CODICE DELLE PUBBLICHE AMMINISTRAZIONI DIGITALI

Legenda:

- sono scritte in **grassetto** le disposizioni nuove o le parti di disposizione innovate;
- sono evidenziati in grigio i riferimenti interni che richiedono l'adeguamento al nuovo impianto normativo;

INDICE SOMMARIO

Capo I – PRINCIPI GENERALI

Art. 1

(Finalità e ambito di applicazione)

1. **La Repubblica assicura la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità elettronica e digitale e si organizza ed agisce utilizzando in modo ottimale le tecnologie dell'informazione e delle comunicazioni.**
2. **Le disposizioni del presente decreto si applicano alle amministrazioni pubbliche di cui all'articolo 1, comma 2 del decreto legislativo 30 marzo 2001, n. 165, salvo che non sia diversamente stabilito.**
3. **Le norme concernenti i documenti informatici, le firme elettroniche, i contratti, i pagamenti informatici, i libri e le scritture, nonché le disposizioni di cui ai capi IV e V relativi alla conservazione e alla trasmissione dei documenti informatici si applicano anche nei rapporti tra privati.**
4. **Le norme di cui ai capi V, VI, VII, concernenti la trasmissione e l'accesso ai documenti informatici e la fruibilità delle informazioni elettroniche digitali si applicano anche ai concessionari dei servizi pubblici.**

Art. 2

(Norme generali per l'azione amministrativa)

1. **Le amministrazioni pubbliche organizzano la propria attività utilizzando le tecnologie dell'informazione e delle comunicazioni nel rispetto dei principi di efficienza, efficacia, economicità, imparzialità, trasparenza e semplificazione.**
2. **Le amministrazioni pubbliche adottano le tecnologie dell'informazione e delle comunicazioni nei rapporti interni, tra le diverse amministrazioni e tra queste e privati, nelle forme previste dalle vigenti disposizioni in materia.**
3. **Le amministrazioni pubbliche operano per assicurare l'uniformità e la graduale integrazione delle modalità di interazione degli utenti con tutti i servizi informatici delle amministrazioni pubbliche, qualunque sia il canale di erogazione, nel pieno rispetto della autonomia e della specificità di ciascun erogatore di servizi.**

4. **La Repubblica promuove la realizzazione e l'utilizzo di reti telematiche come strumento di interazione tra le pubbliche amministrazioni ed i privati.**
5. **Le amministrazioni pubbliche utilizzano le tecnologie dell'informazione e delle comunicazioni, garantendo, nel rispetto delle vigenti normative, l'accesso alla consultazione, la circolazione e lo scambio di dati e informazioni, nonché l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni nel rispetto delle regole tecniche stabilite ai sensi dell'articolo….**

6. **Nell'individuare le soluzioni tecnologiche da adottare le amministrazioni pubbliche motivano adeguatamente le proprie scelte alla luce dei principi contenuti nel presente decreto e delle regole tecniche vigenti.**

Art. 3

(Partecipazione democratica elettronica)

1. **La Repubblica favorisce ogni forma di uso delle nuove tecnologie che promuova una maggiore partecipazione dei cittadini al processo democratico e favorisca l'esercizio dei diritti politici e civili sia individuali che collettivi.**
2. **Al fine di favorire e semplificare l'esercizio dei diritti politici e civili dei cittadini italiani, anche residenti all'estero, attraverso l'applicazione delle tecnologie digitali, la Repubblica promuove l'utilizzo del voto elettronico.**

Art. 4

(Rapporti tra Stato, Regioni ed enti locali)

1. **In attuazione del disposto dell'articolo 117, secondo comma, lettera r), della Costituzione, lo Stato assicura il coordinamento informatico dei dati dell'amministrazione statale, regionale e locale, a tal fine anche dettando le regole tecniche necessarie per garantire la sicurezza e l'interoperabilità dei sistemi informatici e dei flussi informativi per la circolazione e lo scambio dei dati e per l'accesso ai servizi erogati in rete dalle amministrazioni medesime.**

2. **Lo Stato promuove le intese e gli accordi con le regioni e gli enti locali utili per realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso; in particolare li promuove sui seguenti oggetti:**
    a) **linee generali di sviluppo del processo di digitalizzazione;**

b) **interconnessione tra le amministrazioni pubbliche e tra queste ed i cittadini e le imprese;**
c) **modalità di erogazione dei servizi in rete;**
d) **riuso dei programmi informatici;**
e) **progetti infrastrutturali volti alla maggiore efficienza ed alla semplificazione dei procedimenti amministrativi.**

Art. 5

(Digitalizzazione e riorganizzazione)

1. **La riorganizzazione strutturale e gestionale delle amministrazioni pubbliche avviene assicurando il più esteso e ottimale utilizzo delle tecnologie dell'informazione e della comunicazione nell'ambito di una coordinata strategia che garantisca il coerente sviluppo del processo di digitalizzazione.**
2. **Le amministrazioni pubbliche, provvedono a riordinare le strutture organizzative, razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese, ridefinendoli affinché utilizzino in modo ottimale le tecnologie dell'informazione e delle comunicazioni.**
3. **La digitalizzazione dell'azione amministrativa è attuata da parte delle amministrazioni centrali, regionali e con modalità idonee a garantire la partecipazione dell'Italia alla costruzione di reti transeuropee per lo scambio elettronico di dati e servizi fra amministrazioni dei Paesi membri della Unione Europea.**

Art. 6

(Competenze del Ministro per l'innovazione e le tecnologie)

1. **Per il perseguimento dei fini di cui al presente decreto, il Ministro per l'innovazione e le tecnologie, nell'attività di coordinamento del processo di digitalizzazione e di coordinamento e di valutazione dei programmi, dei progetti e dei piani di azione formulati dalle amministrazioni pubbliche centrali per lo sviluppo dei sistemi informativi:**

a) **definisce con proprie direttive le linee strategiche, la pianificazione e le aree di intervento dell'innovazione tecnologica nelle pubbliche amministrazioni, e ne verifica l'attuazione; (art. 26 Finanziaria 2003)**
b) **valuta, sulla base di criteri e metodiche di ottimizzazione della spesa, il corretto utilizzo delle risorse finanziarie per l'informatica e la telematica da parte delle singole amministrazioni; (art. 26 Finanziaria 2003)**
c) **sostiene progetti di grande contenuto innovativo, di rilevanza strategica, di preminente interesse nazionale, con particolare attenzione per i progetti di carattere intersettoriale; (art 27 l. 3/03)**
d) **promuove l'informazione circa le iniziative per la diffusione delle nuove tecnologie;(art. 26 Finanziaria 2003)**
e) **sentito il Centro nazionale per l'informatica nella pubblica amministrazione, detta norme tecniche e criteri in tema di pianificazione, progettazione, realizzazione, gestione, mantenimento dei sistemi informativi automatizzati delle amministrazioni e delle loro interconnessioni, nonché della loro qualità e relativi aspetti organizzativi e della loro sicurezza; (art. 9 D.lgs. 39/93)**

Art. 7

(Centro nazionale per l'informatica nella pubblica amministrazione - CNIPA)

1. **Il Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA) opera ai sensi del decreto legislativo 12 febbraio 1993, n. 39, attuando le politiche del Ministro per l'innovazione e le tecnologie.**
2. **Il CNIPA, ferme restando le funzioni previste dal decreto legislativo 12 febbraio 1993, n. 39 svolge i compiti , di cui ai decreti del Presidente del Consiglio dei Ministri 18 maggio 2001 e 30 luglio 2003, già attribuiti al soppresso Centro tecnico di cui all'articolo 17, comma 19, della legge 15 maggio 1997, n. 127.**
3. **Il CNIPA può esprimere, a richiesta, pareri sulla congruità tecnico economica degli schemi di contratti concernenti l'acquisizione di beni e servizi informatici delle regioni e degli enti locali nei limiti di cui all'articolo 8 del decreto legislativo 12 febbraio 1993, n. 39.**
4. **Con regolamento ai sensi dell'artico 17, comma 1, della legge 23 agosto 1988, n. 400, da emanarsi sentita la Conferenza unificata di cui all'articolo 9 del decreto legislativo 28**

agosto 1997, n. 281 sono definite le modalità attraverso le quali le regioni e gli enti locali possono chiedere i pareri di cui al comma 3.

5. **Il C.N.I.P.A. , in particolare, fornisce supporto al Ministro per l'innovazione e le tecnologie ai fini della definizione delle politiche in materia di governo elettronico, di programmi di informatizzazione delle pubbliche amministrazioni e di formazione del personale delle pubbliche amministrazioni nel settore del settore delle tecnologie dell'informazione e comunicazione, cura l'attuazione delle suddette politiche anche attraverso la realizzazione di specifici programmi e progetti, nonché fornisce, nel quadro delle direttive impartite dal Ministro per l'innovazione e le tecnologie e in raccordo con il Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri, assistenza tecnica alle Regioni e agli enti locali per l'utilizzo dei fondi relativi alle politiche di innovazione.**

6. **Il C.N.I.P.A. , fermo restando l'adempimento dei propri fini istituzionali, può svolgere su convenzione attività di consulenza ed assistenza per le amministrazioni pubbliche.**

Art. 8

(Principi di organizzazione)

1. **Con regolamento ai sensi dell'articolo 17, comma 4-bis della legge 23 agosto 1988, n. 400, sono istituite presso le amministrazioni dello Stato strutture di livello dirigenziale generale per l'organizzazione, l'innovazione e le tecnologie.**
2. **Le strutture di cui al comma 1, assicurano l'attuazione delle linee strategiche della digitalizzazione dell'amministrazione definite dal Governo: a tal fine ad esse sono attribuiti i compiti relativi a:**
    a) **indirizzo e coordinamento strategico dello sviluppo dei sistemi informativi, in modo da assicurare anche la coerenza con gli *standard* tecnici e organizzativi comuni;**
    b) **indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi dell'amministrazione;**
    c) **indirizzo, coordinamento e monitoraggio della sicurezza informatica;**
    d) **verifica della coerenza tra l'organizzazione e l'attività dell'amministrazione e la diffusione delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrazione;**

e) **indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi;**

f) **progettazione e coordinamento delle iniziative rilevanti ai fini della cooperazione applicativa con altre amministrazioni pubbliche ivi inclusa la predisposizione e l'attuazione degli accordi di servizio con le altre amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;**

g) **indirizzo, coordinamento e monitoraggio delle iniziative attinenti all'attuazione delle direttive impartite dal Ministro per l'innovazione e le tecnologie;**

h) **pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di posta elettronica, protocollo informatico, firma digitale e mandato informatico;**

i) **valutazione degli investimenti effettuati nel settore.**

Art. 9

(Consigliere per l'innovazione e le tecnologie)

1. **Nelle amministrazioni dello Stato può essere istituito, nell'ambito degli uffici di diretta collaborazione di cui all'articolo 7 del decreto legislativo 30 luglio 1999, n. 300, il Consigliere per l'innovazione e le tecnologie.**
2. **Il Consigliere per l'innovazione e le tecnologie coadiuva il Ministro nell'esercizio delle funzioni di indirizzo politico-amministrativo di cui all'articolo 4, comma 1 del decreto legislativo 30 marzo 2001, n. 165, con riferimento all'introduzione ed all'utilizzo delle innovazioni tecnologiche e organizzative.**
3. **Il Consigliere per l'innovazione e le tecnologie è nominato, ai sensi dell'articolo 19 del decreto legislativo 30 marzo 2001, n. 165, tra i dirigenti di prima fascia dello Stato ed equiparati, i professori universitari di ruolo o fuori ruolo in servizio, ovvero tra esperti, appartenenti ad altre categorie o estranei alla pubblica amministrazione, dotati di elevata professionalità, e risponde direttamente all'organo di vertice politico. Se scelto tra i dipendenti statali o tra i docenti universitari, per l'intera durata dell'incarico, è collocato, rispettivamente, nella posizione di fuori ruolo e di aspettativa, secondo quanto previsto dai rispettivi ordinamenti.**

4. **Nell'ambito dei rispettivi ordinamenti, le altre amministrazioni pubbliche di cui all'articolo 1, comma 2, del citato decreto legislativo 30 marzo 2001, n.165, possono istituire il Consigliere per l'innovazione e le tecnologie.**

Art. 10

(Conferenza permanente per l'innovazione e le tecnologie)

1. **Al fine di coordinare le politiche pubbliche per lo sviluppo e l'attuazione dell'innovazione tecnologica nelle amministrazioni dello Stato è istituita la Conferenza permanente per l'innovazione e le tecnologie.**
2. **La Conferenza permanente per l'innovazione e le tecnologie è presieduta dal Presidente del Centro nazionale per l'informatica nella pubblica amministrazione, ed è composta dai componenti dell'organo collegiale del predetto Centro, nonché dai dirigenti generali preposti alle strutture di cui all'articolo 7, comma 1, e, ove previsti, dai Consiglieri per l'innovazione e le tecnologie.**
3. **La Conferenza permanente per l'innovazione e le tecnologie si riunisce con cadenza almeno semestrale per la verifica dello stato di attuazione dei programmi in materia di innovazione e tecnologie e del piano triennale di cui all'articolo 9 del decreto legislativo 12 febbraio 1993, n. 39.**
4. **Il Ministro per l'innovazione e le tecnologie provvede, con proprio decreto, a disciplinare il funzionamento della Conferenza permanente per l'innovazione e le tecnologie.**

Capo II –DATI DELLE PUBBLICHE AMMINISTRAZIONI

Art. 11

(Tipologia dei dati)

1. **Ai fini del presente decreto si intende:**
   a) **per dato pubblico il dato conoscibile da chiunque;**
   b) **per dato delle amministrazioni pubbliche il dato formato, o comunque trattato da una amministrazione pubblica;**
   c) **per dato a conoscibilità limitata il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti.**

Art. 12

(Disponibilità dei dati)

1. **I dati delle amministrazioni pubbliche sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre amministrazioni pubbliche e dai privati; restano salvi i limiti alla conoscibilità dei dati previsti dalle leggi e dai regolamenti e le norme in materia di protezione dei dati personali.**
2. **Qualunque dato trattato da una amministrazione pubblica è utilizzabile da un'altra amministrazione pubblica nei limiti dell'esercizio delle proprie funzioni, nel rispetto della normativa sulla tutela della riservatezza e salvi i casi previsti dall'articolo 24 della legge 7 agosto 1990, n. 241.**
3. **Lo Stato promuove ed attua tutte le iniziative necessarie a rendere coerenti e ad uniformare le informazioni tra le amministrazioni pubbliche.**

Art. 13

(Conoscibilità dei dati)

1. La conoscenza dei dati dell'amministrazione pubblica avviene mediante:

- **a) partecipazione al procedimento amministrativo e accesso ai documenti amministrativi da parte del soggetto interessato ai sensi della legge 7 agosto 1990, n. 241;**
- **b) comunicazione da parte dell'amministrazione pubblica che tratta il dato nei confronti di uno o più destinatari determinati;**
- **c) diffusione da parte dell'amministrazione pubblica che tratta il dato nei confronti di soggetti indeterminati.**

2. La conoscenza dei dati ai sensi del comma 1 è resa possibile di norma attraverso l'uso delle tecnologie dell'informazione e della comunicazione.

Art. 14

(Sicurezza dei dati)

1. **Le amministrazioni pubbliche adottano opportune misure informatiche, tecnologiche, organizzative, logistiche e procedurali di sicurezza, secondo le regole dettate ai sensi dell'articolo … per garantire l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati.**
2. **Gli atti, i dati ed i documenti informatici delle amministrazioni pubbliche devono essere custoditi e controllati con modalità tali da ridurre i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della banca dati o dell'archivio.**

Capo III – DOCUMENTO INFORMATICO , FIRME ELETTRONICHE E GESTIONE DOCUMENTALE

Sezione I

Documento informatico

Art. 15

(Documento informatico)
(art. 8, commi 1, 2, 3, 4, dpr 445)

1. **Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.**
2. **Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge, se conformi alle disposizioni vigenti.**
3. **Il documento informatico soddisfa il requisito legale della forma scritta se formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo … che garantiscano l'inalterabilità nel tempo del contenuto.**
4. Le regole tecniche per la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici sono stabilite ai sensi dell'articolo…
5. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico, anche con riferimento all'eventuale uso di chiavi biometriche di cui all'articolo 22, lettera e).
6. Restano ferme le disposizioni di legge in materia di protezione dei dati personali.

Art. 16

(Valore probatorio del documento informatico sottoscritto)
(art. 10 + 29-quater dpr 445)

1. **L'efficacia probatoria del** documento informatico, formato ai sensi dell'articolo 14, comma 3, sottoscritto con una firma elettronica, **è valutata ai sensi dei commi 2 e 3.**
2. Il documento informatico, sottoscritto con firma elettronica **o con firma elettronica avanzata** sul piano probatorio è liberamente valutabile tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza. Esso inoltre soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.
3. **La firma digitale apposta ad un documento ne garantisce la provenienza, l'autenticità e l'integrità.**
4. Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica **qualificata**, fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto **se colui contro il quale è prodotta non la disconosce.**
5. L'apposizione ad un documento informatico di una firma elettronica basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.
6. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su di un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:
   a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, ed è accreditato in uno Stato membro;
   b) il certificato qualificato è garantito da un certificatore stabilito nella Comunità europea, in possesso dei requisiti di cui alla medesima direttiva;
   c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra la Comunità e Paesi terzi o organizzazioni internazionali.
7. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con decreto del Ministro dell'economia e delle finanze, **di concerto con il Ministro per l'innovazione e le tecnologie**.

Art. 17

(Documenti informatici delle amministrazioni pubbliche)
(art. 9, comma 1, 2 4, dpr 445 – il comma 3 è contenutoo nel capo IX)

1. Gli atti formati con strumenti informatici, i dati e i documenti informatici delle pubbliche amministrazioni, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge.
2. Nelle operazioni riguardanti le attività di produzione, immissione, conservazione, riproduzione e trasmissione di dati, documenti ed atti amministrativi con sistemi informatici e telematici, ivi compresa l'emanazione degli atti con i medesimi sistemi, devono essere indicati e resi facilmente individuabili sia i dati relativi alle amministrazioni interessate sia il soggetto che ha effettuato l'operazione.
3. Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite ai sensi dell'articolo … d'intesa con il Dipartimento della funzione pubblica ed il Ministero per i beni e le attività culturali, sentito il Garante per la protezione dei dati personali e, per il materiale classificato d'intesa con le Amministrazioni della difesa, dell'interno e dell'economia e delle finanze, rispettivamente competenti.

Art. 18

(Copie di atti e documenti informatici)
(dpr 445, art. 20, commi 1, 2, 3, 4)

1. **All'articolo 2712 del codice civile dopo le parole "riproduzioni fotografiche" è inserita la parola: ", informatiche".**
2. I duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi a tutti gli effetti di legge, **se conformi alle vigenti disposizioni tecniche.**
3. I documenti informatici contenenti copia o riproduzione di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata, da parte di colui che li spedisce o rilascia, **una firma digitale o altro tipo di firma elettronica qualificata**.
4. Le copie su supporto informatico di documenti, formati in origine su supporto cartaceo o, comunque, non informatico, sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è autenticata da un notaio o da altro pubblico

ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo ….

5. La spedizione o il rilascio di copie di atti e documenti di cui al comma 3 esonera dalla produzione e dalla esibizione dell'originale formato su supporto cartaceo quando richieste ad ogni effetto di legge.

Sezione II

Firme elettroniche

Art. 19

(Definizioni)

(art. 22 dpr 445)

1. Ai fini del presente decreto si intende per:

a) 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;

b) FIRMA ELETTRONICA AVANZATA, la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione **informatica**, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;

c) FIRMA ELETTRONICA QUALIFICATA la firma elettronica avanzata che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma;

d) FIRMA DIGITALE, un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, 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;

e) SISTEMA DI VALIDAZIONE, il sistema informatico e crittografico in grado di generare ed apporre la firma digitale o di verificarne la validità;

f) CHIAVI ASIMMETRICHE, la coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, utilizzate nell'ambito dei sistemi di validazione di documenti informatici;

g) CHIAVE PRIVATA, l'elemento della coppia di chiavi asimmetriche, **utilizzato** soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;

h) CHIAVE PUBBLICA, l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;

i) CHIAVE BIOMETRICA, la sequenza di codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità personale basati su specifiche caratteristiche fisiche dell'utente;

l) VALIDAZIONE TEMPORALE, il risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi;

m) INDIRIZZO ELETTRONICO, l'identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici;

n) CERTIFICATI ELETTRONICI, gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi;

o) CERTIFICATORE, il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;

p) CERTIFICATORE QUALIFICATO il certificatore che rilascia al pubblico certificati elettronici conformi ai requisiti indicati nel presente testo unico e nelle regole tecniche di cui all'articolo 8, comma 2;

q) CERTIFICATORE ACCREDITATO, il certificatore accreditato in Italia ovvero in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva n. 1999/93/CE, nonché ai sensi del presente testo unico;

r) CERTIFICATI QUALIFICATI, i certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva n. 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;

s) DATI PER LA CREAZIONE DI UNA FIRMA i dati peculiari, come codici o chiavi crittografiche private, utilizzati dal titolare per creare la firma elettronica;

t) DISPOSITIVO PER LA CREAZIONE DELLA FIRMA il programma informatico adeguatamente configurato (software) o l'apparato strumentale (hardware) usati per la creazione della firma elettronica;

u) DISPOSITIVO SICURO PER LA CREAZIONE DELLA FIRMA, l'apparato strumentale usato per la creazione della firma elettronica;

v) DATI PER LA VERIFICA DELLA FIRMA i dati peculiari, come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica;

z) DISPOSITIVO DI VERIFICA DELLA FIRMA il programma informatico (software) adeguatamente configurato o l'apparato strumentale (hardware) usati per effettuare la verifica della firma elettronica;

aa) ACCREDITAMENTO FACOLTATIVO, il riconoscimento del possesso, da parte del certificatore che l**o** richieda, dei requisiti del livello più elevato, in termini di qualità e di sicurezza;

bb) REVOCA DEL CERTIFICATO ELETTRONICO, l'operazione con cui il certificatore **fa cessare** la validità del certificato da un dato momento, in poi;

cc) SOSPENSIONE DEL CERTIFICATO ELETTRONICO, l'operazione con cui il certificatore sospende la validità del certificato per un periodo transitorio;

dd) VALIDITÀ DEL CERTIFICATO ELETTRONICO, l'efficacia e l'opponibilità al titolare dei dati in esso contenuti;

Art. 20

(Firma digitale)
(art. 23 dpr 445)

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.
2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.
3. Per la generazione della firma digitale deve adoperarsi una chiave privata la cui corrispondente chiave pubblica sia stata oggetto dell'emissione di un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.

4. Attraverso il certificato elettronico si devono rilevare, secondo le regole tecniche stabilite ai sensi dell'articolo …, la validità del certificato elettronico stesso, nonché gli elementi identificativi del titolare e del certificatore.

Art. 21

(Firma autenticata)
(art. 24, commi 1, 2, 3 e 4 dpr 445)

1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale **o altro tipo di firma elettronica qualificata** autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.
2. L'autenticazione della firma digitale **o di altro tipo di firma elettronica qualificata** consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità della chiave utilizzata e del fatto che il documento sottoscritto risponde alla volontà della parte e non è in contrasto con l'ordinamento giuridico.
3. L'apposizione della firma digitale **o di altro tipo di firma elettronica qualificata** da parte del pubblico ufficiale integra e sostituisce ad ogni fine di legge la apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti.
4. Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 20, comma 3.

Art. 22

(Firma di documenti informatici delle pubbliche amministrazioni)
(art. 25 dpr 445 modificato)

1. **Le comunicazioni tra amministrazioni pubbliche, concessionarie di pubblici servizi, regioni ed enti locali e le comunicazioni interne tra le medesime sottoscritte con una delle firme elettroniche di cui al presente decreto sono valide ai fini del procedimento amministrativo.**
2. **Per gli atti dai quali possano nascere diritti, doveri, legittime aspettative di terzi, la firma autografa o la firma, comunque prevista, è sostituita dalla firma digitale, in conformità alle norme del presente decreto.**

Art. 23

Certificatori
(art. 26 dpr 445)

1. L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva. Detti certificatori o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione, devono possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in materia bancaria e creditizia, approvato con decreto legislativo 1° settembre 1993, n. 385.
2. L'accertamento successivo dell'assenza o del venir meno dei requisiti di cui al comma 1 comporta il divieto di prosecuzione dell'attività intrapresa.
3. Ai certificatori qualificati e ai certificatori accreditati che hanno sede stabile in altri Stati membri dell'Unione europea non si applicano le norme del presente decreto e le relative norme tecniche di cui all'articolo 8, comma 2, e si applicano le rispettive norme di recepimento della direttiva 1999/93/CE.

Art. 24

(Certificatori qualificati)
(art. 27 dpr 445)

1. I certificatori che rilasciano al pubblico certificati qualificati devono trovarsi nelle condizioni previste dall'articolo 26.
2. I certificatori di cui al comma 1 devono inoltre:

   a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione;

   b) **utilizzare** personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia delle firme elettroniche e della dimestichezza con procedure di sicurezza appropriate, e che sia in grado di rispettare le norme del presente **decreto** e le regole tecniche di cui all'articolo 8, comma 2;

c) applicare procedure e metodi amministrativi e di gestione adeguati e conformi a tecniche consolidate;

d) utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo e internazionale e certificati ai sensi dello schema nazionale di cui all'articolo 10, comma 1, del decreto legislativo 23 gennaio 2002, n. 10;

e) adottare adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi **crittografiche** nei casi in cui il certificatore generi tali chiavi.

3. I certificatori di cui al comma 1 devono comunicare, prima dell'inizio dell'attività, anche in via telematica, una dichiarazione di inizio di attività al Dipartimento dell'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri, attestante l'esistenza dei presupposti e dei requisiti previsti dal presente **decreto**.

4.Il Dipartimento procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la sussistenza dei presupposti e dei requisiti previsti dal presente **decreto** e dispone, se del caso, con provvedimento motivato da notificare all'interessato, il divieto di prosecuzione dell'attività, salvo che, ove ciò sia possibile, l'interessato provveda a conformare alla normativa vigente detta attività ed i suoi effetti entro il termine prefissatogli dall'amministrazione stessa.

Art. 25

(Certificati qualificati)
(art. 27-bis dpr 445)

1. I certificati qualificati devono contenere almeno le seguenti informazioni:

a) indicazione che il certificato elettronico rilasciato è un certificato qualificato;

b) numero di serie o altro codice identificativo del certificato;

c) nome, ragione o denominazione sociale del certificatore **che ha rilasciato il certificato** e lo Stato nel quale è stabilito;

d) nome, cognome e codice fiscale del titolare del certificato o uno pseudonimo chiaramente identificato come tale;

e) dati per la verifica della firma corrispondenti ai dati per la creazione della stessa in possesso del titolare;

f) indicazione del termine iniziale e finale del periodo di validità del certificato;

g) firma elettronica avanzata del certificatore che ha rilasciato il certificato.

2. In aggiunta alle informazioni di cui al comma 1, fatta salva la possibilità di utilizzare uno pseudonimo, per i titolari residenti all'estero cui non risulti attribuito il codice fiscale, si deve indicare il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di sicurezza sociale o un codice identificativo generale.

3. Il certificato qualificato può inoltre contenere, su domanda del titolare o del terzo interessato, le seguenti informazioni, se pertinenti allo scopo per il quale il certificato è richiesto:

a) le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;

b) limiti d'uso del certificato, ai sensi dell'articolo 28-bis, comma 3;

c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili.

Art. 26

(Accreditamento)
(art. 28 dpr 445)

1. I certificatori che intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, possono chiedere di essere accreditati presso la Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, che a tali fini può avvalersi delle strutture pubbliche di cui all'articolo 29.
2. Il richiedente deve rispondere ai requisiti di cui all'articolo 27 ed allegare alla domanda oltre ai documenti indicati nel medesimo articolo il profilo professionale del personale responsabile della generazione dei dati per la creazione e per la verifica della firma, della emissione dei certificati e della gestione del registro dei certificati nonché l'impegno al rispetto delle regole di tecniche.
3. Il richiedente, se soggetto privato, in aggiunta a quanto previsto dal comma 2, deve inoltre:

a) avere natura giuridica di società di capitali e un capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione alla attività bancaria ai sensi dell'articolo 14 del testo unico delle leggi in materia bancaria e creditizia, approvato con decreto legislativo 1° settembre 1993, n. 385;

b) garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e dei componenti **gli organi preposti al controllo**, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di

amministrazione, direzione e controllo presso banche ai sensi dell'articolo 26 citato del decreto legislativo 1° settembre 1993, n. 385.

4. La domanda di accreditamento si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.
5. Il termine di cui al comma 4 può essere **sospeso** una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità del Dipartimento per l'innovazione e le tecnologie o che questo non possa acquisire autonomamente. In tal caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.
6. A seguito dell'accoglimento della domanda, il Dipartimento per l'innovazione e le tecnologie dispone l'iscrizione del richiedente in un apposito elenco pubblico, tenuto dal Dipartimento stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.
7. Il certificatore accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni.

Art. 27

(Responsabilità del certificatore)
(art. 28-bis dpr 445)

1. Il certificatore che rilascia al pubblico un certificato qualificato o che garantisce al pubblico l'affidabilità del certificato è responsabile, se non prova d'aver agito senza colpa, del danno cagionato a chi abbia fatto ragionevole affidamento:
    a) sull'esattezza e sulla completezza delle informazioni necessarie alla verifica della firma in esso contenute alla data del rilascio e sulla loro completezza rispetto ai requisiti fissati per i certificati qualificati;
    b) sul possesso – da parte del firmatario – dei dati e degli strumenti necessari per la generazione della firma sulla garanzia che al momento del rilascio del certificato il firmatario detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato;
    c) sulla garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare, nei casi in cui il certificatore generi entrambi;
    d) sull'adempimento degli obblighi previsti dall'articolo 28.

2. Il certificatore che rilascia al pubblico un certificato qualificato è responsabile, nei confronti dei terzi che facciano ragionevole affidamento sul certificato stesso, dei danni provocati per effetto della mancata **o non tempestiva** registrazione della revoca o non tempestiva sospensione del certificato, salvo che provi d'aver agito senza colpa.
3. **Il certificato qualificato può contenere limiti d'uso** ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, purché i limiti d'uso o il valore limite siano riconoscibili da parte dei terzi. Il certificatore non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.

Art. 28

(Vigilanza sull'attività di certificazione)
(art. 29 dpr 445)

1. La Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, svolge funzioni di vigilanza e controllo sull'attività di certificazione, anche attraverso le strutture di cui si avvale il Ministro per l'innovazione e le tecnologie.
2. Fatto salvo quanto previsto dal comma 1, il Dipartimento per l'innovazione e le tecnologie provvede al controllo periodico dei certificatori accreditati.

Art. 29

(Obblighi del titolare e del certificatore)
(art. 29-bis dpr 445)

1. **Il titolare del certificato di firma è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri ed a custodire e utilizzare il dispositivo sicuro per la creazione della firma con la diligenza del buon padre di famiglia.**
2. Il certificatore è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.
3. Il certificatore che rilascia, ai sensi dell'articolo 27, certificati qualificati deve inoltre:
    a) identificare con certezza la persona che fa richiesta della certificazione;
    b) rilasciare e rendere pubblico il certificato elettronico nei modi e nei casi stabiliti dalle regole tecniche di cui all'articolo …, nel rispetto del decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni;

c) specificare, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della sussistenza degli stessi;

d) attenersi alle regole tecniche di cui all'articolo …;

e) informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;

f) adottare le misure di sicurezza per il trattamento dei dati personali, ai sensi dell'articolo 29, comma 9, decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni;

g) non rendersi depositario di dati per la creazione della firma del titolare;

h) procedere alla **tempestiva** pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri **del titolare**, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni;

i) garantire il funzionamento efficiente, puntuale e sicuro dei servizi di elencazione, nonché garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo;

l) assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;

m) tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per dieci anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;

n) non copiare, né conservare le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione;

o) predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il certificatore;

p) utilizzare sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato.

4. **Il certificatore è responsabile dell'identificazione del richiedente il certificato qualificato di firma anche se tale attività è delegata a terzi.**
5. **I dati personali raccolti per il rilascio dei certificati qualificati sono sottoposti alla disciplina in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.**

Art. 30

(Uso di pseudonimi)
(art. 29-ter dpr 445)

1. In luogo del nome del titolare il certificatore può riportare sul certificato elettronico uno pseudonimo, qualificandolo come tale. Se il certificato è qualificato, il certificatore ha l'obbligo di conservare le informazioni relative alla reale identità del titolare per almeno dieci anni dopo la scadenza del certificato stesso.

Art. 31

(Norme particolari per le pubbliche amministrazioni e per altri soggetti qualificati)
(art. 29-quinquies dpr 445)

1. Ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni:

   a) possono svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tale fine l'obbligo di accreditarsi ai sensi dell'articolo 28; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici o privati. I certificati qualificati rilasciati in favore di categorie di terzi possono essere utilizzati soltanto nei rapporti con l'Amministrazione certificante, al di fuori dei quali sono privi di ogni effetto; con decreto del Presidente del Consiglio dei Ministri, su proposta dei Ministri per la funzione pubblica e per l'innovazione e le tecnologie e

dei Ministri interessati, di concerto con il Ministro dell'economia e delle finanze, sono definite le categorie di terzi e le caratteristiche dei certificati qualificati;

b) possono rivolgersi a certificatori accreditati, secondo la vigente normativa in materia di contratti pubblici.

2. Per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo ….
3. Le regole tecniche concernenti la qualifica di pubblico ufficiale, l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni sono emanate con decreti del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica, con il Ministro della giustizia e con gli altri Ministri di volta in volta interessati, sulla base dei princìpi generali stabiliti dai rispettivi ordinamenti.
4. Nelle more della definizione delle specifiche regole tecniche di cui al comma 3, si applicano le norme tecniche di cui all'articolo ….

Art. 32

(Dispositivi sicuri e procedure per la generazione della firma)
(art. 29-sexies dpr 445)

1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:

   a) sia riservata;

   b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni;

   c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.
2. I dispositivi sicuri di cui al comma 1 devono garantire l'integrità dei dati elettronici a cui la firma si riferisce. I dati devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma.
3. Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica, purché l'attivazione della procedura sia chiaramente riconducibile alla volontà del titolare.
4. I dispositivi sicuri di firma sono sottoposti alla valutazione e certificazione di sicurezza ai sensi dello schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione di cui all'articolo 10, comma 1, del decreto legislativo 23 gennaio 2002, n. 10.

Art. 33

(Revoca e sospensione dei certificati qualificati)
(art. 29-septies dpr 445)

1. Il certificato qualificato deve essere a cura del certificatore:

   a) revocato in caso di cessazione dell'attività del certificatore **salvo quanto previsto dall'articolo *successivo*, comma 2**;

   b) revocato o sospeso in esecuzione di un provvedimento dell'autorità;

   c) revocato o sospeso a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare, secondo le modalità previste nel presente decreto;

   d) revocato o sospeso in presenza di cause limitative della capacità del titolare o di abusi o falsificazioni.
2. Il certificato qualificato può, inoltre, essere revocato o sospeso nei casi previsti dalle regole tecniche di cui all'articolo ….
3. La revoca o la sospensione del certificato qualificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione della lista che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale.
4. Le modalità di revoca o sospensione sono previste nelle regole tecniche di cui all'articolo ….

Art. 34

(Cessazione dell'attività)
(art. 29-octies dpr 445)

1. Il certificatore qualificato o accreditato che intende cessare l'attività deve, almeno sessanta giorni prima della data di cessazione, darne avviso al Dipartimento per l'innovazione e le tecnologie, informando senza indugio i titolari dei certificati da lui emessi specificando che tutti i certificati non scaduti al momento della cessazione saranno revocati.
2. Il certificatore di cui al comma 1 comunica contestualmente la rilevazione della documentazione da parte di altro certificatore o l'annullamento della stessa. L'indicazione di un certificatore sostitutivo non impone la revoca di tutti i certificati non scaduti al momento della cessazione.
3. Il certificatore di cui al comma 1 deve indicare altro depositario del registro dei certificati e della relativa documentazione.
4. Il Dipartimento rende nota la data di cessazione dell'attività del certificatore accreditato tramite l'elenco di cui all'articolo 28, comma 6.

Sezione III

Contratti, pagamenti, libri e scritture

Art. 35

Contratti stipulati con strumenti informatici o per via telematica
(art. 11 dpr 445)

1. **Ai contratti stipulati con strumenti informatici o per via telematica mediante l'uso della firma digitale o altro tipo di firma elettronica qualificata secondo le disposizioni del presente decreto si applicano le vigenti disposizioni in materia di contratti negoziati al di fuori dei locali commerciali.**
2. **Quando, secondo la legge o la volontà delle parti, un contratto deve essere provato per iscritto, ovvero nei casi in cui la forma scritta è richiesta sotto pena di nullità, l'apposizione o l'associazione al documento informatico della firma digitale o altro tipo di firma elettronica qualificata costituisce valida sottoscrizione.**

Art. 36

(Pagamenti informatici)
(art. 12 dpr 445)

1. Il trasferimento in via telematica di fondi tra pubbliche amministrazioni e tra queste e soggetti privati è effettuato secondo **le regole tecniche stabilite ai sensi dell'articolo …** di concerto con i Ministri per la funzione pubblica, della giustizia e dell'economia e delle finanze, sentiti il Garante per la protezione dei dati personali e la Banca d'Italia.

Art. 37

(Libri e scritture)
(art. 13 dpr 445)

1. I libri, i repertori e le scritture, ivi compresi quelli previsti dalla legge sull'ordinamento del notariato e degli archivi notarili, di cui sia obbligatoria la tenuta possono essere formati e conservati su supporti informatici in conformità alle disposizioni del presente **decreto** e secondo le regole tecniche stabilite ai sensi dell'articolo ….

Sezione IV

Gestione dei documenti e protocollo

Art. 38

(Protocollazione con sistemi automatizzati)

1. **La gestione dei documenti ed il protocollo dei documenti formati dalle amministrazioni pubbliche o, comunque, dalle stesse utilizzati è effettuata mediante sistemi informativi automatizzati.**
2. **Per area organizzativa omogenea, di seguito AOO, si intende un insieme di unità organizzative dell'amministrazione che usufruiscono, in modo omogeneo e coordinato, degli stessi servizi per la gestione dei documenti ed il protocollo.**
3. **Ciascuna area organizzativa omogenea è provvista di un servizio di protocollazione dei documenti in entrata ed in uscita che avviene utilizzando una unica sequenza numerica, rinnovata ad ogni anno solare, propria all'area stessa.**

Art. 39

(Regole tecniche sul protocollo)

1. Le regole tecniche, i criteri e le specifiche delle informazioni per la gestione dei documenti e per le operazioni di registrazione di protocollo, per la predisposizione del manuale di gestione, per le caratteristiche della segnatura di protocollo, per le procedure di salvataggio e conservazione dei documenti sono stabilite con decreto ai sensi dell'articolo … di concerto con il Ministro per la funzione pubblica.

Art. 40

(Registrazione di protocollo)
(art. 53, commi 1, 2)

1. La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione di informazioni **registrate in forma non modificabile.**
2. Il sistema deve consentire la produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

3. Sono oggetto di registrazione **informatica** obbligatoria i documenti ricevuti e spediti dall'amministrazione **formati su qualsiasi tipo di supporto**.
4. **Le amministrazioni pubbliche centrali adottano un manuale di gestione per la registrazione di protocollo.**

Art. 41

(Segnatura di protocollo)
(art. 55, comma 1 solo in parte)

1. La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso; essa consente di individuare ciascun documento in modo inequivocabile.

Art. 42

(Procedure di salvataggio e conservazione delle informazioni del sistema)
(art. 62 commi 2, 3 e 4 e art. 70 dpr 445)

1. È consentito il trasferimento delle informazioni di protocollo relative ai fascicoli che fanno riferimento a procedimenti conclusi su qualsiasi tipo di supporto informatico.
2. Le pubbliche amministrazioni devono assicurare, per ogni aggiornamento del sistema, il pieno recupero e la riutilizzazione delle informazioni, **da conservare,** acquisite con le versioni precedenti.
3. Le informazioni trasferite sono sempre consultabili. A tal fine, la riproduzione delle informazioni del protocollo è effettuata con adeguata cadenza ed in relazione all'evoluzione delle conoscenze scientifiche e tecnologiche, **secondo le procedure di conservazione e sostituzione previste nelle regole tecniche.**

Art. 43

(Informazioni annullate)

1. **Le informazioni concernenti la registrazione di protocollo possono essere annullate esclusivamente secondo la procedura prevista nelle regole tecniche di cui all'articolo 40.**

Art. 44

(Registro di emergenza)
(art. 63 dpr 445)

1. Qualora per cause tecniche non sia possibile utilizzare la normale procedura informatica le operazioni di registrazione di protocollo sono effettuate sul registro di emergenza.

Art. 45

(Sistema di gestione informatica dei documenti)
(art. 52 dpr 445)

1. Il sistema di gestione informatica dei documenti, **ove previsto,** deve:

   a) presentare i requisiti di sicurezza ed integrità;

   b) garantire la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita;

   c) fornire informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali;

   d) consentire il reperimento delle informazioni riguardanti i documenti registrati;

   e) consentire, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di tutela delle persone e di altri soggetti **relativamente** al trattamento dei dati personali;

   f) garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Art. 46

(Specificazione delle informazioni previste dal sistema di gestione dei flussi documentali)
(art. 66 dpr 445)

1. Le regole tecniche, i criteri e le specifiche delle informazioni previste, delle operazioni di registrazione e del formato dei dati relativi ai sistemi informatici per la gestione dei flussi documentali sono specificate **nelle regole tecniche di cui all'articolo …** di concerto con il Ministro della funzione pubblica.

Capo IV - CONSERVAZIONE DEI DOCUMENTI

Art. 47

(Sviluppo dei sistemi informativi delle pubbliche amministrazioni)
(art. 51 comma 3 dpr 445)

1. Le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, **nel rispetto delle regole tecniche sulla conservazione sostitutiva…**

Art. 48

(Riproduzione e conservazione dei documenti)
(art. 6, commi 1,2 (modificati) 3 e 4 dpr 445)

1. **I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento, di cui è prescritta la conservazione per legge o regolamento, sono validi e rilevanti a tutti gli effetti di legge, se riprodotti su supporti informatici idonei a garantire la conformità dei documenti agli originali e la conservazione nel tempo dei documenti medesimi, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo… ed in funzione dei principi di cui all'articolo 2, comma 1.**
2. **Non è consentita la conservazione cartacea dei documenti creati o trasmessi in forma digitale.**
3. I limiti e le modalità tecniche della riproduzione e dell'autenticazione dei documenti riprodotti ai sensi del comma 1 sono stabiliti nelle regole tecniche **ai sensi dell'**articolo…
4. Sono fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle amministrazioni pubbliche e sugli archivi privati dichiarati di notevole interesse storico ai sensi delle disposizioni del capo II del decreto legislativo 29 ottobre 1999, n. 490.

Sezione V
Procedimenti amministrativi gestiti con modalità digitali

Art. 49

(Procedimento amministrativo informatizzato)

1. **Il procedimento amministrativo come disciplinato dalla legge 7 agosto 1990, n. 241, è attuato e gestito per mezzo delle tecnologie dell'informazione e delle comunicazioni.**
2. **Gli atti del procedimento sono formati ovvero, se originariamente formati su diverso supporto, trasposti su supporto informatico e sono raccolti in fascicoli virtuali.**
3. **L'Amministrazione pubblica titolare del procedimento raccoglie nel fascicolo virtuale tutti gli atti del procedimento medesimo da chiunque formati; all'atto della comunicazione dell'avvio del procedimento ai sensi dell'articolo 8 della legge 7 agosto 1990, n. 241 comunica agli interessati le modalità per esercitare in via telematica i diritti di cui all'articolo 10 della citata legge 7 agosto 1990, n. 241.**

Capo V – TRASMISSIONE

Art. 50

Trasmissione del documento informatico
(articolo 43, comma 6 del 445 + art. 14 dpr 445, anche come modificato dal dpr posta certificata)

1.I documenti trasmessi da chiunque ad una pubblica amministrazione tramite fax, o con altro 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.

2.Per indirizzo elettronico si intende una casella di posta elettronica idonea ad identificare una risorsa tecnologica in grado di trasmettere, ricevere e mantenere a disposizione messaggi di posta elettronica.

3.Il documento informatico trasmesso per via telematica si intende inviato dal mittente se trasmesso, e si intende consegnato al destinatario, se disponibile all'indirizzo elettronico da questi dichiarato.

4.La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alle disposizioni del presente codice e conformemente alle regole tecniche di cui all'articolo …, sono opponibili ai terzi.

Art. 51

(Trasmissione dei documenti attraverso la posta elettronica nelle pubbliche amministrazioni)

1. **Le comunicazioni tra amministrazioni pubbliche, enti pubblici, regioni ed enti locali avvengono mediante l'utilizzo della posta elettronica; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.**
2. **Ai fini della verifica della provenienza le comunicazioni sono valide se:**
   a) **sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;**
   b) **ovvero sono dotate di protocollo informatizzato;**
   c) **ovvero se è comunque possibile accertarne altrimenti la provenienza.**

Art. 52

(Posta elettronica certificata)
(art. 14, comma 3 dpr 445)

1. **Le comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avvengono mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica ggmmaa, n. …**
2. La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.

Art. 53

Segretezza della corrispondenza trasmessa per via telematica
(art. 17 dpr 445)

1. Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.
2. Agli effetti del presente **decreto**, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario

Capo VI – SERVIZI AI CITTADINI E ALLE IMPRESE

Art. 54

(Organizzazione e finalità dei servizi in linea)

1. **Le amministrazioni pubbliche individuano le modalità di erogazione dei servizi in linea in base a criteri di valutazione di efficacia, economicità ed utilità, tenendo comunque presenti le dimensioni dell'utenza, la frequenza dell'uso e l'eventuale destinazione all'utilizzazione da parte di categorie in situazioni di disagio.**
2. **Le amministrazioni pubbliche progettano e realizzano i servizi in linea mirando alla ottimale soddisfazione delle esigenze degli utenti, in particolare garantendo la completezza del processo, la certificazione dell'esito e l'accertamento del grado di soddisfazione dell'utente.**
3. **Le amministrazioni collaborano per integrare i procedimenti di rispettiva competenza al fine di agevolare gli adempimenti di cittadini ed imprese e rendere più efficienti i processi che interessano più amministrazioni, attraverso idonei sistemi di cooperazione.**

Art. 55

(Caratteristiche dei siti)
(art. 11 testo C)

1. **Le amministrazioni pubbliche realizzano siti istituzionali su reti telematiche che rispettano i principi di usabilità, reperibilità, accessibilità anche da parte delle persone disabili, completezza di informazione, chiarezza di linguaggio, affidabilità, semplicità di consultazione, qualità, omogeneità ed interoperabilità.**
2. **Lo Stato promuove intese ed azioni comuni con le regioni e gli enti locali affinché realizzino siti istituzionali con le caratteristiche di cui al comma 1.**

Art. 56

(Dati pubblici contenuti nei siti)

1. **Le amministrazioni pubbliche pubblicano su siti telematici accessibili i documenti di cui all'articolo 26 della legge 7 agosto 1990, n. 241,** le direttive, i programmi, le istruzioni, le circolari e ogni atto che dispone in generale sulla organizzazione, sulle funzioni, sugli obiettivi, sui procedimenti di una pubblica amministrazione ovvero nel quale si determina l'interpretazione di norme giuridiche o si dettano disposizioni per l'applicazione di esse **comunque tutti i documenti, anche normativi, utili per rendere note le informazioni anche di interesse di cittadini e imprese concernenti la propria attività ed organizzazione nonché il settore dell'ordinamento giuridico riferibile all'attività da essi svolta.**
2. **Le amministrazioni pubbliche garantiscono che le informazioni contenute sui siti siano conformi e corrispondenti alle informazioni contenute nei provvedimenti amministrativi originali dei quali si fornisce comunicazione tramite il sito.**

Art. 57

(Moduli e formulari)
(art. 9, comma 3 dpr 445)

1. Le pubbliche amministrazioni provvedono a definire e a rendere disponibili per via telematica moduli e formulari elettronici validi ad ogni effetto di legge, **anche ai fini delle autocertificazione e delle dichiarazioni sostitutive di notorietà.**
2. **Trascorsi 24 mesi dall'entrata in vigore del presente decreto i documenti non pubblicati sul sito non sono validi ed i relativi procedimenti possono essere conclusi anche in assenza dei suddetti documenti.**

Art. 58

(Accesso alle reti di comunicazione elettronica)

1. **Ai fini del presente decreto si intende per:**
   a) **identificazione informatica l'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto che ne distinguono l'identità in rete;**
   b) **validazione informatica la verifica dell'identità dell'utilizzatore della rete attraverso opportune tecnologie al fine di garantire la sicurezza dell'accesso;**
   ~~c)~~ **autorizzazione informatica la verifica, attraverso opportune tecnologie della corrispondenza delle abilitazioni esistenti tra il soggetto richiedente ed il tipo di operazione che il soggetto intende eseguire.**

Art. 59

(Certificato di autenticazione)

1. **Per certificato di autenticazione si intende l'attestato elettronico che assicura l'autenticità delle informazioni necessarie per l'identificazione in rete del titolare della carta nazionale dei servizi.**

Art. 60

(Accesso telematico ai dati e documenti pubblici)

1. **L'accesso telematico a dati, documenti e procedure è disciplinato dalle pubbliche amministrazioni secondo le disposizioni del presente decreto e nel rispetto delle disposizioni di legge e di regolamento in materia di protezione dei dati personali, di accesso ai documenti amministrativi, di tutela del segreto e di divieto di divulgazione. I regolamenti che disciplinano l'esercizio del diritto di accesso sono pubblicati su pubblici siti accessibili per via telematica.**

Art. 61

(Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni)
(art. 36, commi 1,2, 3, 4, 5, 6 dpr 445 ***ricorda di non abrogare il comma 7*** *)*

1. **Costituiscono strumento per l'accesso ai servizi erogati in rete dalle amministrazioni pubbliche la Carta d'identità elettronica e la Carta nazionale dei servizi.**
2. **Le amministrazioni pubbliche possono consentire l'accesso ai servizi in rete da esse erogati anche con strumenti diversi dalla Carta d'identità elettronica e dalla Carta nazionale dei servizi, purché tali strumenti consentano l'identificazione e l'autenticazione del soggetto. L'accesso con Carta d'identità elettronica e Carta nazionale dei servizi è consentito indipendentemente dalle modalità di accesso predisposte dalle amministrazioni.**
3. **Con decreto del Presidente del Consiglio dei ministri o per sua delega del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica è fissata la data dalla quale non è più consentito l'accesso ai servizi erogati in rete dalle amministrazioni pubbliche con tecnologie diverse dalla Carta d'identità elettronica e la Carta nazionale dei servizi.**

4. Le caratteristiche e le modalità per il rilascio, **per la diffusione e l'uso** della carta d'identità elettronica, del documento d'identità elettronico e della carta nazionale dei servizi sono definite con decreto del Presidente del Consiglio dei Ministri, adottato su proposta del Ministro dell'interno, di concerto con il Ministro per la funzione pubblica, con il Ministro per l'innovazione e le tecnologie e con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali**.**

5. La carta d'identità elettronica e l'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento del quindicesimo anno, devono contenere:

   a) i dati identificativi della persona;

   b) il codice fiscale;

6. La carta d'identità elettronica e l'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento del quindicesimo anno, possono contenere:

   a) l'indicazione del gruppo sanguigno;

   b) le opzioni di carattere sanitario previste dalla legge;

   c) i dati biometrici indicati col decreto di cui al comma 1, con esclusione, in ogni caso, del DNA;

   d) tutti gli altri dati utili al fine di razionalizzare e semplificare l'azione amministrativa e i servizi resi al cittadino, anche per mezzo dei portali, nel rispetto della normativa in materia di riservatezza;

   e) le procedure informatiche e le informazioni che possono o debbono essere conosciute dalla pubblica amministrazione e da altri soggetti, occorrenti per la firma elettronica.

7. La carta d'identità elettronica e la carta nazionale dei servizi possono essere utilizzate **quali strumenti di identificazione per l'effettuazione di** pagamenti tra soggetti privati e pubbliche amministrazioni, secondo le modalità stabilite con **le regole tecniche ai sensi dell'art…** di concerto con il Ministro dell'economia e delle finanze, sentita la Banca d'Italia.

8. Con decreto del Ministro dell'interno, del Ministro per l'innovazione e le tecnologie e del Ministro dell'economia e delle finanze, sentiti il Garante per la protezione dei dati personali e la Conferenza Stato-città ed autonomie locali, sono dettate le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della carta di identità elettronica, del documento di identità elettronico e della carta nazionale dei servizi, **nonché le modalità di impiego.**

9. Nel rispetto della disciplina generale fissata dai decreti di cui al presente articolo e delle vigenti disposizioni in materia di protezione dei dati personali, le pubbliche

amministrazioni, nell'ambito dei rispettivi ordinamenti, possono sperimentare modalità di utilizzazione dei documenti di cui al presente articolo per l'erogazione di ulteriori servizi o utilità.

Art. 62

(Istanze e dichiarazioni da presentare alla pubblica amministrazione)
*(art. 38 **solo il** comma 2 dpr 445)*

1. Le istanze e le dichiarazioni inviate per via telematica sono valide:

   a) se sottoscritte mediante la firma digitale, rilasciata da un certificatore accreditato;

   b) ovvero quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi**, di cui all'articolo 56, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente.**

2. **Le istanze e le dichiarazioni inviate secondo le modalità previste dal comma 1 sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento.**

Capo VII - FRUIBILITA'

Art. 63

(Nozione di fruibilità)

1. **Per fruibilità di un dato si intende la possibilità di utilizzare il dato anche trasferendolo nei propri sistemi informativi automatizzati.**
2. **Il trasferimento di un dato da un sistema informativo ad un altro non modifica la titolarità del dato.**

Art. 64

(Limiti e modalità della fruibilità del dato)

1. **Le amministrazioni pubbliche rendono accessibile e fruibile ad un'altra amministrazione i dati di cui siano titolari quando l'utilizzazione del dato sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente, nel rispetto della normativa in materia di protezione dei dati personali.**

2. **Le amministrazioni stipulano tra loro convenzioni finalizzate alla fruibilità informatica dei dati.**

Art. 65

(Dati territoriali)

1. **Per dato territoriale si intende qualunque informazione geograficamente localizzata.**
2. **Con intesa tra Stato, Regioni ed enti locali è istituito il Comitato per le regole tecniche sui dati territoriali delle amministrazioni pubbliche, con il compito di definire le regole tecniche per la realizzazione delle basi dei dati territoriali la documentazione, la fruibilità e lo scambio dei dati stessi tra le pubbliche amministrazioni centrali e locali.**
3. **Per agevolare la pubblicità dei dati di interesse generale, disponibili presso le pubbliche amministrazioni a livello nazionale, regionale e locale, presso il Centro nazionale per l'informatica nella pubblica amministrazione è istituito il Repertorio nazionale dei dati territoriali.**
4. **Con decreto ai sensi dell'articolo …, su proposta del Comitato per le regole tecniche sui dati territoriali delle amministrazioni pubbliche, sono definite le regole tecniche per la definizione del contenuto Repertorio nazionale dei dati territoriali, nonché delle modalità di prima costituzione e di successivo aggiornamento dello stesso, per la formazione, la documentazione e lo scambio dei dati territoriali detenuti dalle singole amministrazioni competenti, nonché le regole e gli oneri per l'utilizzo dei dati stessi tra le pubbliche amministrazioni centrali e locali e da parte dei privati.**