ASL CN 2

ROSSINI TIZIANA

RESPONSABILE DELLA GESTIONE DOCUMENTALE

L'AMMINISTRAZIONE DIGITALE

YES, WE CAN

PARTE I^

- IL DOCUMENTO INFORMATICO
- LA FIRMA DIGITALE

OBAMA nel 2013, parlando alla Nazione disse:

Non possiamo gestire il futuro con una Pubblica Amministrazione del passato

E' difficile affrontare le nuove sfide sociali con una Pubblica Amministrazione pensata e cresciuta nel passato.

Se questo è vero negli Stati Uniti è tanto più vero in Italia!

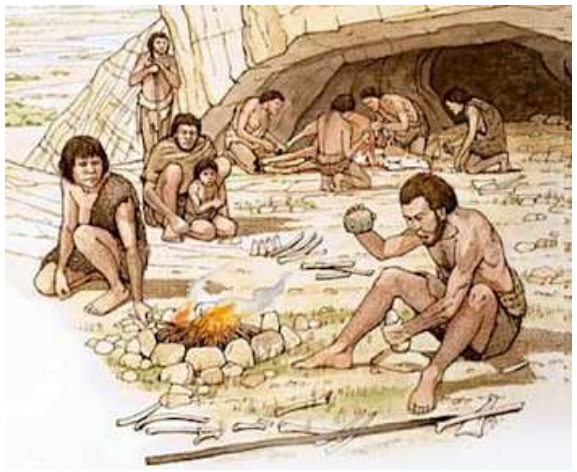
occorre INNOVAZIONE

La civiltà di un paese si misura dal grado di digitalizzazione raggiunto

Tanto minore è la digitalizzazione tanto maggiore è la corruzione

L'amministrazione digitale

COME È



COME DOVREBBE ESSERE

OGGI NON ESISTE SANITÀ, SCUOLA, LAVORO GIUSTIZIA SE NON SONO ANCHE DIGITALI

In Italia esiste un problema di EMERGENZA DIGITALE, di cui non si ha coscienza

Luca Attias

a FORUM PA 2015

I NUMERI DELLA NOSTRA INEFFICIENZA

VOCE	ITALIA	NOTE
CED	11.000	200.000 in Francia decine di migliaia in UK e USA
APPLICAZIONI	11.000	Ogni P.A. - per la medesima funzione - ha il suo applicativo, non interoperativo
N. AMMINISTRAZIONI	10.000	Molte inutili
CENTRALI DI ACQUISTO	30.000	Dovrebbe esserci solo CONSIP

L'Italia è solo al 69° posto tra i paesi meno corrotti (almeno 30 posizioni dopo la Spagna e il Portogallo)

Siamo tra i paesi che spendono di più nel digitale... ma il nostro livello di informatizzazione è pari a quello di Bulgaria e Romania

Le cause di tanta inefficienza e le soluzioni:

CARENZA DI CONOSCENZE INFORMATICHE DA PARTE DI CHI GESTISCE LA COSA PUBBLICA
(politici e dirigenti)

ENDORSEMENT:
sostegno politico

MANCANZA DI COINVOLGIMENTO DEGLI UTENTI, portatori di competenze e di soluzioni
(c.d. sussidiarietà orizzontale)

ENGAGEMENT:
coinvolgimento dei cittadini

CARENZA DI COMPETENZE DEI DIPENDENTI PUBBLICI

EMPOWERMENT:
crescita dei dipendenti pubblici

A monte occorre dare soluzione allo

TSUNAMI DI ADEMPIMENTI NORMATIVI

Troppe norme?

- Leggi nazionali
- Usi e prassi (anche giurisprudenziali)
- La legislazione europea ed internazionale
- I provvedimenti del garante e dell'Ag.I.D.
- Standard tecnici e le linee guida

Quale applicare?

Nella somma corruzione della cosa pubblica, infinito il numero di leggi.

PUBLIO CORNELIO TACITO

La complessità delle regole determina la non attuazione delle stesse !!!

Quante leggi ci sono in Italia ?

75.000 (secondo Normattiva)	ITALIA
160.000 (secondo Sabino Cassese)	ITALIA
7.000	FRANCIA
5.500	GERMANIA
3.000	GRAN BRETAGNA

Le leggi emanate spesso sono illeggibili
… art. 1294 comma 89 ter

Il numero degli avvocati di Roma è lo stesso degli avvocati di tutta Francia

Quanti conoscono l'esistenza del C.A.D.?

IL CAD era al momento della sua emanazione considerata una norma AVANZATA ma è rimasta lettera morta.
Molteplici le ragioni e ne vedremo alcune ma sicuramente la sua complessità e la carenza di provvedimenti attuativi hanno relegato gli auspici in essa contenuti all'interno di una gabbia.

C'è bisogno di DENORMAZIONE

LE NORME COMPLESSE VANNO SOSTITUITE CON NORME PIÙ SEMPLICI

NON CI PUÒ ESSERE UNA REGOLA PER TUTTO

ALTRI PAESI

I PROCESSI

ITALIA

In Italia si sono create soluzioni digitali più complesse di quelle non digitali!!

Per riprodurre in digitale la RICEVUTA DI RITORNO della Raccomandata postale si è inventata la P.E.C. (Posta Elettronica Certificata) che esiste solo nel nostro Paese ed in Tanzania.

Il FASCICOLO SANITARIO ELETTRONICO è gestito a livello regionale e cambiando Regione le informazioni in esso contenute non transitano da una Regione ad un'altra.

OCCORRE SEMPLIFICARE!

GLI UTENTI UTILIZZANO I SERVIZI NON SE REGOLATI DA NORME MA SE FUNZIONALI

IL 90% DELLA POPOLAZIONE USA
WHATSAPP e non si chiede dove sono i server,
ma solo ne apprezza la semplicità e funzionalità.

OCCORRE FARE I.T. A LIVELLO CENTRALE E AD UN LIVELLO ACCETTABILE

LA SFIDA È DISEGNARE SERVIZI COSÌ BEN FATTI CHE TUTTI LI VORRANNO UTILIZZARE,

come hanno già fatto Uber, Tripadvisor, car2go, ecc.

IL GOVERNO INGLESE HA DA ANNI UN UNICO SITO DELLA P.A.

Bisogna arrivare qui!

Il governo inglese ha introdotto nel 2012 lo standard **DIGITAL BY DEFAULT** nella Pubblica Amministrazione.
Il digital by default è il principio in base al quale i servizi pubblici debbono essere erogati prioritariamente in modalità digitale

E qui stiamo andando!

ATTI PROGRAMMATORI EUROPEI

L'Agenda Digitale Europea (A.D.E.)

è una delle **sette** strategie promosse dall'UE per raggiungere i traguardi di crescita economica sostenibile programmati per il **2020.**

Con essa gli Stati membri si impegnano a sfruttare il potenziale economico e sociale delle TIC (Tecnologie dell'informazione e della comunicazione), e in special modo di INTERNET

L'Europa ha assegnato all'Agenda un fondo di **1,1 miliardi di euro**: **l'Italia** ce ne metterà altri **2** per rispettare la propria tabella di marcia.

FINE CRESCITA :

- **in INNOVAZIONE**
- **ECONOMICA**
- **in COMPETITIVITÀ**
- **di OCCUPAZIONE**

MEZZI:

- **ALFABETIZZAZIONE INFORMATICA**
- **CREAZIONE DI NUOVE FIGURE PROFESSIONALI**
- **DIGITALIZZAZIONE DELLA PUBBLICA AMMINISTRAZIONE**

BROADBAND (2020 TARGET)

Citizens covered by basic broadband — **100%**

Broadband coverage of over 30 Mbit/s — **100%**

Use of connection of more than 100 Mbit/s — **50%**

DIGITAL INCLUSION (2015 TARGET)

Residents who regularly use the internet — **75%**

Vulnerable groups who regularly use the internet — **60%**

Maximum percentage of population who have never used the internet — **15%**

SERVICES (2015 TARGET)

Population that makes purchases on the internet — **50%**

Small and medium-sized companies that buy and sell online — **33%**

Citizens who use the public authorities' digital services — **50%**

LA BANDA LARGA, per tutti, o quasi

Nel linguaggio comune per **banda larga** si intende una connessione a Internet molto veloce.

Detto più tecnicamente, la banda larga è la trasmissione e ricezione di dati informativi inviati in grande quantità attraverso una linea che sfrutta, appunto, una banda larga, cioè superiore rispetto alla banda stretta su cui viaggiavano i vecchi sistemi di telecomunicazione.

La velocità di trasmissione dei dati aumenterà a 100 MB/s ovunque sia possibile, per salire ad almeno 30 MB nelle aree più marginali

Europa dixit

non ci sono più costi aggiuntivi di roaming per chi accede a Internet dal proprio smartphone trovandosi in uno Stato Estero dell'Unione.

L'obiettivo è realizzare un ***mercato unico delle telecomunicazioni****.*

Con questa riforma le tariffe delle telefonate e del traffico internet dovranno essere uguali in tutti i Paesi Ue. I provider internet non potranno dare priorità a particolari tipi di traffico (ad esempio lo streaming video, per ottenerne guadagni) per ottenerne guadagni

La cultura digitale

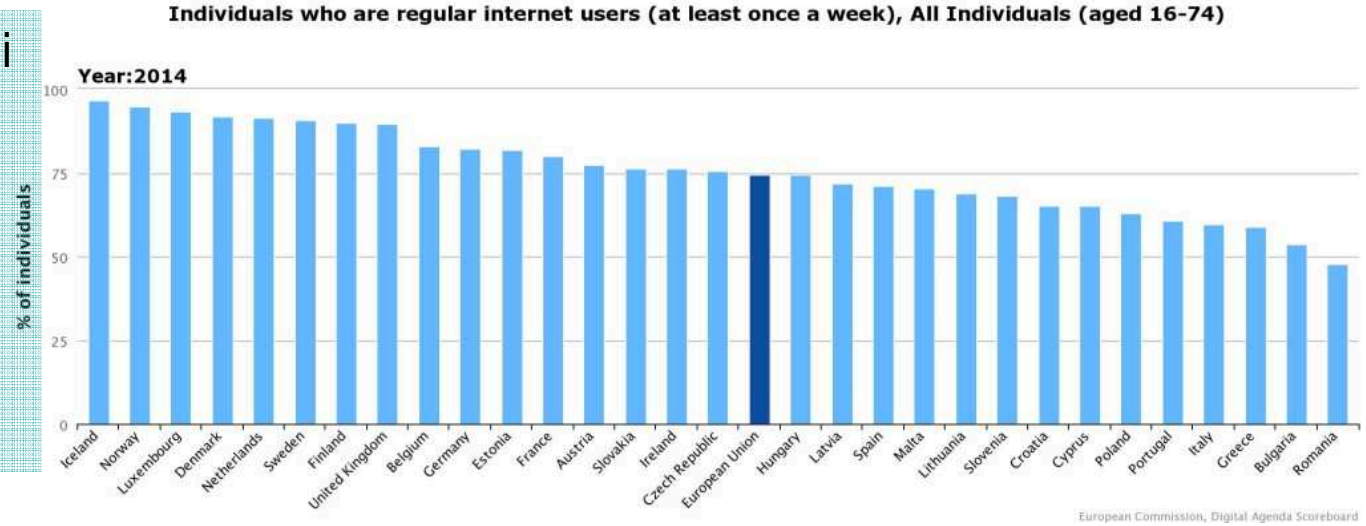
Obiettivo dell'Agenda Digitale a cui prestare particolare attenzione: la **diffusione di una cultura digitale** tra i cittadini e gli imprenditori delle piccole/medie imprese, per formare nuove competenze.

OBIETTIVO 2015: dimezzare la percentuale di cittadini europei che non hanno mai usato Internet **dal 30% al 15%.**

Percentuale media di utilizzo regolare di **Internet:**

- 74% in Europa
- 59% in Italia

davanti a
Grecia
Bulgaria
Romania



<u>Internet come mezzo di contatto con la PA (dati 2014)</u>

- il 36% gli italiani
- il 58% gli europei.

Le aziende italiane che vendono in **e-commerce** sono appena un terzo di quelle europee

Regolamento 910/2014/UE del 17 settembre 2014
noto come

Regolamento eIDAS –

electronic identification and trust services for electronic transactions in the internal market

Con obbligo di adeguamento dal 1 luglio 2016

Fine: creando le condizioni adatte per il **MERCATO UNICO DIGITALE**, attraverso il riconoscimento reciproco transfrontaliero di funzioni essenziali quali **l'identificazione elettronica**, i **documenti elettronici**, le **firme elettroniche** e i **servizi elettronici di recapito**, nonché per l'interoperabilità dei **servizi di *eGovernment*** in tutta l'Unione europea

favorire e incentivare la nascita di un quadro tecnico-giuridico unico, omogeneo e interoperabile a livello europeo, relativamente ai cosiddetti Trusted service (servizi fiduciari).

Si tratta di servizi erogati da certificatori rispetto ai quali la fiducia è di fondamentale importanza: firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, documenti elettronici, nonché servizi di raccomandata elettronica e servizi di certificazione per Autenticazione web; tutti servizi che si richiede vengano realizzati da terze parti fidate che siano vigilate e controllate dagli Stati membri, al fine di garantire certezza e fiducia al mercato elettronico interno.

ATTI PROGRAMMATORI ITALIANI

il **PIANO E-GOV 2012,** lanciato nel **gennaio 2009** dal Ministro per la Pubblica Amministrazione e Innovazione Renato Brunetta.

Con esso si sono definiti i settori strategici e un insieme di progetti di innovazione digitale da perseguire entro il termine temporale del 2012

Principali interventi

SALUTE

- **CERTIFICATI MEDICI ON LINE**
- **FASCICOLO SANITARIO ELETTRONICO**
- **RICETTA DIGITALE**

SCUOLA

- SCUOLA MIA
- INNOVA SCUOLA
- SCUOLE IN Wi.Fi.
- ICT4UNIVERSITY

GIUSTIZIA

- PIANO STRAORDINARIO PER LA GIUSTIZIA DIGITALE

RAPPORTO CITTADINO P.A.

- PEC
- VIVIFACILE
- LINEA AMICA
- RETI AMICHE

ATTI PROGRAMMATORI ITALIANI (dopo l'ADE)

L'AGENDA DIGITALE ITALIANA, elaborata dall'Italia nel quadro dell'Agenda Digitale Europea (ADE) ed approvata il **7 aprile 2014**.

Tale documento individua le priorità e le modalità di intervento, nonché le azioni da compiere e da misurare sulla base di specifici indicatori, in linea con gli indicatori dell'ADE.

i **piani nazionali** denominati:

STRATEGIA NAZIONALE PER LA BANDA ULTRA LARGA

STRATEGIA PER LA CRESCITA DIGITALE 2014-2020

approvati dal Consiglio dei Ministri il **3 marzo 2015** in coerenza con gli obiettivi dell'ADE.

Progetti previsti dall'Agenda Digitale Italiana

AREE DI INTERVENTO PRINCIPALI

- Infrastrutture e Architetture
- Pubblica Amministrazione
- Competenze Digitali
- Open Data
- Città e Comunità Intelligenti
- Innovazione del Mercato
- Progetti e Programmi Internazionali

L'AGENZIA PER L'ITALIA DIGITALE

(istituita con decreto Sviluppo del 15 giugno 2012)

è il soggetto incaricato di verificare il raggiungimento degli obiettivi, sulla base di specifici indicatori e di aggiornare il Piano per la crescita digitale.

LE AUTORITA' PER L'INFORMATICA

- **Autorita' per l'Informatica nelle Pubbliche Amministrazioni (AIPA),** istituita con il D.Lgs. n. 39 del 12 febbraio **1993**

- **Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA),** istituita con il d.lgs n. 196 del 30 giugno **2003**

- **DigitPA,** già CNIPA ex D.lgs. n. 177 del 1º dicembre **2009**

- **Agenzia per l'Italia Digitale (AgID)** D.L. n. 83 del 22 giugno **2012**

LA NUOVA PUBBLICA AMMNISTRAZIONE, anzi la RIVOLUZIONE della P.A. o anche la P.A. a portata di CLICK

Attraverso il **Servizio Pubblico di Identità Digitale (SPID)** ogni cittadino avrà un accesso personale a servizi in rete basati sulla tecnologia CLOUD: i dati relativi alle proprie pratiche saranno cioè accessibili da qualsiasi computer connesso a Internet. La piattaforma di accesso alla PA, agli appalti pubblici, alla propria cartella clinica elettronica, alle scuole, sarà unica per tutti i servizi e ha già un nome: **ITALIA LOGIN**.

Tra qualche anno non esisteranno più sportelli fisici ma solo sportelli virtuali, scadenze e avvisi arriveranno direttamente sul proprio pc e i pagamenti si potranno fare ON LINE.

Ma non bisogna aspettare il 2020 per vedere i cambiamenti previsti dall'Agenda Digitale: ***il processo di digitalizzazione è già in corso****, basti pensare agli* ***OPEN DATA, alla fatturazione elettronica, alla ricetta dematerializzata, ecc.***

GLI OPEN DATA = dati aperti

Il **24 aprile 2015** sono state emanate le Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico

I dati aperti sono dati che possono essere **liberamente e gratuitamente** *utilizzati, riutilizzati e ridistribuiti da chiunque (anche a fini commerciali).*

Gli Open Data sono un elemento centrale nelle strategie di e-Gov per favorire:
trasparenza e partecipazione

La Pubblica Amministrazione produce in generale due tipi di dati:

- **dati gestionali, relativi ai processi organizzativi e di servizio**
- **dati di tipo statistico, descrittivi dei fenomeni che gestisce**

Essi devono essere resi accessibili e fruibili, fermo restando il rispetto della normativa in materia di protezione dei dati personali *(tipicamente non devono essere riferibili a singole persone)*.

LA CONDIVISIONE DEI DATI

Le pubbliche amministrazioni devono realizzare i **servizi in rete** al fine di migliorare e rendere più efficiente il proprio operato

A tal fine devono garantire ad altre PP.AA. l'accesso telematico a dati, documenti e procedimenti e il riutilizzo degli stessi.

La condivisione di dati riguarda solitamente **contesti ristretti** (PA o enti con finalità pubbliche) e agisce sulla base di un **determinato scopo** di condivisione e su un insieme di **dati specifici**, inclusi **anche i dati personali**.

Dal 31 marzo 2015 è esteso a tutte le Pubbliche Amministrazioni l'obbligo di emettere, trasmettere, gestire e conservare le fatture esclusivamente in formato elettronico, secondo la normativa vigente.

La **fattura elettronica** è un documento in formato digitale la cui autenticità e integrità sono garantite:
•dalla presenza della firma elettronica di chi emette la fattura;
•dalla trasmissione della fattura ad uno specifico Sistema di Interscambio (SDI).

Un **Sistema di Interscambio** è la piattaforma che:
•trasmette la fattura elettronica dal fornitore alla Pubblica Amministrazione;
•trasmette le notifiche relative alle attività svolte alla Pubblica Amministrazione e al fornitore;
•consente al Ministero dell'Economia e delle Finanze (MEF) il Monitoraggio della Finanza Pubblica.

Le caratteristiche tecniche di un file di fattura elettronica sono regolamentate dagli standard FatturaPA, Agenzia delle Entrate.
Il 9 marzo 2015, il Dipartimento Finanze del Ministero dell' Economia e delle Finanze e il Dipartimento della Funzione Pubblica del Ministero per la pubblica amministrazione e semplificazione, hanno pubblicato una circolare interpretativa che definisce nel dettaglio le scadenze per il passaggio alla fatturazione elettronica delle diverse amministrazioni.

Piemonte, definito il piano per far arrivare la banda ultralarga in tutta la Regione

L'obiettivo è la copertura totale entro il 2018 secondo i criteri del Piano nazionale, ovvero copertura:
•ad almeno 100 mbps per l'85 % della popolazione
•ad almeno 30 mbps per il 100% della popolazione

Il piano illustrato il **18 aprile 2016** in Giunta dall'assessore alle Attività produttive

COSTO: 500 milioni di euro

300 milioni di finanziamento pubblico tramite i fondi europei, a cui se ne aggiungeranno almeno 200 di investimento privato.

il 2% della superficie, che comprende il 50% della popolazione, ricade in aree in cui gli operatori privati faranno investimenti diretti nei prossimi anni. **L'accordo quadro Stato-Regioni prevede che i finanziamenti pubblici vengano ammessi esclusivamente sulle aree marginali**

Ai bandi saranno chiamati a rispondere gli operatori che realizzeranno l'infrastruttura passiva e che l'avranno in **concessione per 25 anni**.

La ratio dell'intervento pubblico è quella di mettere in condizione ogni territorio di poter avere pari condizioni per lo sviluppo.

La crescita economica di un territorio va di pari passo con l'innovazione tecnologica, che è indissolubilmente legata all'accesso a Internet e ai servizi online.

QUADRO NORMATIVO

La disciplina sui documenti (analogici e digitali) della Pubblica Amministrazione è contenuta in un pluralità di norme che sotto diversi aspetti ne regolano la formazione, la gestione e la stessa distruzione.

L. 07/08/1990, n. 241

NUOVE NORME IN MATERIA DI PROCEDIMENTO AMMINISTRATIVO E DI DIRITTO DI ACCESSO AI DOCUMENTI AMMINISTRATIVI

D.P.R. 28/12/2000, n. 445

TESTO UNICO DELLE DISPOSIZIONI LEGISLATIVE E REGOLAMENTARI IN MATERIA DI DOCUMENTAZIONE AMMINISTRATIVA

D. lgs. 30/06/ 2003, n. 196

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

D. lgs. 22/01/2004, n. 42

CODICE DEI BENI CULTURALI E DEL PAESAGGIO

NORMA PRIMARIA Legge 59/97, c.d. "Bassanini":

"Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge" (art .15, comma 2)

Il digitale: una possibilità

L'Italia è stato il primo paese UE che, nel 1997, si è dotato di una legge sui documenti digitali.

La Bassanini 1 aveva come scopo semplificare la comunicazione tra pubbliche amministrazioni e tra pubblica amministrazione e cittadini.

Tra il 1997 e il 2005 sono state emanate diverse norme, che sono poi state riorganizzate nel **Codice dell'Amministrazione digitale**

D.Lgs. 07/03/2005, n. 82
CODICE DELL'AMMINISTRAZIONE DIGITALE (C.A.D.)

NEL 2005 È STATO EMANATO IL CAD.

aggiornato e integrato con il testo del NUOVO CAD (di cui al Decreto Legislativo n. 235/2010)

L'amministrazione digitale diventa il paradigma delle Amministrazioni moderne, che devono rispettare requisiti di:

- *Trasparenza ed accessibilità*
- *Semplificazione amministrativa*
- *Documenti "esclusivamente" e "nativamente" digitali*
- *Dati aperti*
- *Condivisione*
- *Erogazione servizi in rete*
- *Rispondenza alle istanze digitali dei cittadini e delle imprese*

Il digitale: un obbligo

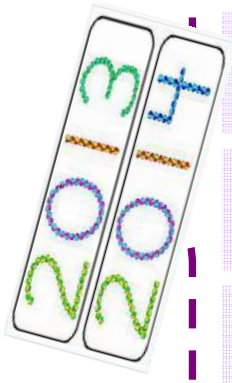
Avrebbe dovuto essere così...

Dopo il CAD

D.P.R. 11/02/2005
Regolamento recante disposizioni per l'utilizzo della **posta elettronica certificata (P.E.C.)**

D.M. 02/11/2005
Regole tecniche in materia di **posta elettronica certificata (P.E.C.)**

2005



D.P.C.M. 22/02/2013
Regole tecniche in materia di **firme elettroniche**

D.P.C.M. 21/03/2013
Individuazione di particolari tipologie di documenti analogici **originali unici**

D.P.C.M. 03/12/2013
Regole tecniche per il **protocollo informatico**

D.P.C.M. 03/12/2013
Regole tecniche in materia di **sistema di conservazione**

D.P.C.M. 13/11/2014
Regole tecniche in materia di **documenti informatici**

LA LEGGE MADIA **(Legge n. 124 del 7 agosto 2015)**

2015

Mancata attuazione del CAD, perché e per colpa di chi?

Negli ultimi 10 anni (tanti ne sono passati dall'adozione del CAD),
nonostante le promesse di una rapida digitalizzazione completa dell'attività amministrativa,
non si è assistito alla scomparsa della carta dagli uffici pubblici.

Perché?

- ✓ amministrazione ancora troppo legata ai vecchi *iter* burocratici tarati sugli strumenti analogici
- ✓ assenza di investimenti (in tecnologie e formazione)
- ✓ difficoltà organizzative
- ✓ norme di difficile interpretazione
- ✓ **mancanza dei decreti attuativi a cui le norme rimandavano**
- ✓ **mancanza di termini per lo stop al cartaceo.**

Per colpa di chi?

- ✓ GLI ORGANI POLITICO AMMINISTRATIVI
- ✓ I DIRIGENTI

(soggetti individuati nell'art. 12 del CAD)

Eppure sembra giunto il momento della svolta, perché

1. le **tecnologie**, come la posta elettronica certificata, sono notevolmente più diffuse (e utilizzate) sia dalle amministrazioni che dai loro utenti.
2. il **quadro normativo**, fatto di norme attuative e regole tecniche, appare ormai quasi completo
3. nei prossimi mesi scadranno i **termini** che le amministrazioni hanno per l'adeguamento ad importanti disposizioni in materia di dematerializzazione e servizi on line.
4. **il Governo ci crede ed ha investito risorse sulla digitalizzazione**

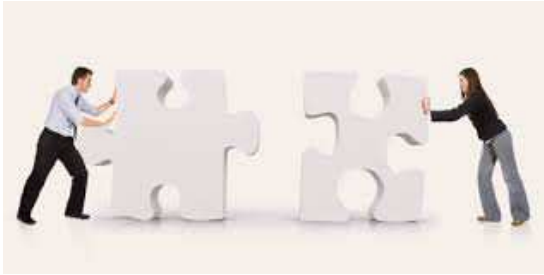
Il Governo intende usare i fondi europei 2014-2020 per tutti progetti digitali della pubblica amministrazione (Sanità, Scuola, Giustizia eccetera), **750 milioni di euro** su un totale di 4,6 miliardi di euro.

CHE COSA SERVE ?

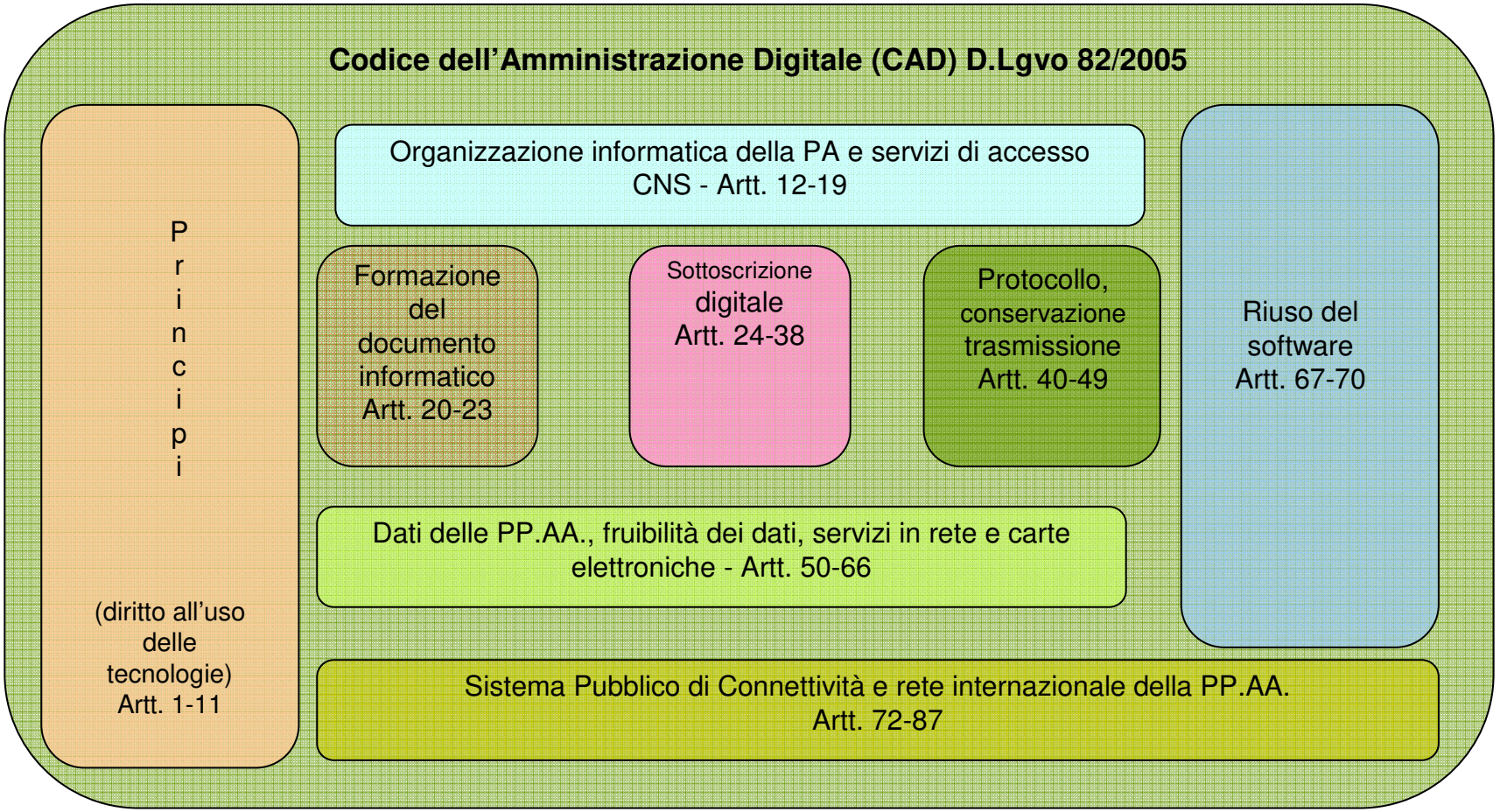
Un percorso di trasformazione strutturato su tre principali filoni:

CULTURALE

ORGANIZZATIVO

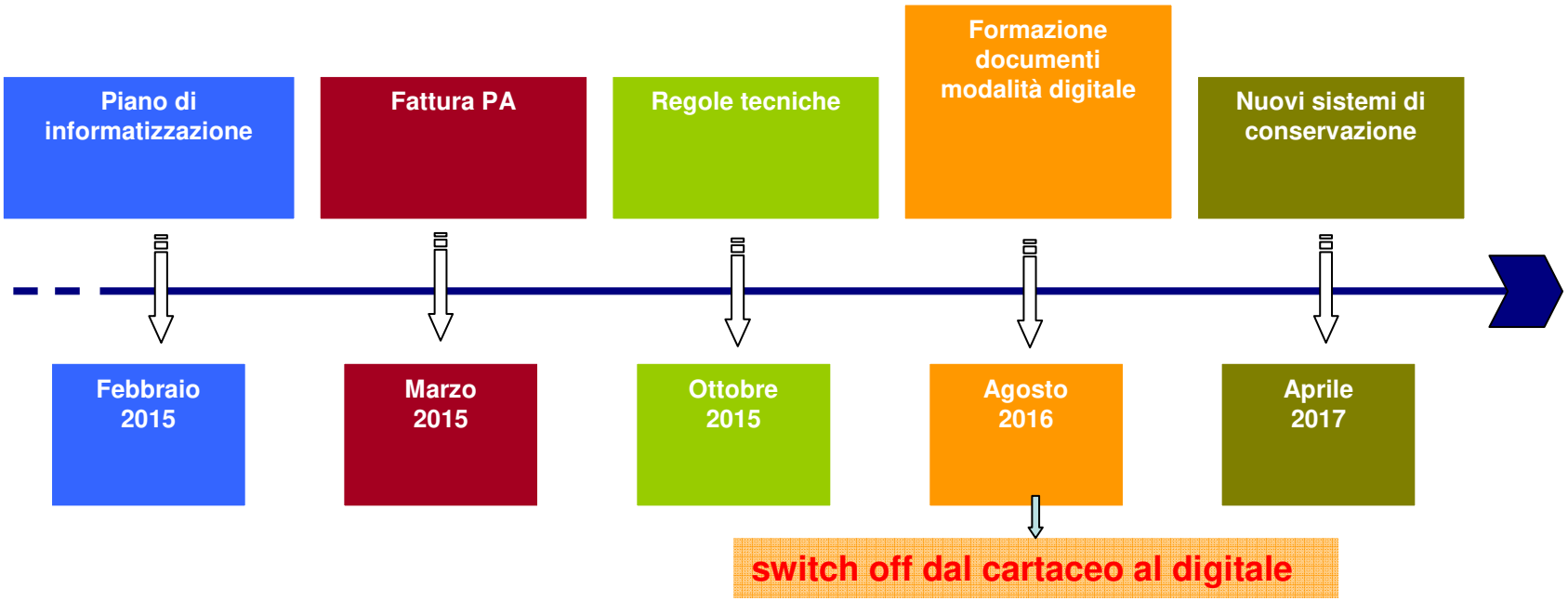


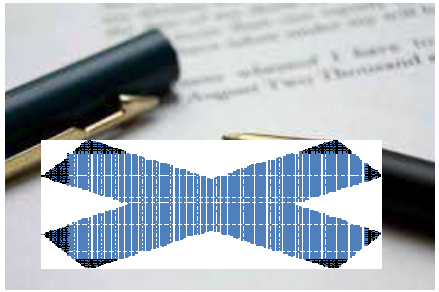
TECNOLOGICO


Codice dell'Amministrazione Digitale (CAD) D.Lgvo 82/2005
Principi
(diritto all'uso delle tecnologie)
Artt. 1-11
Organizzazione informatica della PA e servizi di accesso
CNS - Artt. 12-19
Formazione del documento informatico
Artt. 20-23
Sottoscrizione digitale
Artt. 24-38
Protocollo, conservazione trasmissione
Artt. 40-49
Riuso del software
Artt. 67-70
Dati delle PP.AA., fruibilità dei dati, servizi in rete e carte elettroniche - Artt. 50-66
Sistema Pubblico di Connettività e rete internazionale della PP.AA.
Artt. 72-87

Le tematiche dell'amministrazione digitale

Carta addio… quando?





Obbligo di stipula dei contratti in modalità elettronica

In caso di aggiudicazione il contratto di appalto deve essere stipulato a pena di nullità

- con atto pubblico notarile informatico
- in modalità elettronica secondo le norme vigenti per ciascuna stazione appaltante
  - in forma pubblica amministrativa a cura dell'Ufficiale rogante dell'amministrazione aggiudicatrice (**dal 30 giugno 2014)**
  - mediante scrittura privata (**dal 1° gennaio 2015)**

(art. 11, comma 13 D.Lgs. 12/04/2006, n. 163 - Codice dei contratti pubblici)

ADEMPIMENTI DERIVANTI:

•Il **bando di gara** deve indicare le modalità di sottoscrizione del contratto da parte dell'aggiudicatario

•ogni amministrazione deve adottare le **disposizioni regolamentari** relative alla "modalità elettronica", anche con rinvio a quelle del CAD

ANAC
Autorità Nazionale Anticorruzione

ha chiarito che:

- L'obbligo di stipula in modalità elettronica trova applicazione solo con riferimento ai **soli contratti di appalto**, **con esclusione dei contratti sottratti all'applicazione del Codice dei contratti**
- "**modalità elettronica**" può essere intesa anche nel senso che è ammesso il **ricorso all'acquisizione digitale della sottoscrizione autografa**, ferma restando l'attestazione, da parte dell'Ufficiale rogante, dotato di firma digitale, che la firma dell'operatore economico è stata apposta in sua presenza, previo accertamento della sua identità personale, ai sensi dell'art. 25, comma 2, del CAD

(ANAC Determinazione n. 1 del 13 febbraio 2013)

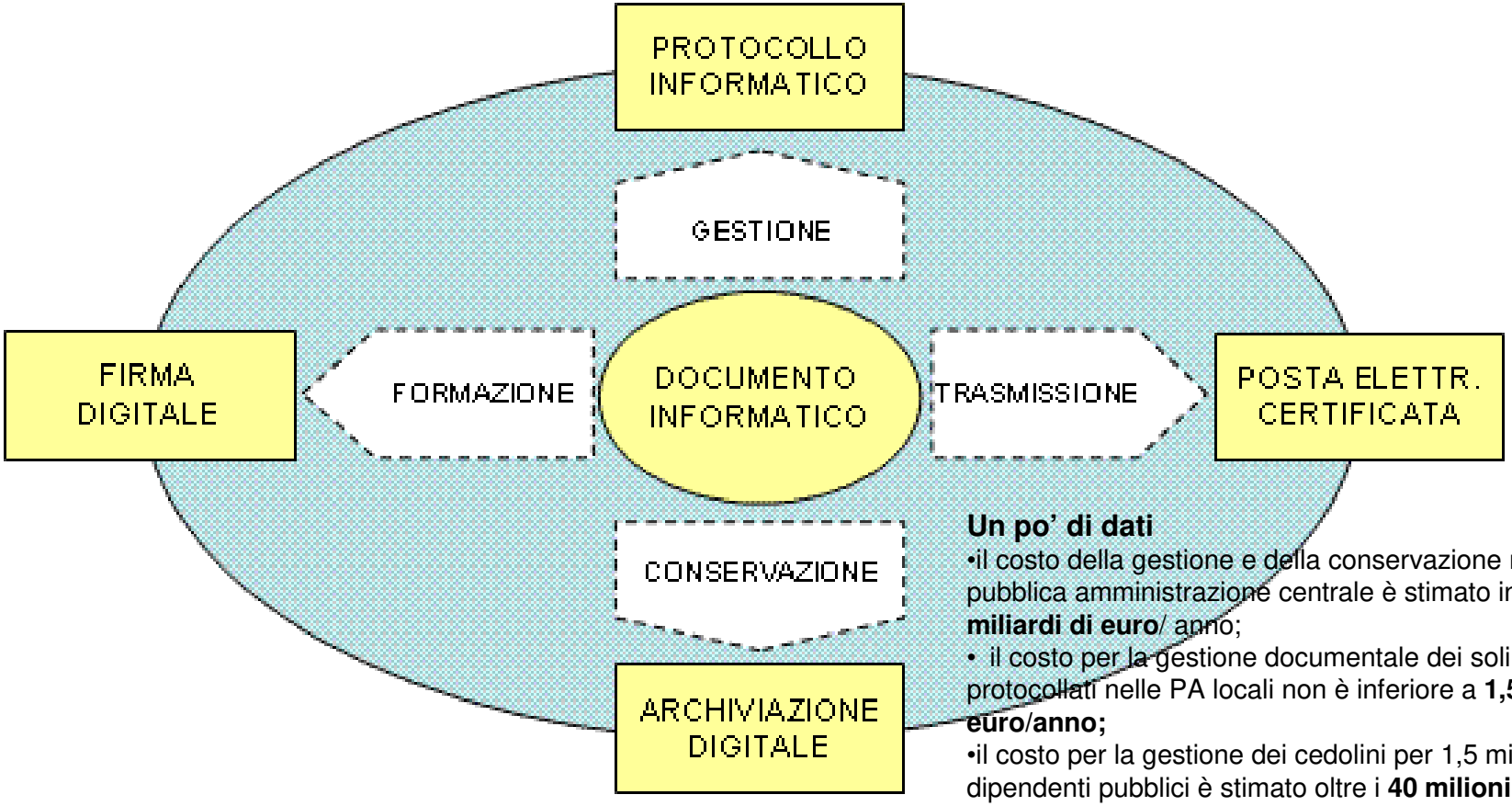
Obbligo di stipula di accordi tra PP.AA. con firma digitale

A fare data dal 30 giugno 2014, a pena la nullità, gli accordi tra amministrazioni pubbliche per disciplinare lo svolgimento in collaborazione di attività di interesse comune sono sottoscritti :

- con firma digitale, ai sensi dell'art. 24 del CAD
- con firma elettronica avanzata, ai sensi dell'art.1, comma1, lett. q-bis) del CAD,
- con altra firma elettronica qualificata.

(art. 15, comma 2 bis L. 241/1990 – in materia di procedimento amministrativo)

I cardini del sistema



Un po' di dati

•il costo della gestione e della conservazione nella pubblica amministrazione centrale è stimato intorno ai **3 miliardi di euro**/ anno;

• il costo per la gestione documentale dei soli documenti protocollati nelle PA locali non è inferiore a **1,5 miliardi di euro/anno;**

•il costo per la gestione dei cedolini per 1,5 milioni di dipendenti pubblici è stimato oltre i **40 milioni di euro/anno**;

•le grandi organizzazioni perdono un documento ogni 12 secondi;

•il 7% dei documenti è perduto in modo definitivo;

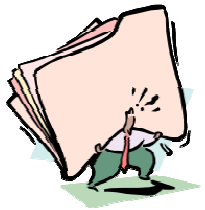
•un dirigente spende in media 9 ore all'anno per ricercare documenti male archiviati, male indicizzati o persi;

•il 3% dei documenti sono archiviati in modo errato.

Documenti analogici e digitali

Il documento informatico altro non è che un complesso di bit impressi su un supporto informatico per la cui lettura si rende indispensabile l'ausilio del computer.

Documento analogico



È un oggetto materiale

È originale

Può essere sottoscritto con firma autografa

Documento digitale

E' un oggetto "quasi" immateriale

Ogni duplicato è un originale

Può essere firmato digitalmente

IL DOCUMENTO INFORMATICO: È UN OBBLIGO PER LE PP.AA.

Formazione di documenti informatici (Art. 40 CAD)

Le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici.

Con apposito regolamento, sulla proposta dei Ministri delegati per la funzione pubblica, per l'innovazione e le tecnologie e del Ministro per i beni e le attività culturali, sono individuate le categorie di documenti amministrativi che **possono essere redatti in originale anche su supporto cartaceo** in relazione al particolare valore di testimonianza storica ed archivistica che sono idonei ad assumere.

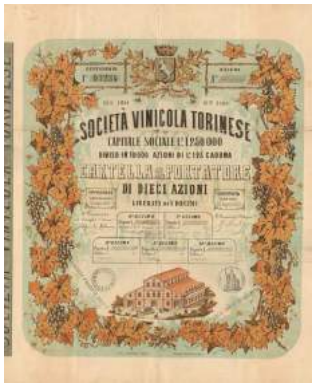
La ratio dell'articolo è che **le PA non dovrebbero, mai o quasi mai produrre documenti cartacei**.

I documenti amministrativi possono essere solo informatici

Gli originali unici

Documenti analogici originali unici per i quali permane l'obbligo della conservazione dell'originale cartaceo. D.P.C.M. 21/03/2013

Documenti di valore storico-artistico



Opere d'arte

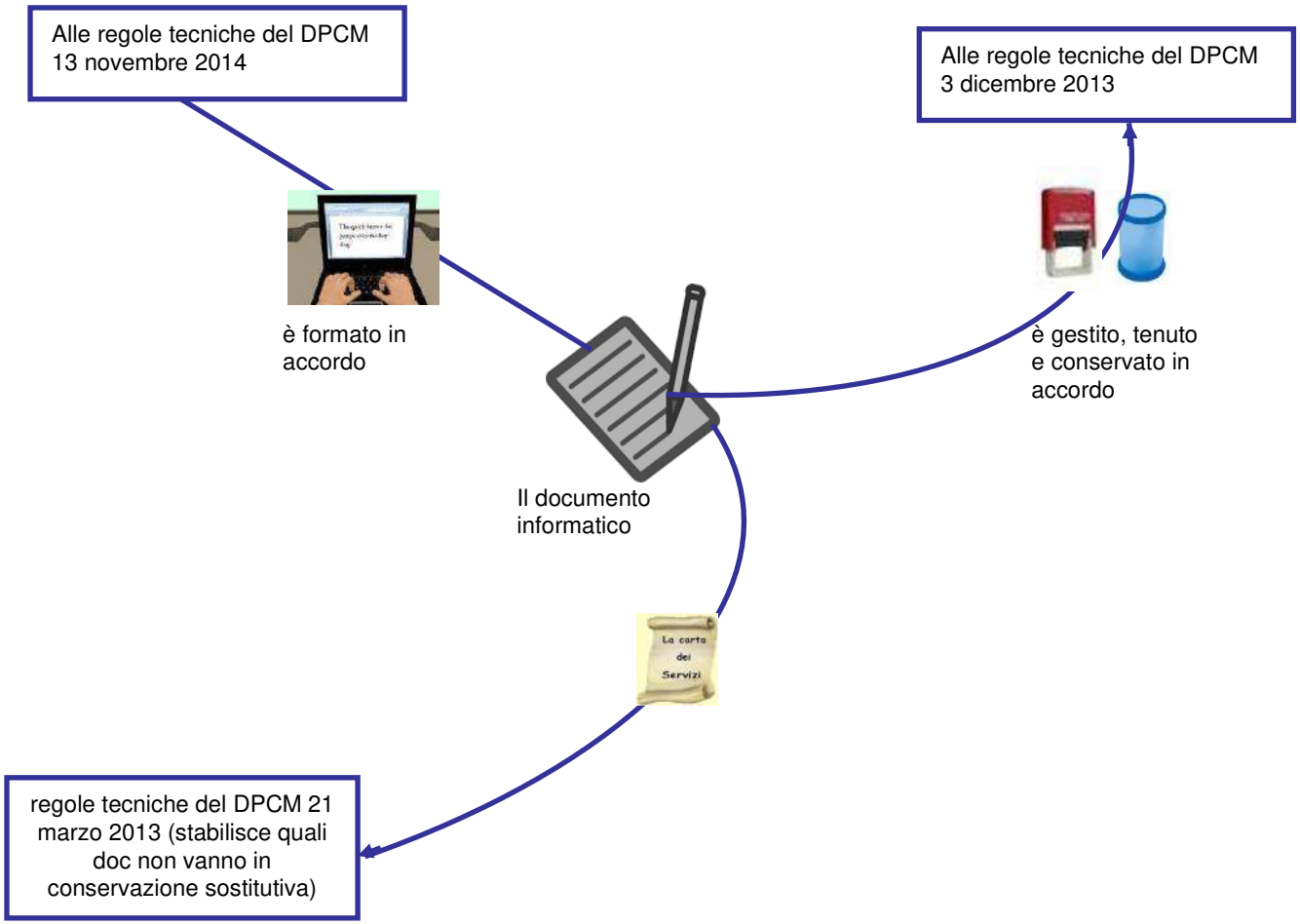
E' ammessa la conservazione sostitutiva, in tal caso però la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi apposta e firmata digitalmente

Atti notarili

Atti giudiziari, processuali e di polizia giudiziaria per i venti anni successivi

I documenti informatici per avere rilevanza di legge debbono essere conformi alle regole tecniche

Art. 20 C.A.D.



Il documento informatico: è rappresentazione informatica di atti, fatti, dati giuridicamente rilevanti (Art 1 comma 1 lett. p) CAD)

Nel Regolamento comunitario eIDAS, il documento elettronico viene definito come *"**qualsiasi contenuto** conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva"*.

Il documento informatico è un **CONTENUTO** (e non il supporto che lo contiene), avente una valenza dal punto di vista del diritto, trattabile in modalità informatica e quindi attraverso gli automatismi propri di un elaboratore.

Il documento informatico può esistere giuridicamente solo se è adeguatamente staticizzato, gestito e conservato in idonei sistemi.

Come si forma un documento informatico ?

Le regole tecniche elencano anzitutto le modalità con cui si forma un documento informatico che sono:

1. **REDAZIONE** tramite l'utilizzo di appositi strumenti software (es. dattiloscrittura di un file word);

2. **ACQUISIZIONE** di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico (es. ricezione di una PEC, scansione di un documento…ecc.)

3. **REGISTRAZIONE** informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente (es. il risultato di una transazione online)

4. **GENERAZIONE O RAGGRUPPAMENTO** anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica (es: la compilazione a fine giornata del registro di protocollo di una PA).

(art. 3, comma 1 DPCM 13/11/2014)

Documenti informatici nativi e duplicati

Documenti informatici nativi

Documenti informatici acquisiti per via telematica o su **supporto informatico**

Registrazione informatica
di informazioni conseguenti
transazioni on line
compilazione di istanze/moduli on line

P.E.C.

SCANNER

Supporti di memoria

Requisiti obbligatori del documento informatico

- **IMMODIFICABILITÀ**
  (della forma e del contenuto)
  nella fase di tenuta e accesso

- **STATICITÀ**
  (della forma e del contenuto)
  nella fase di conservazione

(ex art. 3 del D.P.C.M. 13/11/2014)

Alcuni FORMATI garantiscono l'immodificabilità e la staticità del documento amministrativo

Immodificabilità

La immodificabilità di un documento informatico dipende dalle modalità di creazione del documento.

Le stesse caratteristiche di immodificabilità ed integrità del documento informatico possono essere soddisfatte in modo diverso a seconda della tipologia del documento.

- Redazione tramite software

è reso immodificabile da

1. Firma digitale o qualificata
2. Validazione temporale
3. Ricevuta completa PEC
4. Memorizzazione su sistemi di gestione documentale che assicurino idonee politiche di sicurezza

- Acquisizione da supporto, da scanner o telematica

è reso immodificabile

dalla memorizzazione in un sistema di gestione informatica dei documenti che garantisca l'inalterabilità di un documento o in un sistema di conservazione

- Documento conseguente a transazione on line o compilazione automatica di moduli da parte dell'utente
- Integrazione di dati provenienti anche da fonti eterogenee

è reso immodificabile

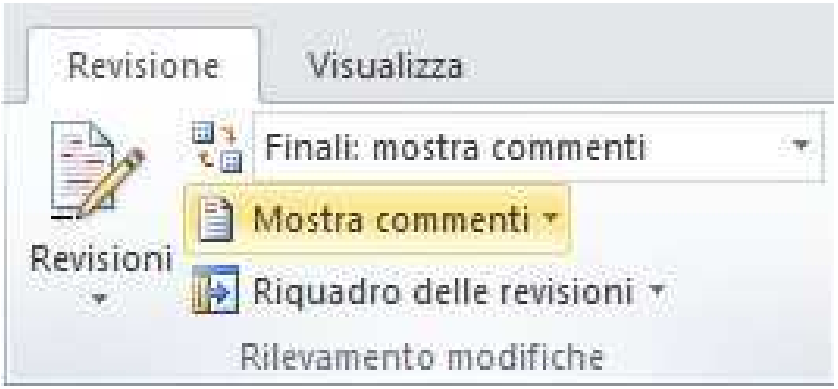
dalla registrazione dei dati e dall'applicazione di misure per la protezione dell'integrità delle basi dati e per la produzione e conservazione dei log di sistema ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione

Staticità

caratteristica che garantisce **l'assenza**

1. sia di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili

2. sia delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione



FORMATO

cioè la modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso **l'estensione del file.**

Documento informatico **immodificabile** → utilizzo di uno dei formati di cui all'allegato 2 delle Regole Tecniche

I formati individuati all'allegato 2 delle regole tecniche assicurano:
- **l'indipendenza dalle piattaforme tecnologiche**
- **l'interoperabilità tra sistemi informatici**
- **la durata nel tempo dei dati in termini di accesso e di leggibilità.**

Interoperabilità: capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi

Leggibilità, insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti

FORMATI APERTI

le cui specifiche sono pubbliche in modo tale che chiunque possa scrivere un programmino per leggere i file, senza dover ricorrere ad un particolare produttore di software

NON sono ammessi il **pdf** ed il **word** perché formati **proprietari** e quindi leggibili solo se in possesso dei programmi Microsoft.

FORMATI "STATICI"

non devono cioè contenere campi che comporterebbero modifica di alcune parti dello stesso non rilevabili alla verifica della firma.

Sono formati statici il **PDF/A**, l'**XML**, i formati immagine (ad es. **TIFF**), i formati testo **e metadati minimi** come il **TXT.**.

Formati diversi possono essere scelti nei casi in cui la natura del documento informatico lo richieda per un utilizzo specifico nel suo contesto tipico.

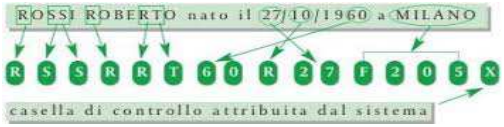
METADATI

D.P.C.M. 13/11/2014 art. 3, comma 9

I METADATI:
sono dati sui dati, ovvero dati che servono a spiegare il significato di altri dati.

AL **DOCUMENTO INFORMATICO** SI ASSOCIANO SEMPRE I SEGUENTI METADATI:

1) L'IDENTIFICATIVO
UNIVOCO E PERSISTENTE



2) LA DATA DI CHIUSURA

3) L'OGGETTO

4) IL SOGGETTO PRODUTTORE

5) IL DESTINATARIO
(EVENTUALE)

6) L'IMPRONTA

L'impronta del documento informatico altro non è che un suo riassunto molto sintetico
da un file di 10 GB se ne può avere un impronta di pochi byte

RIFERIMENTO TEMPORALE / MARCA TEMPORALE: non sono la stessa cosa

Il **riferimento temporale** è una semplice annotazione che attesta la data di ultima modifica di un documento.

Essa può essere elaborata da un procedura informatica ed essere inserita nel documento o ad esso allegata.

Della apposizione del riferimento temporale è responsabile il soggetto che forma documento.

Il riferimento temporale non è opponibile a terzi.

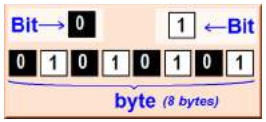
La **marca temporale** è un certificato rilasciato da un soggetto terzo accreditato (c.d. Timestamping Autority) e da questi sottoscritto in modo digitale, che attesta che il documento informatico esisteva alla data del rilascio del certificato.

La marca temporale è opponibile a terzi.

E quindi è efficace in ogni situazione in cui un documento deve avere una data certa.

Copie e duplicati informatici

BIT



CARTA

DUPLICATI se ho un file word sul mio hard disk e lo copio con una chiavetta USB quale dei due è il mio documento? La risposta è semplice: ENTRAMBI, infatti i due files sono semplicemente dei DUPLICATI INFORMATICI (è come se avessi redatto due copie del contenuto di un documento, entrambe lo rappresentano, ma nessuna delle due in maniera esclusiva). Essi hanno lo **stesso contenuto e la stessa sequenza di valori binari**.

COPIA INFORMATICA DI DOCUMENTI INFORMATICI se ho un file word sul mio hard disk e lo trasformo in un file PDF allora in questo caso il contenuto rappresentato è identico ma con modalità informatiche differenti. Il due files sono COPIE INFORMATICHE DI DOCUMENTI INFORMATICI ed hanno lo **stesso contenuto ma diversa sequenza di valori binari**.

COPIA PER IMMAGINE DI UN DOCUMENTO ANALOGICO: se tramite uno scanner produco un'immagine di un documento cartaceo e lo salvo in formato .tiff, .jeg, .pdf, ecc. ho ancora ottenuto un documento informatico. Esso è una COPIA PER IMMAGINE DI UN DOCUMENTO ANALOGICO. In tal caso esso appare ai nostri occhi esattamente come l'originale cartaceo, ossia, secondo il legislatore ne ha la **stessa forma e contenuto**.

COPIA INFORMATICA DI DOCUMENTO ANALOGICO: se ricopio un documento a computer oppure se attraverso un software (OCR) ne edito il testo avrò realizzato una COPIA INFORMATICA DI DOCUMENTO ANALOGICO. In tal caso esso ha lo **stesso contenuto** del documento analogico ma **forma diversa.**

La copia informatica o l'estratto informatico di documento informatico

SE

notaio o pubblico ufficiale a ciò autorizzato

ATTESTA LA CONFORMITA' ALL'ORIGINALE

- *nel documento informatico contenente la copia per immagine*
- *oppure in un documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine*

e sottoscrive la copia con firma digitale o nel caso di *pubblico ufficiale anche con firma elettronica qualificata*

la copia informatica/estratto del documento informatico

⇩

HA LA STESSA EFFICACIA PROBATORIA DELL'ORIGINALE

La conformità all'originale di copia per immagine di documento analogico può essere autenticata con le medesime modalità, però occorre attestare altresì che **l'immagine acquisita corrisponde al documento analogico originale** oppure che l'operazione di acquisizione del documento analogico è avvenuto con tecniche certificate che assicurano tale corrispondenza (ex art. 4 D.P.C.M. 13/11/2014)

La copia informatica o l'estratto informatico di documento informatico

SE *colui che estrae copia*

SOTTOSCRIVE la copia con firma digitale.

la copia informatica/estratto del documento informatico

HA STESSA EFFICACIA PROBATORIA DELL'ORIGINALE SALVO DISCONOSCIMENTO

La copia per immagine di documento analogico può essere sottoscritta con firma digitale o firma elettronica avanzata da chi effettua la copia. Quest'ultima, ancorchè sottoscritta, però, non ha alcuna efficacia probatoria.

Copie analogiche di documenti informatici

1 **SE AUTENTICATE**

STESSA EFFICACIA PROBATORIA ORIGINALE

2 **SE NON AUTENTICATE**

STESSA EFFICACIA PROBATORIA ORIGINALE SALVO DISCONOSCIMENTO

L'autentica

VERIFICHE preliminari

- verifica del **formato** del documento di cui si fa la copia sia documento, che deve essere idoneo alla firma e cioè "statico".
- verifica della **firma**, dando atto, nella formula di conformità dell'esito della verifica effettuata e di tutti quei dati, contenuti nel certificato, che caratterizzano la firma stessa (certificatore emittente, numero del certificato, eventuali qualifiche del soggetto titolare indicate al suo interno, assenza di espresse limitazioni all'utilizzo del certificato stesso, etc.).

FORMULA di copia conforme

Copia conforme all'originale informatico, sottoscritto con firma digitale, il cui certificato è intestato al signor … (eventuali qualifiche contenute nel certificato e relative all'utilizzo della connessa firma digitale), rilasciato da … (Certificatore: Infocert, Intesa, Postecom, etc.) n. …, valido e non revocato, la cui verifica ha avuto esito positivo.
Numero dei fogli impiegati:_____

Data e luogo del rilascio

nome e cognome,
qualifica rivestita
firma per esteso
timbro dell'ufficio

Il documento amministrativo informatico

Il documento amministrativo informatico **è**

- quello prodotto dalla P.A.
- quello ricevuto e registrato da una P.A.

Deve avere requisiti addizionali rispetto ai documenti informatici **perché**

è un documento di una **Pubblica Amministrazione**, per cui fa pubblica fede e ciò richiede l'adozione di misure specifiche

Con quali strumenti è prodotto

Esso è prodotto con gli strumenti indicati nel **MANUALE DI GESTIONE** del protocollo informatico

Dove è registrato

TUTTI I DOCUMENTI INFORMATICI VANNO PROTOCOLLATI AL PROTOCOLLO GENERALE E ACQUISITI nel sistema di gestione documentale dell'Ente.

Possono esserci dei casi in cui dei documenti non sono registrati al protocollo generale, ma in registri appositi. Nel **MANUALE DI GESTIONE** del protocollo informatico tali casistiche vanno specificate, descrivendo anche come avviene la registrazione di tali documenti.

CON LA REGISTRAZIONE A PROTOCOLLO E' GARANTITA L'IMMODIFICABILITA' DEL DOCUMENTO INFORMATICO

Metadati da associare al documento amministrativo informatico

Al documento amministrativo informatico registrato al protocollo generale vanno associati un insieme minimo di metadati che sono:

- **NUMERO DI PROTOCOLLO** del documento generato automaticamente dal sistema e registrato in forma non modificabile;
- **DATA DI REGISTRAZIONE** di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
- **MITTENTE** per i documenti ricevuti o **DESTINATARIO** o destinatari per i documenti spediti, registrati in forma non modificabile;
- **OGGETTO** del documento, registrato in forma non modificabile;
- data e protocollo del documento ricevuto, se disponibili;
- **IMPRONTA** del documento informatico

Art. 53 D.P.R. 445/2000 come richiamato dall'art. 9, comma 7, del D.P.C.M. 13/11/2014

Informazioni che debbono essere rese disponibili sul sito

Ai fini della trasmissione telematica di documenti amministrativi informatici, le pubbliche amministrazioni **devono** pubblicare sui loro siti:

- gli standard tecnici di riferimento
- le codifiche utilizzate
- le specifiche per lo sviluppo degli applicativi software di colloquio

Le PP.AA. **possono** rendere eventualmente disponibile gratuitamente sul proprio sito il software per la trasmissione di dati coerenti alle suddette codifiche e specifiche

Le PP.AA., al fine di abilitare alla trasmissione telematica gli applicativi software sviluppati da terzi, **devono** richiedere a questi opportuna certificazione di correttezza funzionale dell'applicativo e di conformità dei dati trasmessi alle codifiche e specifiche pubblicate.

La firma e la data

PERCHE' UN DOCUMENTO (analogico o informatico) **DEVE ESSERE FIRMATO?**

- per poter dimostrare che chi ho la scritto ne aveva la **competenza**
- per poter addossare la **responsabilità** del contenuto al sottoscrittore e quindi per poter individuare la **paternità** del documento

La sottoscrizione è quindi rilevante sulle problematiche relative alla **competenza** ed alla **identità** del sottoscrittore.

PERCHE' OCCORRE APPORRE LA DATA DELLA SOTTOSCRIZIONE?

- per poter verificare la sussistenza della **competenza** alla firma al momento della sottoscrizione
- per poter verificare il momento in cui sono intervenute eventuali **correzioni** (le correzioni sono state fatte prima o dopo la sottoscrizione, se successive chi le ha fatte?)

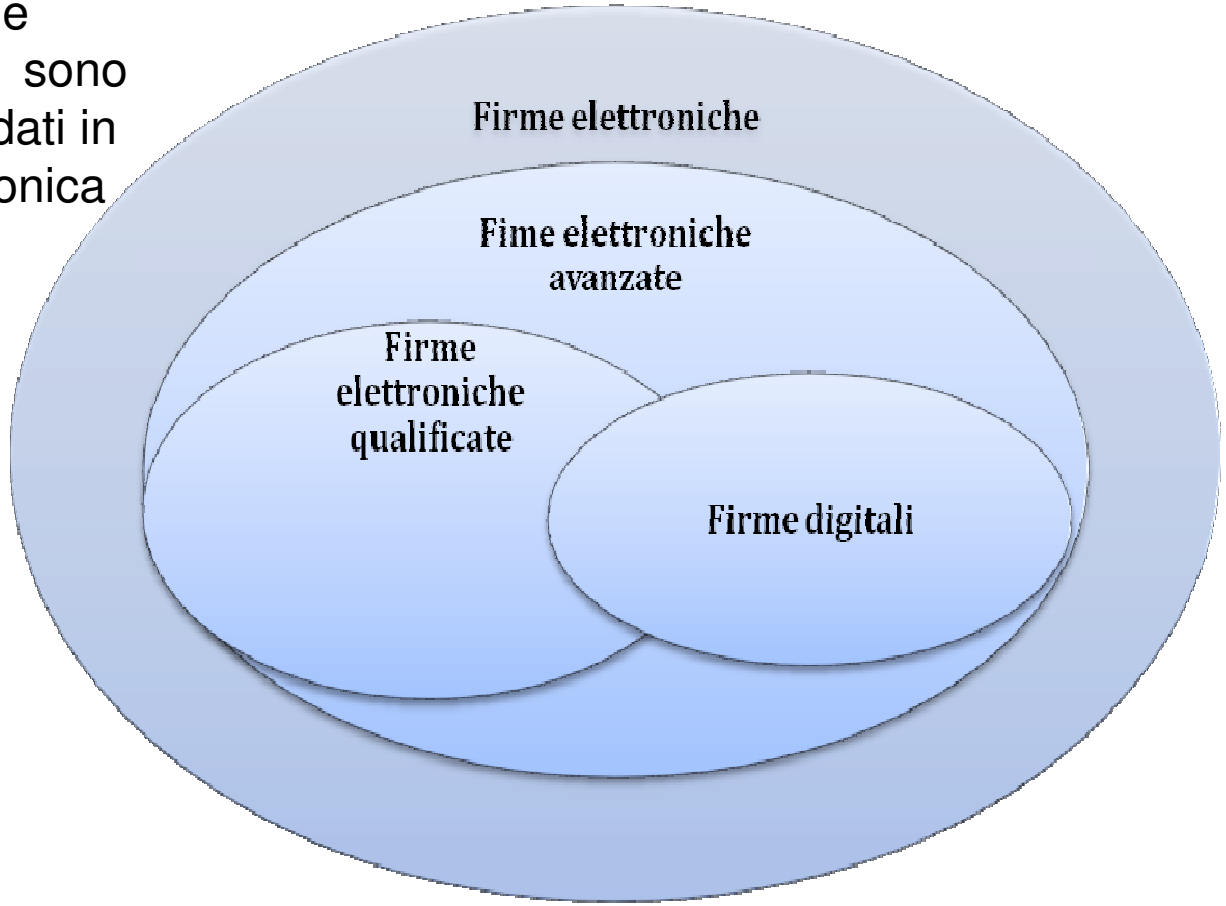
La data in cui è stata apposta la sottoscrizione è quindi rilevante sulle problematiche relative alla **competenza** del sottoscrittore e su quelle relative alla **immodificabilità** di un documento.

Tipologie di firma

Il CAD riconosce 4 differenti tipi di firma elettronica:

- ✓ la firma elettronica
- ✓ la firma elettronica avanzata
- ✓ la firma qualificata
- ✓ la firma digitale

Tutte le firme elettroniche sono insiemi dei dati in forma elettronica



La firma elettronica

c.d. “firma debole”

Il CAD definisce la firma elettronica come: l'insieme dei **dati** in forma elettronica, allegati oppure connessi tramite associazione logica ad altri **dati** elettronici, utilizzati come metodo di identificazione informatica.

la firma elettronica è un insieme di dati usato per autenticarsi

(ad es. utenza e password per accedere a facebook sono un esempio di firma elettronica)

Nulla si dice sulla sua attendibilità ed essa non è necessariamente riferita ad un documento

La firma elettronica avanzata

è una firma elettronica con le seguenti caratteristiche:

Essa è:

- riferita ad un **documento specifico**
- creata con **mezzi** di cui il firmatario ha il controllo esclusivo

Essa permette:

- permette l'**identificazione dell'autore**

Essa garantisce di poter risalire univocamente da un documento al suo sottoscrittore

- di conservare l'**integrità** del documento

i dati ai quali la firma si riferisce sono collegati ad altri dati in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati
cioè se un documento firmato con firma elettronica avanzata viene successivamente modificato, un software per il riconoscimento delle firme se ne accorgerà immediatamente segnalando di aver trovato un falso.

La legge riconosce a tale tipologia di firma un **ambito di applicabilità inferiore a quello della firma digitale**.
La firma elettronica avanzata non può essere usata per i contratti che trattano vendite o locazioni di immobili (ad esempio) e ha valenza **solo** nei rapporti tra firmatario e controparte se questa ha proposto di usare quella particolare soluzione di firma, **non ha cioè una valenza verso tutti come la firma digitale**.

Un esempio di firma elettronica avanzata sono le firme grafometriche, quali ad esempio le firme su un tablet (c.d. tablet notarile) per esempio quello utilizzato negli uffici postali o quando un corriere ti consegna un pacco o in banca.

La firma elettronica qualificata

è una firma elettronica avanzata con in

UN CERTIFICATO QUALIFICATO

(cioè un documento informatico contenente un' attestazione, proveniente da un soggetto terzo, dotato degli opportuni criteri di affidabilità, che ci permette di avere la certezza in ordine al firmatario)

+

UN DISPOSITIVO FISICO SICURO PER LA CREAZIONE DELLA FIRMA

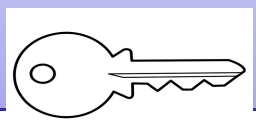
(tipicamente un token USB che inserito nel PC permette di firmare il documento previo inserimento di nome utente e password, come ad es. il bancomat)

La firma digitale

è una firma elettronica avanzata con in

CERTIFICATO QUALIFICATO

il certificatore attesta, nel documento informatico da lui sottoscritto, non solo l'**identità** del sottoscrittore ma inserisce anche, nel certificato, la **chiave pubblica** dello stesso



Nella firma digitale sono critiche le informazioni sul tempo di apposizione della sottoscrizione e lo stato del certificato digitale (revoche e sospensioni).
Nel certificato digitale possono essere inserite anche una serie di ulteriori informazioni sul sottoscrittore, per esempio il titolo, le limitazioni d'uso, le limitazioni nei valori negoziali, l'utilizzo di sottoscrizione con procedura automatica.

UN SISTEMA DI CHIAVI CRITTOGRAFATE

ciascun soggetto firmatario di un documento deve disporre di:
una **chiave privata**, nota solo a lui che gli permette di firmare i documenti
una **chiave pubblica**, necessaria a tutti coloro che intendano leggere il documento, tramite essa è possibile verificare che il documento è stato effettivamente firmato dal firmatario e non è stato alterato

Non c'è riferimento ad un dispositivo fisico, cioè per firmare digitalmente un documento non è necessario un dispositivo fisico (token USB, card o altri).
La chiave pubblica è nota a chi deve leggere il documento poichè contenuta nel certificato qualificato.

La crittografia

Per crittografia è una tecnica che permette di "cifrare" un messaggio rendendolo incomprensibile a tutti fuorchè al suo destinatario.

Al momento della crittografia dei dati, viene applicato un algoritmo per codificarli in modo tale che perdano la loro forma originale e non possano essere letti.

I dati possono essere decodificati nella loro forma originale solo applicando una specifica chiave di decrittografia.

CRITTOGRAFIA SIMMETRICA

DETTA ANCHE A CHIAVE PRIVATA

la stessa chiave (privata) permette di criptare e decriptare il messaggio.

Tutti sono a conoscenza della chiave e quindi il sistema è poco sicuro

CRITTOGRAFIA ASIMMETRICA

DETTA ANCHE A CHIAVE PUBBLICA

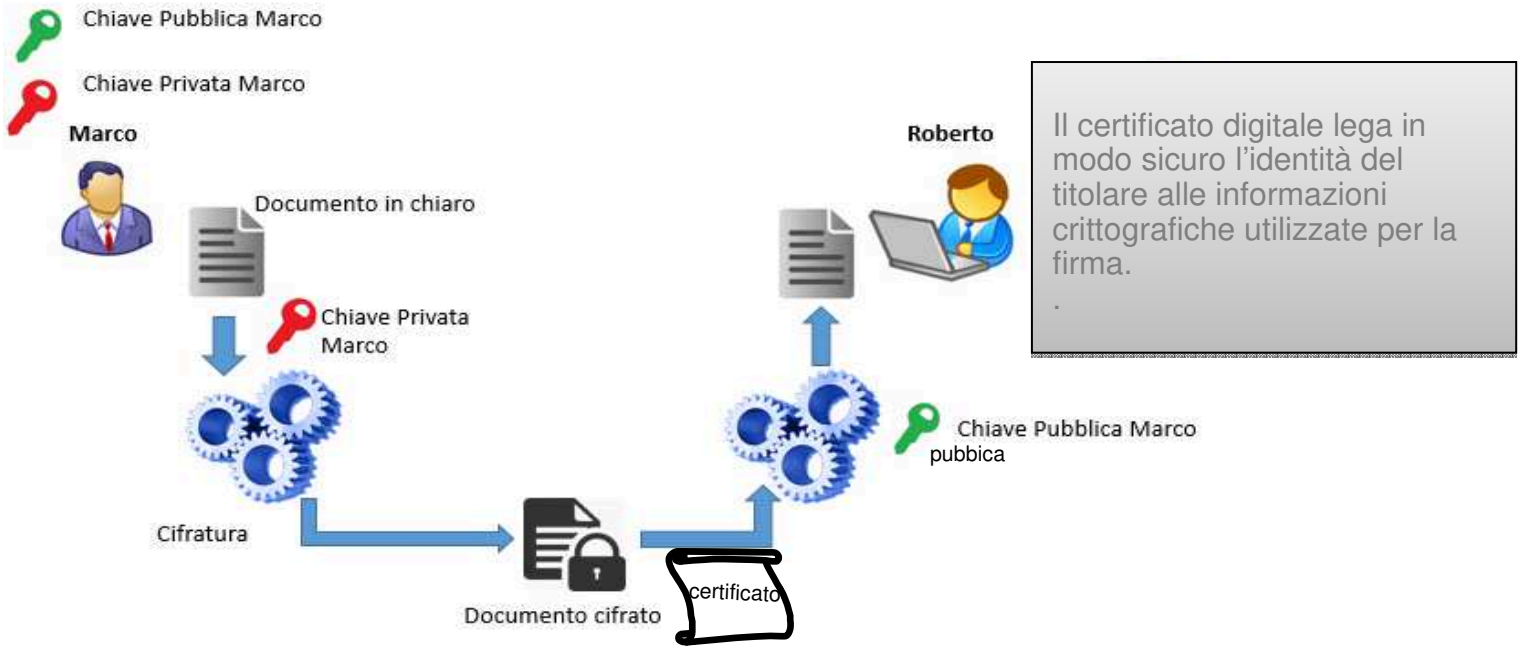
Sono necessarie due chiavi diverse una per criptare (privata) e l'altra per decriptare il messaggio (pubblica).

Le chiavi sono invertibili.

Solo la chiave pubblica è nota a tutti. Il sistema è sicuro.

La crittografia asimmetrica (o a coppia di chiavi, o a chiave pubblica/privata)

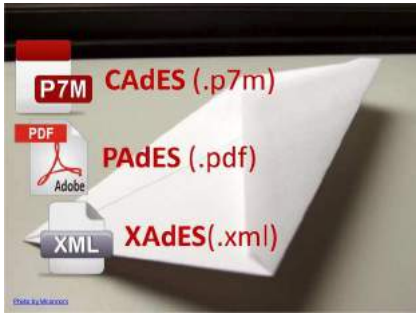
GARANTISCE: segretezza, integrità e non ripudiabilità di un documento



Invio di un messaggio cifrato di cui si voglia garantire autenticità e non ripudiabilità

Immaginiamo che l'utente Marco voglia inviare un messaggio cifrato all'utente Roberto, lasciando che il suo interlocutore possa verificarne l'autenticità e l'origine con certezza. Marco utilizza la sua chiave privata per cifrare il documento da inviare a Roberto. A questo punto Roberto potrà decodificare il messaggio ed essere certo che sia stato Marco ad inviarlo e che il messaggio è autentico. Il processo descritto garantisce quindi l'autenticità e la non ripudiabilità dell'informazione trasferita tra i due attori.

I FORMATI DELLA FIRMA DIGITALE



• FORMATO p7m (CAdES)

LA FIRMA E' ASSOCIATA AL DOCUMENTO

OBBLIGATORIO PER LE PP.AA.

Con la firma digitale il documento è trasformato in **formato . p7m.**

Questo meccanismo mi permette di creare una **busta crittografata** che contiene il certificato di firma digitale e la chiave pubblica. Il documento firmato può essere inserito nella busta o essere disgiunto.

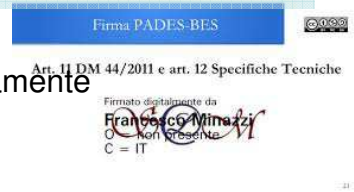
La firma p7m può essere anche multipla, cioè uno stesso documento può contenere più firme. Le firme possono essere **indipendenti** (cioè apposte in modo parellelo e disgiunto) o "**amidate**" (cioè apposte in modo ricorsivo e quindi non possono essere rimosse senza inficiare la validità del documento, come accade per i documenti cartacei).

• FORMATO pdf (PAdES)

LA FIRMA INCORPORATA NEL DOCUMENTO

Con la firma digitale il documento rimane in **formato . Pdf**, leggibile con acrobat reader.

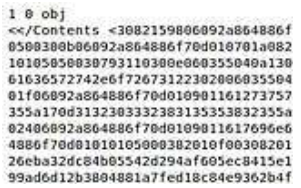
Spesso ha una rappresentazione grafica per cui chi visualizza il documento può capire immediatamente che il documento è firmato. Il documento ha un'apparenza simile a quella della carta firmata.



Non richiede imbustamento

• FORMATO xml (XAdES)

E' apribile con un editor di testo. E' pensata per documenti da elaborare in modo automatico da parte di applicativi. E' usato in particolare nel settore bancario e sanitario (per la cartella sanitaria elettronica, per i referti medici, ecc.). Esso è di difficile lettura, perciò non è molto usato.



SOLUZIONI TECNOLOGICHE

Smart card

Contiene un microchip, che funziona da elaboratore, con un suo sistema operativo.

Al suo interno la **chiave privata**, il **PIN** ed il **certificato.**

VANTAGGI:

è facilmente trasportabile,

è una soluzione economica

può avere una banda magnetica, ad es. per la rilevazione delle presenze)

può essere personalizzata dal punto di vista grafico

SVANTAGGI:

serve un lettore di smart card

non è utilizzabile su dispositivi mobili

occorre installare sul P.C. le librerie della smart card

tende a logorarsi

SOLUZIONI TECNOLOGICHE

Chiavetta

Contiene un lettore di smart card ed una smart card in formato SIM.

Al suo interno oltre alla **chiave privata**, al **PIN** ed al **certificato, ci sono anche:le applicazioni di firma, i drivers e molto spazio di memoria per i documenti.**

VANTAGGI:

è facilmente trasportabile,

è pronta all'uso (non richiede installazione)

molta memoria

SVANTAGGI:

più costosa della smart card

alcuni antivirus tendono ad ostacolarne l'uso

non è utilizzabile su tablet

SOLUZIONI TECNOLOGICHE

Firma remota

La **chiave privata** ed il **certificato, sono sul server di firma collocato presso il certificatore**

VANTAGGI:

L'utente può firmare dovunque senza dotarsi di alcun dispositivo di firma

E' possibile firmare anche con smart phone e tablet

1) Invio al server di firma il documento, il PIN ed il codice OTP

2) Il server di firma genera la firma digitale

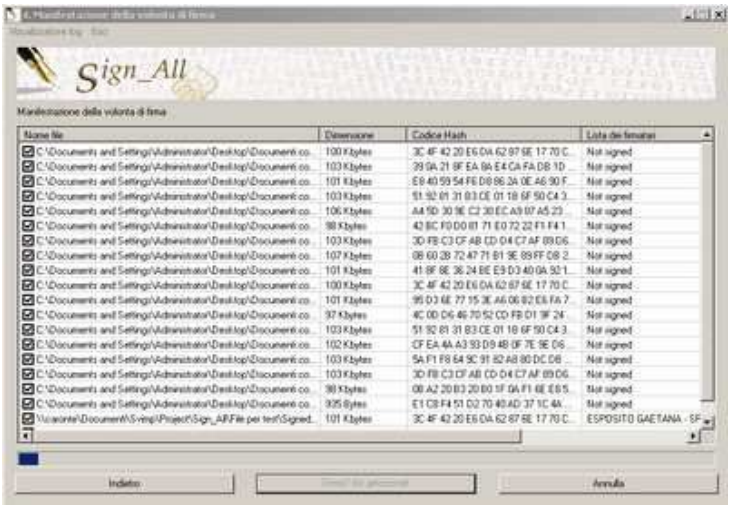
Le comunicazioni tra l'applicativo di firma ed il server sono CRIPTATE

SVANTAGGI:

Per firmare devo essere on line

SOLUZIONI TECNOLOGICHE

Firma massiva



Funziona come la firma remota

ma:

la **chiave privata** ed il **certificato, sono sul server di firma collocato presso l'utente**

Quando occorre firmare documenti in modo massivo ad esempio:

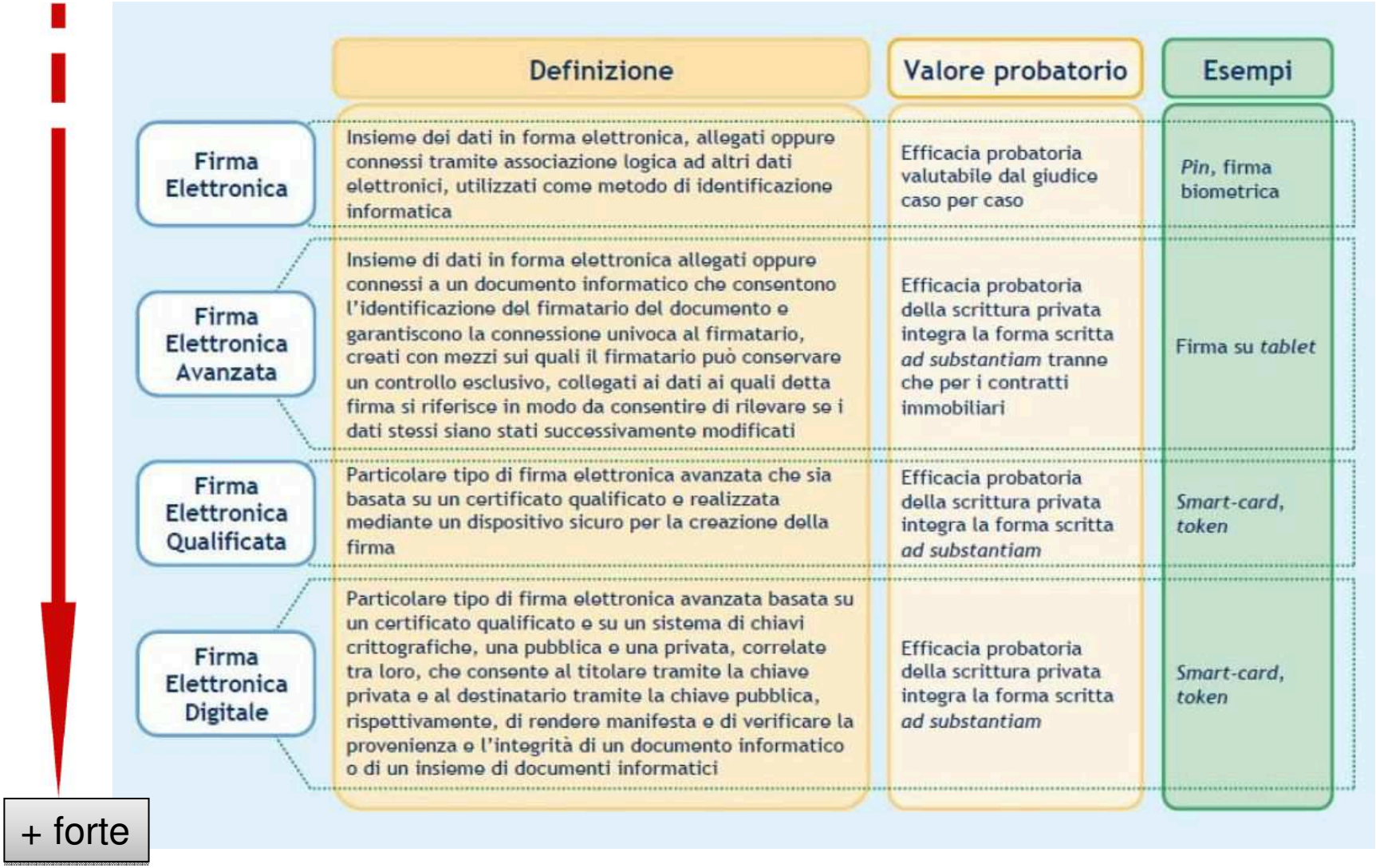
-a fini di conservazione sostitutiva

-fatturazione elettronica conto terzi

-mandati di pagamento

Nella firma remota e massiva la chiave privata non è più nelle mani del firmatario ma è contenuta nel dispositivo HSM che il firmatario utilizza "da remoto", attraverso una connessione di rete.
Si tratta di hardware e software che realizzano dispositivi sicuri per la creazione di firme, in grado di gestire con la massima sicurezza una o più coppie di chiavi crittografiche.
Gli HSM sono generatori di firme digitali e come tali, devono garantire determinati livelli di sicurezza, secondo quanto dettato dal CAD.

Valore probatorio



La Firma digitale garantisce

- **AUTENTICITA':** il destinatario può accertare e verificare l'identità del mittente
- **INTEGRITA':** il destinatario o altri non può falsare in alcun modo un documento firmato dal mittente
- **NON RIPUDIO:** il mittente non può disconoscere un documento da lui firmato

L'apposizione della firma digitale sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente

IL CERTIFICATO DI FIRMA DIGITALE NON DEVE ESSERE

- **SCADUTO**
- **REVOCATO**
- **SOSPESO**

L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico: scaduto, revocato o sospeso:

EQUIVALE A MANCATA SOTTOSCRIZIONE

Le firme elettroniche ancorchè sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore sono valide se alle stesse è associabile

UN RIFERIMENTO TEMPORALE OPPONIBILE A TERZI

che collochi dette firme rispettivamente in un momento antecedente la scadenza, la revoca, la sospensione del suddetto certificato.

RIFERIMENTI TEMPORALI OPPONIBILI A TERZI

- MARCA TEMPORALE

- PROTOCOLLO INFORMATICO

- PEC

- CONSERVAZIONE SOSTITUTIVA

COME **DESTINATARIO** DI UN DOCUMENTO SOTTOSCRITTO CON FIRMA DIGITALE

DEVO **CONTROLLARE** LA VALIDITA' DELLA FIRMA DIGITALE APPOSTA

COME **PRODUTTORE** DI UN DOCUMENTO SOTTOSCRITTO CON FIRMA DIGITALE

DEVO **SALVAGUARDARE** LA VALIDITA' DELLA FIRMA DIGITALE APPOSTA

I certificatori

A norma del CAD l'attività di certificazione è libera e non necessita di particolari autorizzazioni per essere eseguita

io posso scegliere se fidarmi o meno di un certificatore che mi attesta qual'è la chiave pubblica di un soggetto

I certificatori accreditati

ci sono particolari soggetti ai quali l'Agenzia per l'Italia Digitale (AGID) ha riconosciuto particolari requisiti di affidabilità ed integrità morale i cui certificati hanno un valore legale di maggior fede. Questi certificatori vengono denominati dal CAD certificatori "accreditati" proprio perchè hanno affrontato un processo di accreditamento presso l'AGID che può comunque sempre disporre visite ispettive presso gli stessi.

Potremmo dire che la differenza tra un certificatore qualunque ed uno accreditato è come la differenza sul piano della pubblica fede che intercorre tra un **cittadino qualunque** *ed un* **notaio o un pubblico ufficiale.**

Esempi di casi in cui e' richiesta la firma digitale rilasciata da certificatore **accreditato**

Ci sono casi specifici in cui la legge impone che la firma digitale debba essere di un **fornitore di firma accreditato**:

- le **istanze presentate alla PA** se firmate digitalmente (ex art. 65 del CAD)
- la **conformità all'originale** di una copia per immagine di un documento analogico attastata da un pubblico ufficiale o da un notaio
- la **firma del rapporto di versamento** con cui il responsabile della conservazione prende in carico i documenti informatici da un sistema di gestione documentale

Dispositivo di firma e obbligo di custodia

- Art. 21 comma 1 CAD: l'utilizzo si presume riconducibile al titolare salvo prova contraria
- Art. 32, comma2, del CAD: il titolare ha l'obbligo di usare personalmente il dispositivo di firma
- Art. 20151 c.c. ciascuno è responsabile delle cose che ha in custodia salvo che provi il caso fortuito.

E' obbligo porre la necessaria cura per la sicurezza e l'archiviazione dei documenti e dei propri dispositivi di identificazione digitale.

Il titolare della coppia di chiavi:
a) assicura la custodia del dispositivo sicuro per la generazione della firma in suo possesso;
b) conserva le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo contenente la chiave e segue le indicazioni fornite dal certificatore;
c) richiede immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi sicuri per la generazione della firma elettronica qualificata o della firma digitale inutilizzabili o di cui abbia perduto il possesso o il controllo esclusivo;
d) mantiene in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma elettronica qualificata o digitale;
e) richiede immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi sicuri per la generazione della firma elettronica qualificata o della firma digitale qualora abbia il ragionevole dubbio che essi possano essere usati da altri.

Art. 8, comma 5, D.P.C.M. 22/02/2013 (Regole tecniche sulle firme digitali)

La firma autografa e la firma digitale

CREAZIONE	MANUALE	ALGORITMO
APPOSIZIONE	SUL DOCUMENTO	IN ALLEGATO AL DOCUMENTO
VERIFICA	MEDIANTE CONFRONTO ⇒ INSICURA	MEDIANTE ALGORITMO ⇒ SICURA
COPIA	DISTINGUIBILE DALL'ORIGINALE	INDISTINGUIBILE DALL'ORIGINALE
VALIDITA' TEMPORALE	ILLIMITATA	LIMITATA

Quale è la firma migliore ?

Nel nostro ordinamento quindi sono disciplinati diversi tipi di firme elettroniche, le quali contribuiscono a determinare il valore giuridico e probatorio dei documenti informatici a cui sono apposte.
Abbiamo visto che i sistemi di firma elettronica si differenziano non solo per le diverse tecnologie utilizzate, ma anche per la loro maggiore o minore capacità di assicurare la presenza di tutti gli elementi idonei a garantire sia **l'imputabilità giuridica** del documento informatico (cioè, la sua provenienza da parte del soggetto firmatario), sia **l'integrità** e **l'immodificabilità** del documento in tal modo firmato (così da poter garantire anche al documento informatico la cd. "forma scritta e sottoscritta").

Non esiste la firma "migliore" in assoluto, ma ogni tipologia di firma può essere utilizzata in modo appropriato in base al livello di "affidabilità giuridica" che si intende conferire al documento informatico che si sta sottoscrivendo.

Quando usare la Firma semplice

La stessa amministrazione pubblica **non è tenuta a utilizzare sempre e comunque la firma digitale** ma, di volta in volta, può individuare differenti soluzioni di firma elettronica a seconda della documentazione che intende sottoscrivere o far sottoscrivere.

In effetti, anche la cosiddetta **firma elettronica "semplice" può essere astrattamente idonea a far acquistare al documento informatico su cui è apposta il valore di forma scritta in base alle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità del processo attraverso il quale si è formata**. La legge richiede al giudice, di volta in volta, di esprimere un giudizio sull'idoneità a soddisfare il requisito della forma scritta e sul relativo valore probatorio di un documento sottoscritto con una firma elettronica semplice, ai sensi dell'art. 20, comma 1 *bis*, del CAD.

Pertanto, la firma elettronica semplice può essere validamente utilizzata in una pubblica amministrazione **per tutti gli ATTI INTERNI**, cioè **quando il documento informatico da sottoscrivere rimane all'interno del sistema gestionale dell'ente –** che ne garantisce la sicurezza informatica, e, in tal modo, anche il valore giuridico – e non necessita quindi del "sigillo di autenticità e integrità" proprio della firma digitale, richiesto invece per sottoscrivere ad esempio un documento informatico contenente un provvedimento definitivamente adottato o un atto da pubblicare sull'albo pretorio on line dell'ente o da trasmettere a un'altra pubblica amministrazione.

Quando usare la F.E.A.

Sono previste alcune limitazioni per l'utilizzo della firma elettronica avanzata (FEA).
Infatti:
• la FEA non può essere utilizzata nelle transazioni immobiliari (in quanto non integra il requisito della forma scritta)

•la FEA non ha valore probatorio nel caso sia utilizzata per documenti AMMINISTRATIVI informatici **a rilevanza esterna**

•la FEA non ha valore probatorio fino a querela di falso solo nel caso sia utilizzata per documenti AMMINISTRATIVI informatici **a rilevanza interna.**

L'art. 23-ter del CAD, in proposito, precisa infatti che:

"***i documenti costituenti atti amministrativi con rilevanza interna al procedimento amministrativo sottoscritti con firma elettronica avanzata hanno l'efficacia prevista dall'art. 2702 del codice civile***".

I computer sono incredibilmente veloci, accurati e stupidi.

Gli uomini sono incredibilmente lenti, inaccurati e intelligenti.

L'insieme dei due costituisce una forza incalcolabile