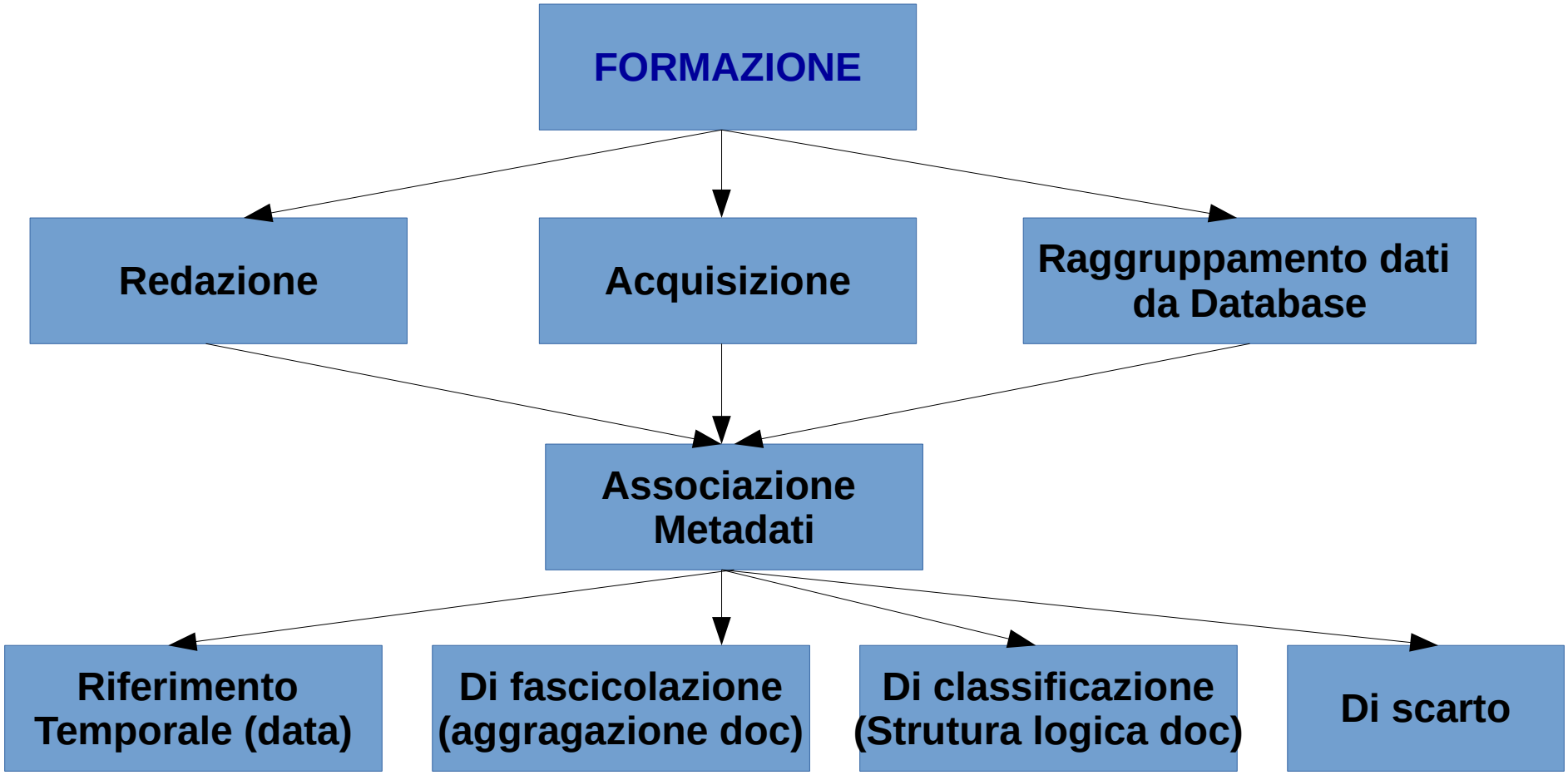
Il ciclo di vita di un documento (amministrativo) informatico può essere suddiviso in tre fasi principali:

1) **Formazione: l'attività di produzione, acquisizione e registrazione informatica del documento**

2) **Gestione: l'attività di sottoscrizione con firma digitale, trasmissione (invio/ricezione), ricerca, pubblicazione, etc. del documento informatico mediante il sistema informatico di gestione documentale (DPCM 03.12.2013 – Regole tecniche Protocollo informatico)**

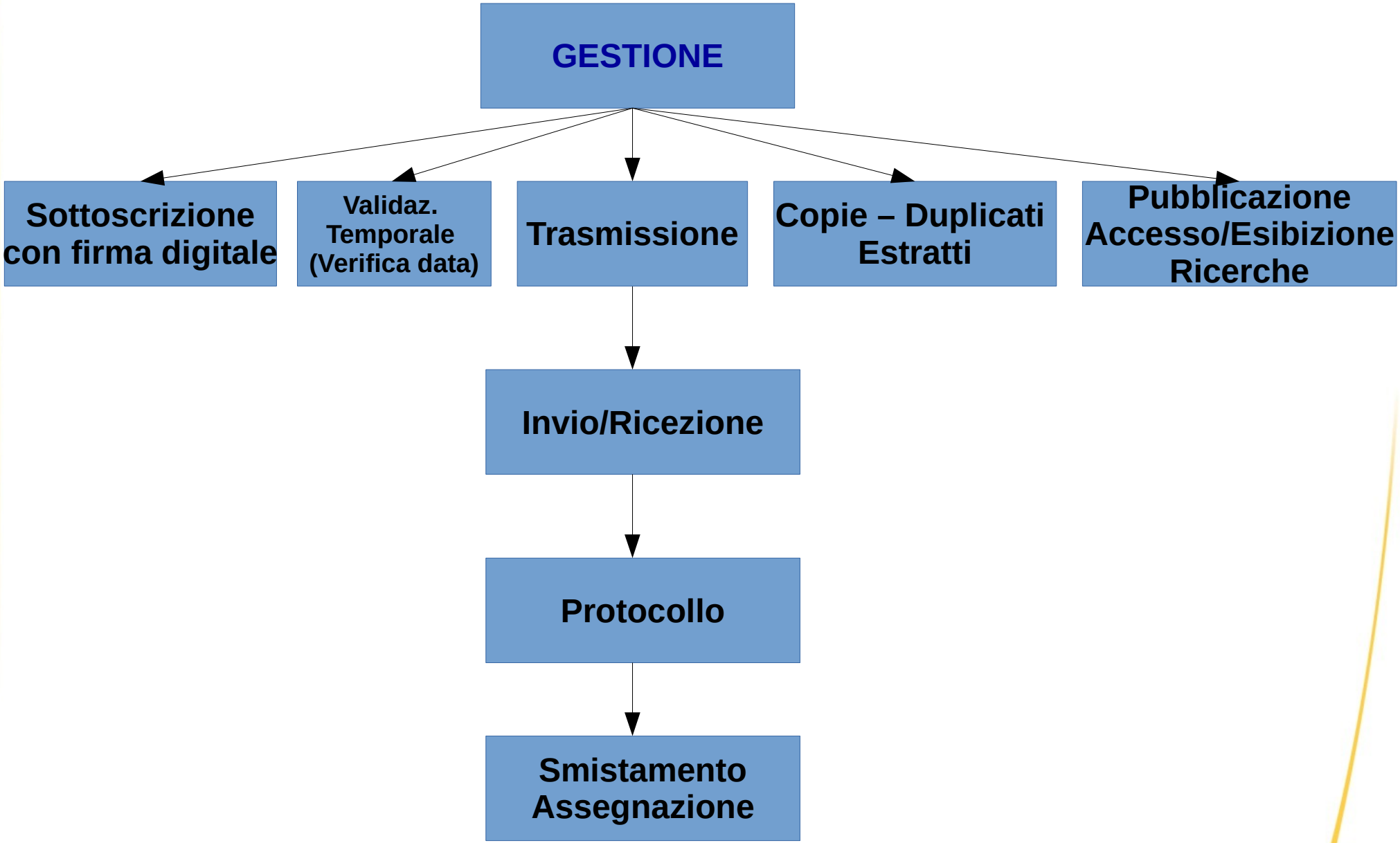
3) **Conservazione: l'attività volta a proteggere e mantenere (ovvero custodire) nel tempo gli archivi di documenti e dati informatici mediante il versamento dei documenti nel sistema di conservazione (DPCM 03.12.2013 – Regole tecniche in materia di conservazione dei documenti)**

FORMAZIONE DEL DOCUMENTO INFORMATICO

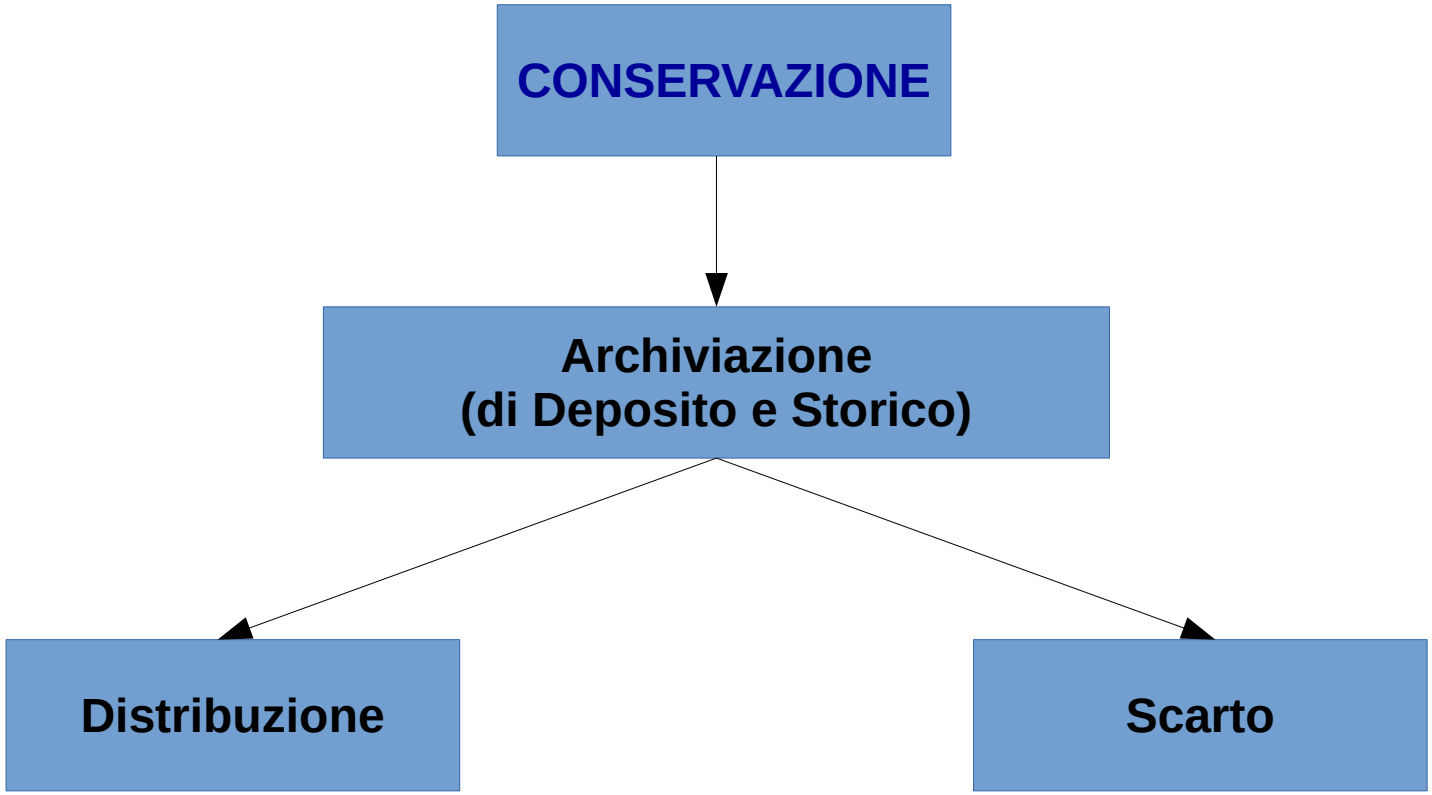


Metadati: sono informazioni associate ad un documento informatico per identificarlo e descriverne: contesto, contenuto e struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione

GESTIONE DEL DOCUMENTO INFORMATICO



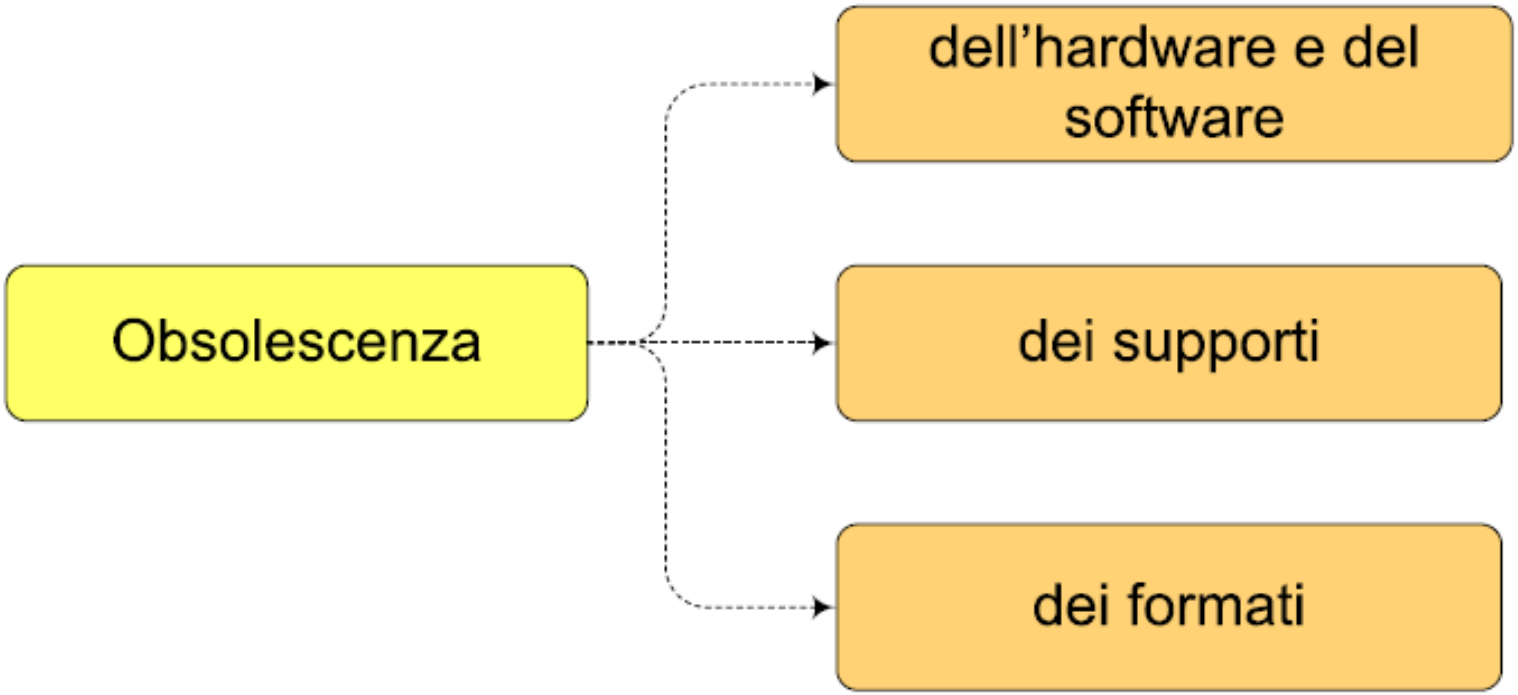
CONSERVAZIONE DEL DOCUMENTO INFORMATICO



Chiude il ciclo di vita di un documento informatico la sua conservazione a norma o, eventualmente, il suo definitivo scarto, ossia l'operazione con cui si eliminano i documenti ritenuti privi di valore amministrativo e di interesse storico culturale

"Almeno una volta all'anno il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti conclusi" (Art. 44 del CAD)

CONSERVAZIONE DEI DOCUMENTI INFORMATICI



Per garantire la conservazione digitale nel lungo periodo occorre un sistema che garantisca:

1) l'integrità della rappresentazione informatica (bit preservation)

2) la conservazione logica (Logical preservation) intesa come la capacità di comprendere e utilizzare l'informazione in futuro

COME GESTIRE LE FASI DEL CICLO DI VITA DI UN DOCUMENTO?

Per gestire le fasi del ciclo di vita di un documento informatico risulta decisivo avvalersi dei seguenti strumenti:

1) Un Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi (regole tecniche protocollo informatico – DPCM 3.12.2013)
Manuale del Comune di Giulianova approvato con la DGC n. 222 del 15.12.2015 – disponibile su http://trasparenza.comune.giulianova.te.it

2) Un sistema di gestione documentale interoperabile con funzionalità di workflow documentale, Document & Content Management)
(Es. LEONARDO ver. 04 della TINN, applicativo Halley, applicativo Sicr@web di Maggioli, etc...)

IL SISTEMA DI PROTOCOLLO INFORMATICO SECONDO LE REGOLE TECNICHE DEL CAD

Il sistema di protocollo informatico oltre a garantire le “funzionalità minime” richieste dalla normativa, deve essere in grado di assicurare:

1) **Univoca identificazione ed autenticazione degli utenti**

2) **la protezione delle informazioni relative a ciascun utente nei confronti degli altri**

3) **la garanzia di accesso alle risorse esclusivamente agli utenti abilitati**

4) **la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione**

IL SISTEMA DI GESTIONE DOCUMENTALE SECONDO LE REGOLE TECNICHE DEL CAD

Il sistema di gestione documentale deve garantire:

A) l'individuazione di tutti i documenti in entrata e in uscita

B) l'attribuzione ad ogni documento ricevuto o spedito di una specifica e univoca identificazione (Art. 53 del D.P.R. 28 dicembre 2000, n. 445)

C) la data e l'ora di invio/ricezione dei documenti

D) l'ordine cronologico dei documenti ricevuti e spediti

E) l'immodificabilità dei documenti registrati a protocollo

F) la riservatezza delle informazioni contenute nei documenti

G) la certezza, qualora necessaria, dell'avvenuto recapito dei documenti inviati (gestione delle ricevute di accettazione e consegna previste dal sistema PEC)

H) l'usabilità delle procedure e degli strumenti informatici utilizzati

VALORE GIURIDICO DEL DOCUMENTO INFORMATICO

Un documento informatico è giuridicamente rilevante quando:

- **Soddisfa la forma scritta (formato del documento)**
- **È imputabile con certezza alla volontà del suo autore (firma digitale)**

Il documento informatico che soddisfa le suddette proprietà è conservabile (a norma) al fine di preservare nel tempo il suo valore giuridico e legale

FORMAZIONE DEL DOCUMENTO INFORMATICO

La formazione del documento informatico è fondamentale in quanto solo una corretta formazione del documento è in grado di garantirne un'efficace gestione e una valida conservazione a lungo termine
(Formazione del documento informatico: DPCM 14 novembre 2014 – in vigore dall'11.02.2015)

In fase di formazione del documento dovrà essere garantita la sua integrità, immodificabilità, identificazione, classificazione, fascicolazione, leggibilità, memorizzazione e conservazione in conformità alle norme e alle regole tecniche (direttive attuative) del CAD.

IMMODIFICABILITA' ED INTEGRITA' DEL DOCUMENTO

Le caratteristiche di immodificabilità e di integrità di un documento informatico sono determinate da una o più delle seguenti operazioni:

1) **la sottoscrizione con firma digitale**

2) **l'apposizione di una data certa (riferimento temporale) acquisita con la segnatura di protocollo, la marca temporale, la procedura di conservazione, la trasmissione via PEC (art. 41 del DPCM 22 febbraio 2013)**

3) **il trasferimento a soggetti terzi con PEC con ricevuta completa (accettazione e consegna)**

4) **la memorizzazione su sistemi di gestione documentale (es. Leonardo) che dovrebbero adottare idonee politiche di sicurezza**

5) **il versamento ad un sistema di conservazione a norma**

AUTENTICITÀ DEL DOCUMENTO INFORMATICO CON LA FIRMA ELETTRONICA

Un documento informatico è giuridicamente rilevante quando, oltre a soddisfare la forma scritta, soddisfa anche l'autenticità

Un documento è autentico quando è riconducibile con certezza alla volontà del suo autore

l'autenticità di un documento viene garantita attraverso l'apposizione della firma informatica

La firma informatica assicura il legame tra il firmatario e il documento informatico

FORMATI DEL DOCUMENTO INFORMATICO (1/3)

La forma scritta è determinata dai formati elettronici adeguati con i quali rappresentare documenti informatici (approfondimenti Allegato 2 DPCM 3 dicembre 2013 - Regole tecniche per il protocollo informatico):

- **Devono essere aperti, standard e documentati**
- **Non devono poter contenere macro istruzioni**
- **Devono essere affidabili, accurati e usabili**
- **Devono essere indipendenti dalle piattaforme tecnologiche (Android, iOS PC, Microsoft Windows, Linux OS, etc.) - GARANZIA DI LEGGIBILITA'**

FORMATI DEL DOCUMENTO INFORMATICO (2/3)

Formati aperti ammessi (v. par. 8.5 Manuale di gestione del Comune di Giulianova -approvato con DGC n. 222 del 15.12.2015):

- **PDF-PDF/A (Portable Document Format): il PDF/A è pienamente statico (.pdf)**
- **OOXML (Office Open XML) formato aperto dei documenti Microsoft che supportano lo standard ISO/IEC 29500 dalla versione Microsoft Office 2010 in poi (.docx, .xlsx, .pptx)**
- **ODF (Open Document Format) formato OASIS Open Document Format for Office Applications (es. Libre Office, Open Office per la produzione dei dormati .odt, .ods .odg, .odp)**
- **XML (Extensible Markup Language) formato fatture elettroniche (.xml)**
- **TXT (Text file) File di testo in ASCII o Unicode (.txt)**
- **Messaggi e-mail formato standard RFC 2822/MIME (.eml)**

FORMATI DEL DOCUMENTO INFORMATICO (3/3)

- **TIFF (Tagged Image File Format), formato per le immagini (con compressione dati senza perdita - “lossless”) in versione compressa o non compressa (.tiff)**
- **JPEG (Joint Photographic Experts Group): formato compresso (compressione dati con perdita - “lossy”) per le immagini (.jpeg o .jpg)**
- **PNG (Portable Network Graphics) per le immagini (compressione “lossless”) (.png)**
- **OGG per i file audio (.ogg)**
- **Theora per file video (.ogv)**
- **Epub per i libri digitali (.epub)**

FIRME INFORMATICHE

Sono 5 + 1:

1) Firma elettronica

2) Firma elettronica avanzata

3) Firma qualificata

4) Firma digitale

5) Sigilli elettronici

+ “l’acquisizione digitale di sottoscrizione autografa, quest’ultima apposta dal titolare davanti ad un pubblico ufficiale che ne accerta l’identità personale” art. 25, c. 2, del CAD

FIRMA ELETTRONICA ("DEBOLE" O "LEGGERA")

Firma elettronica (Regolamento eIDAS, art 3, p.to 10): "dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare"

Es.: Accesso all'e-mail mediante le credenziali (utente e password)

Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità

(Art. 21, c. 1 del CAD)

FIRMA ELETTRONICA AVANZATA (FIRMA DIGITALE)

Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche del CAD (DPCM 22.02.2013) è giuridicamente rilevante ed ha l'efficacia probatoria prevista dal codice civile.

L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria (inversione dell'onere della prova). (art. 21, c. 2 del CAD)

FIRMA DIGITALE: DEFINIZIONE

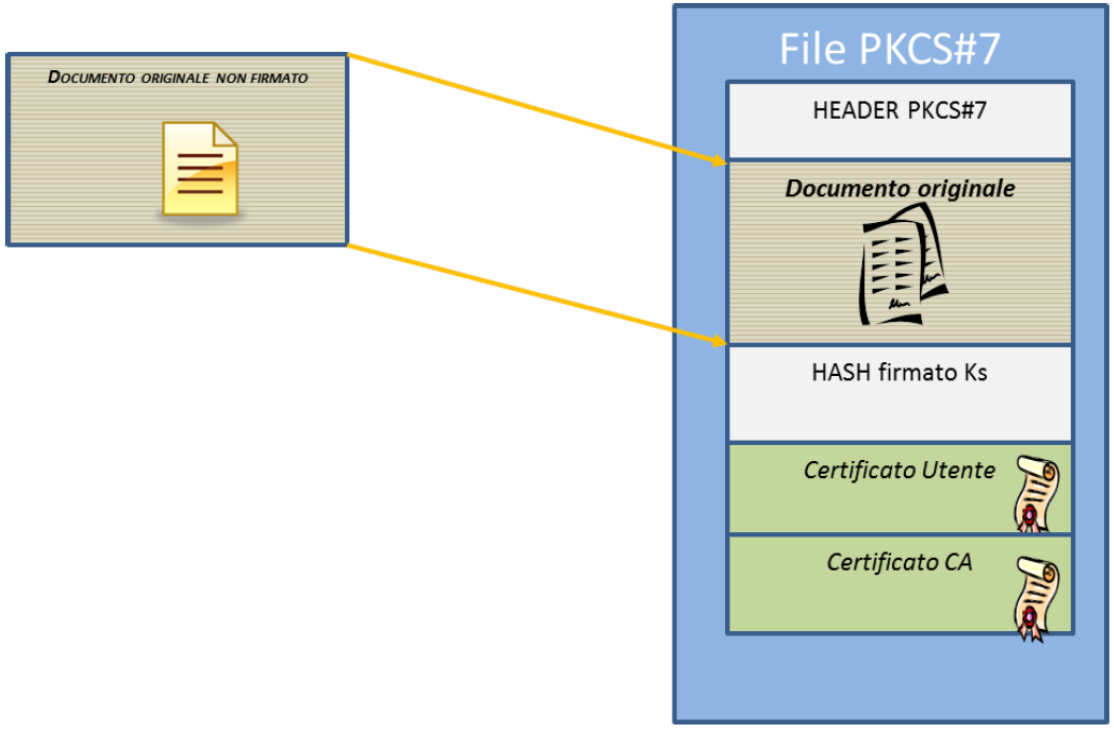
La firma digitale (Definizione del CAD): un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici

Valore probatorio: l'efficacia probatoria è la stessa della scrittura privata ed integra in modo sostanziale la forma scritta del documento

Esempi di dispositivi per l'apposizione della firma: Lettore Smartcard e Token usb (chiavetta usb)

IN COSA CONSISTE LA FIRMA DIGITALE

La firma digitale consiste nella creazione di un file c.d. "busta crittografica" contenente: il documento originale, l'evidenza informatica della firma e il certificato utente del sottoscrittore che a sua volta contiene la chiave (pubblica) per la verifica della stessa



L'autenticità del certificato è garantita da un'Autorità di certificazione (CA) mediante certificatori accreditati (Art. 29 del CAD)

COME GENERARE UNA FIRMA GITALE

E’ necessario dotarsi di un “Kit di firma digitale”composto da:

- **un dispositivo sicuro di generazione delle firme: lettore smartcard o token USB**
- **un PC per poter utilizzare uno specifico software (es. Dike, File Protector, etc.), quest’ultimo indispensabile per utilizzare il dispositivo di generazione firme e/o verificare una firma digitale CadES apposta su un documento**

TIPI DI SOTTOSCRIZIONE DIGITALE

La sottoscrizione elettronica di un documento mediante la firma digitale è un processo informatico basato su algoritmi di crittografia a chiave asimmettrica (o pubblica) costituita da una chiave privata, (esclusiva del titolare), e chiave pubblica (distribuita ai destinatari)

Gli standard europei prevedono tre tipi di sottoscrizione digitale:

1) **Sottoscrizione di tipo CadES (file .p7m) leggibile solo con software Dike, File Protector**

2) **Sottoscrizione di tipo PadES (file .pdf) leggibile direttamente con Acrobat Reader**

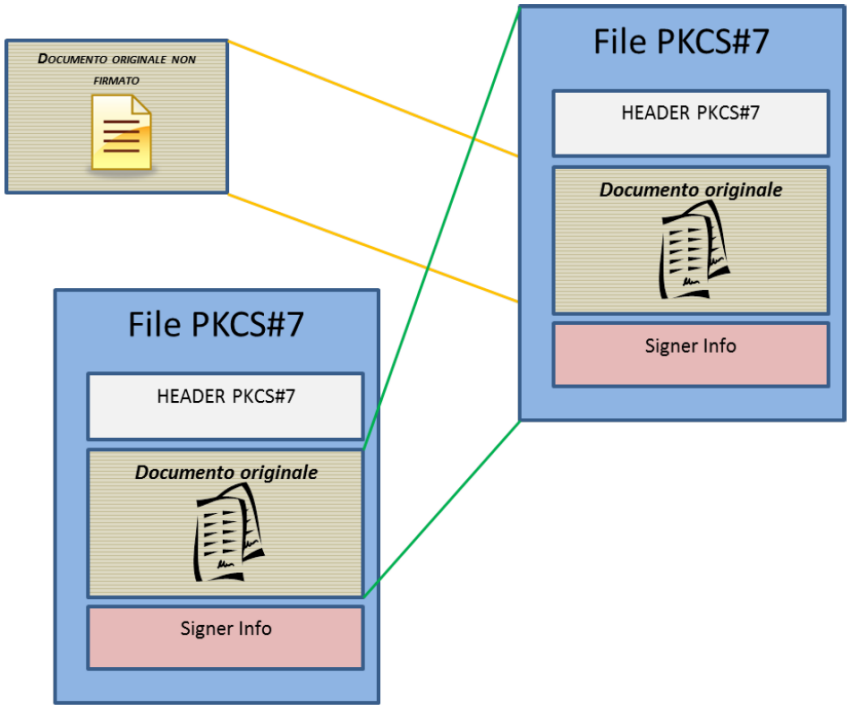
3) **Sottoscrizione di tipo XadES nuovo standard di firma basato sul XML**

CadES: LIMITI E FIRME MULTIPLE

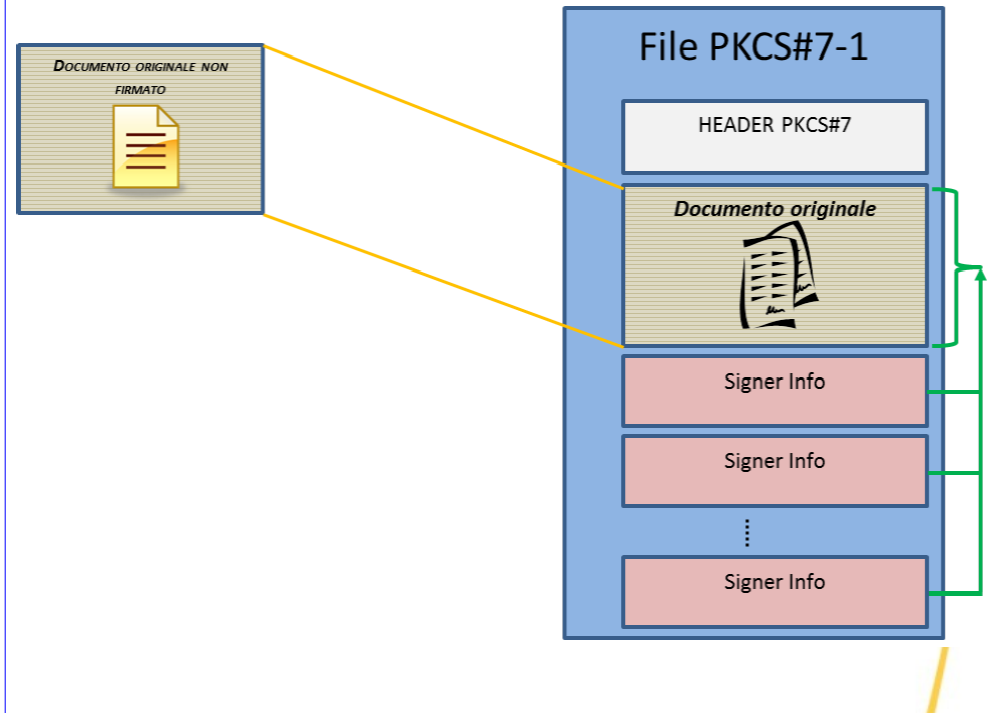
Il formato CadES presenta i seguenti limiti:

- **non consente di visualizzare il documento .p7m in modo agevole senza l'utilizzo di un software specifico (come Dike, File Protector, etc.)**
- **non è possibile gestire diverse versioni di uno stesso documento all'interno della busta crittografica in quanto renderebbe la firma invalida**

Firme a matrioska (controfirma) CaDES



Firme congiunte CadES

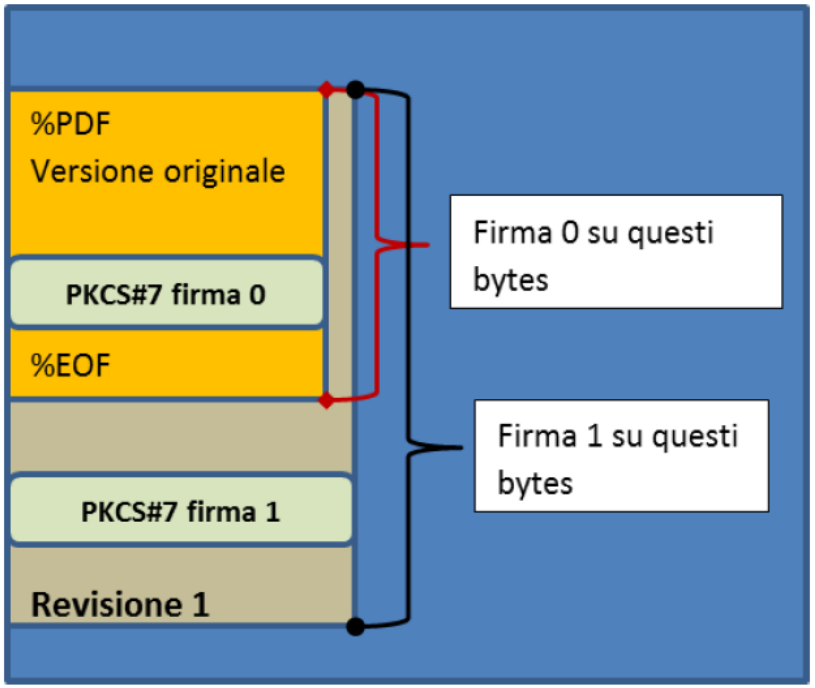


PadES: CARATTERISTICHE E FIRME MULTIPLE

La “firma PDF” ha delle caratteristiche integrative rispetto al CadES:

- **è accessibile immediatamente tramite i comuni Reader**
- **consente di gestire diverse versioni del documento (funzione versioning) senza invalidare le firme digitali apposte**
- **consente di collocare fisicamente la firma digitale in un preciso punto del documento**

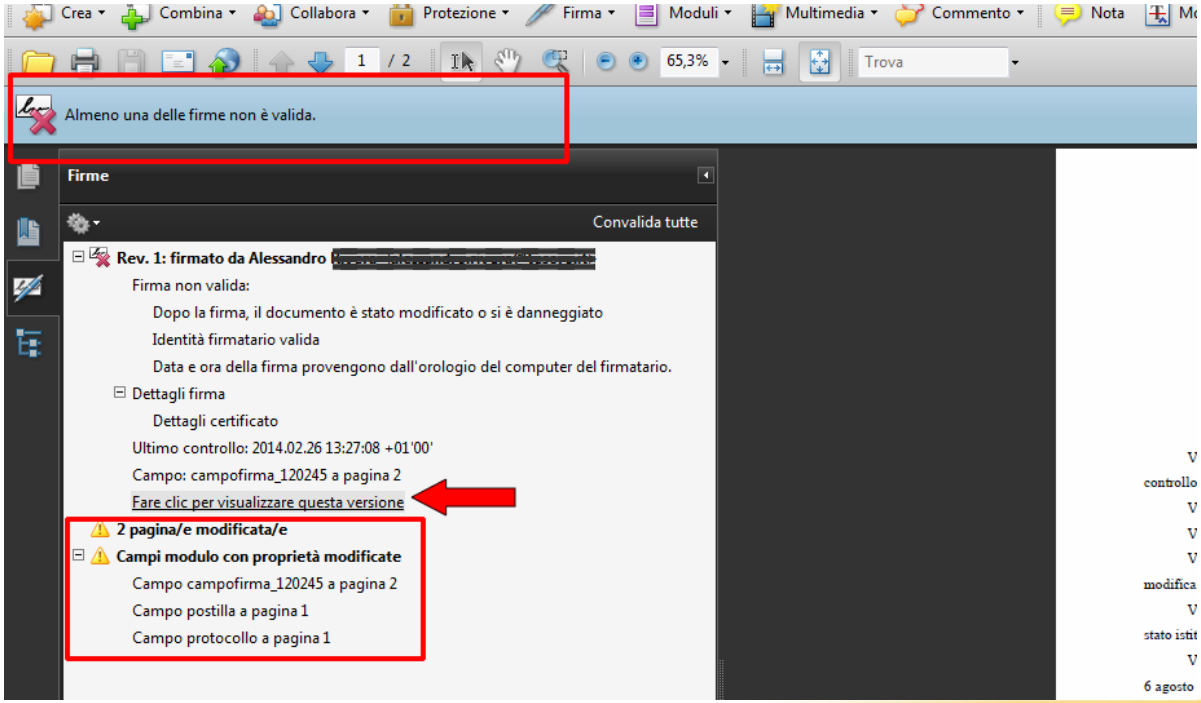
Firme PadES di versioni del documento



PadES: CARATTERISTICHE E FIRME MULTIPLE

Se nella busta PAdES è presente ed è accessibile anche la versione non modificata del documento, essa conserva piena efficacia giuridica coerentemente con quanto previsto dalle "regole tecniche sulle firme elettroniche avanzate" (D.P.C.M. del 22 febbraio 2013)

Questa modalità di gestire le versioni del documento PDF, consente di risolvere il problema della segnatura di protocollo dell'art. 55 del D.P.R. 445/2000



APPOSIZIONE DI UNA FIRMA DIGITALE

Apporre una firma digitale ad un documento significa:

1) **applicare al documento una funzione matematica (c.d. "hash") che trasforma il relativo contenuto (o testo) in una stringa binaria o esadecimale a lunghezza fissa, dalla quale si ottiene l'impronta digitale (o message digest) ovvero un file di dimensione fissa che 'sintetizza' le informazioni contenute nel documento (con il formato standard ISO/IEC 10118-3:2004)**

2) **codificare l'impronta con la chiave privata del titolare (evidenza informatica della firma), basata su un certificato qualificato e realizzata mediante un dispositivo sicuro (token usb, lettore smartcard, etc.) per la creazione della firma;**

3) **allegare al documento la firma così ottenuta (file busta crittografica)**

Un documento sottoscritto con firma digitale ha piena efficacia giuridica

LA VERIFICA DI UNA FIRMA DIGITALE

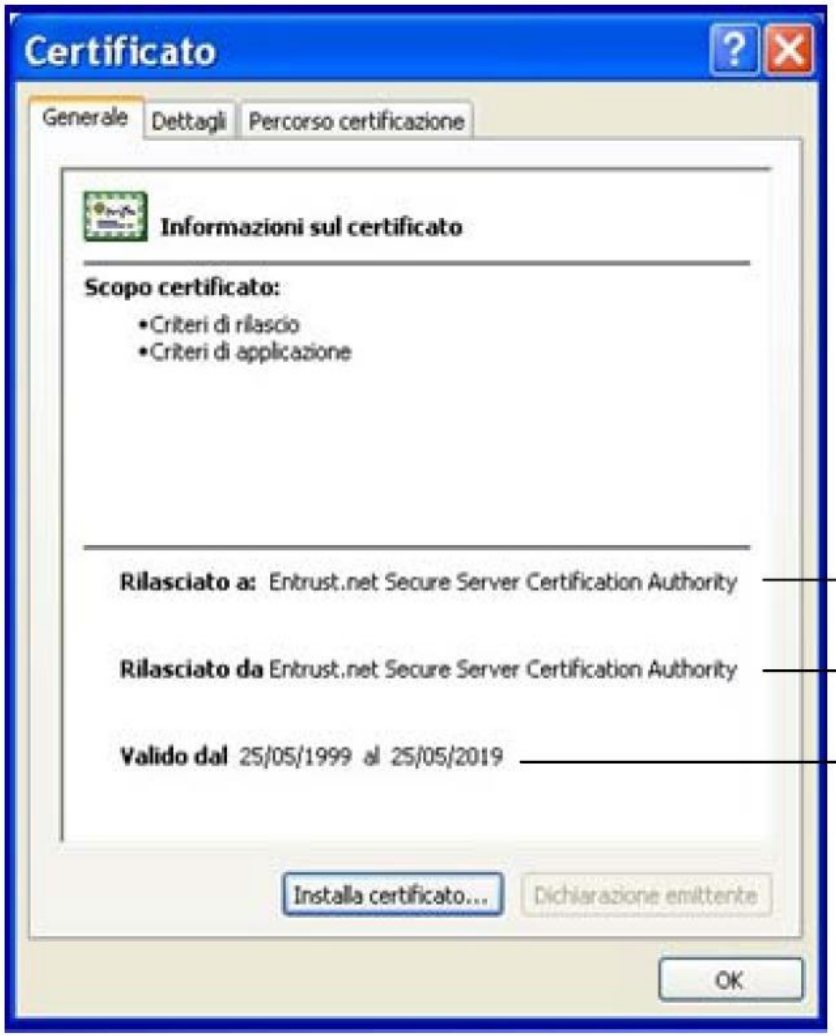
La verifica della firma digitale apposta su un documento viene effettuata mediante le seguenti fasi:

1) **utilizzare la chiave pubblica del mittente (titolare della firma) ottenendo l'impronta digitale (message digest) generata dal mittente**

2) **confrontare l'impronta digitale del mittente (di cui al punto 1.) con quella che si ottiene applicando la stessa funzione di hash pubblica al documento medesimo**

3) **se le due impronte ottenute sono uguali il documento risulta integro e imputabile al sottoscrittore**

ESEMPIO DI CERTIFICATO DIGITALE



ATTRIBUTI DEL CERTIFICATO

Di chi è il certificato

CA che ha rilasciato il certificato

Periodo di validità del certificato.
Per motivi di sicurezza la validità di un certificato non può essere superiore a 3 anni.

VALIDITA' DI UNA FIRMA DIGITALE

Il certificato del sottoscrittore ha un periodo di validità in genere di 3 anni

Il certificato può anche essere revocato o sospeso prima della naturale scadenza

La revoca sopravviene in diversi casi:
1) In caso di guasto, sottrazione o smarrimento del dispositivo di firma

2) quando il titolare ha perso il controllo esclusivo del dispositivo

3) quando il titolare abbia il ragionevole dubbio che i certificati qualificati possano essere utilizzati da altri

L'apposizione ad un documento informatico di una firma digitale con certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione (art. 21, c. 3 del CAD)

Le firme digitali con certificato scaduto, revocato o sospeso sono valide se alle stesse e' associabile un riferimento temporale opponibile ai terzi che collochi la generazione di dette firme rispettivamente in un momento precedente alla scadenza, revoca o sospensione del suddetto certificato (art. 62 DPCM 22 febbraio 2013)

"Non possiamo pretendere che le cose cambino se continuiamo a fare le stesse cose"

A. Einstein

Grazie per l'attenzione!