RACCOLTA COORDINATA IN MATERIA DI DOCUMENTO INFORMATICO, FIRMA ELETTRONICA E COMUNICAZIONE TELEMATICA CON L'AMMINISTRAZIONE

(aggiornata al 2 maggio 2023)

LEGGE 20 LUGLIO 2005 n.115

LEGGE SUL DOCUMENTO INFORMATICO E LA FIRMA ELETTRONICA

TESTO COORDINATO CON LE MODIFICHE DERIVANTI DA:
LEGGE 29 MAGGIO 2013 N.58
DECRETO DELEGATO 21 MARZO 2023 N.51

DECRETO 8 NOVEMBRE 2005 N.156

REGOLE TECNICHE PER LA FORMAZIONE, LA TRASMISSIONE, LA CONSERVAZIONE, LA DUPLICAZIONE, LA RIPRODUZIONE E LA VALIDAZIONE, ANCHE TEMPORALE, DEI DOCUMENTI INFORMATICI.

TESTO COORDINATO CON LE MODIFICHE DERIVANTI DA:
DECRETO DELEGATO 30 GENNAIO 2020 N.9
DECRETO DELEGATO 29 MARZO 2021 N.61
DECRETO DELEGATO 29 OTTOBRE 2021 N.184
DECRETO DELEGATO 21 MARZO 2023 N.51

DECRETO DELEGATO 21 marzo 2023 n.51

TESTO UNICO INNOVATIVO DELLE DISPOSIZIONI IN MATERIA DI COMUNICAZIONE TELEMATICA CON L'AMMINISTRAZIONE E DI ACCESSO AI SERVIZI IN LINEA DELL'AMMINISTRAZIONE

Sommario

ATTI NORMATIVI CITATI NEL TESTO COORDINATO

Legge 23 maggio 1995 n.70
Decreto 20 gennaio 2000 n.10
Legge 25 gennaio 2011 n.5
Legge 23 gennaio 2015 n.2
Legge 20 luglio 2005 n.115
Decreto 8 novembre 2005 n.156
Legge 22 dicembre 2010 n. 194
Legge 5 ottobre 2011 n. 159
Legge 5 ottobre 2011 n. 160
Legge 5 dicembre 2011 n. 188
Legge 11 maggio 2012 n. 50
Decreto Delegato 8 luglio 2013 n.81
Legge 29 luglio 2013 n.100
Decreto Delegato 2 marzo 2015 n.26
Decreto Delegato 9 dicembre 2015 n. 179
Decreto delegato 11 aprile 2016 n.46
Decreto Delegato 24 febbraio 2016 n.18
Legge 14 dicembre 2017 n.140
Regolamento 22 novembre 2018 n.7
Legge 31 ottobre 2018 n.137
Decreto Delegato 20 novembre 2018 n.146
Decreto Delegato 11 dicembre 2018 n.155
Decreto Delegato 26 luglio 2018 n. 92
Legge 31 ottobre 2018 n.137
Decreto Delegato 11 dicembre 2018 n.155
Regolamento 7 marzo 2019 n.3

Legge 30 maggio 2019 n.88
Decreto delegato 30 gennaio 2020 n.9
Legge 7 luglio 2020 n.113
Decreto Delegato 20 novembre 2020 n.204
Decreto Delegato 29 ottobre 2021 n.184
Decreto Delegato 15 settembre 2022 n.130
Decreto Delegato 21 marzo 2023 n.51

LEGGE 20 luglio 2005 n.115 - LEGGE SUL DOCUMENTO INFORMATICO E LA FIRMA ELETTRONICA

Art. 1
(Definizioni)

1. Ai fini della presente legge, valgono le seguenti definizioni:

a) "documento amministrativo", ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa;

b) "documento informatico", la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

c) "firma elettronica" ("digital signature"), dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di validazione;

d) "firma elettronica avanzata", una firma elettronica ottenuta attraverso una procedura informatica, che soddisfi i seguenti requisiti:
   I. essere connessa in maniera unica al firmatario;
   II. essere idonea ad identificare il firmatario;
   III. essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo;
   IV. essere collegata ai dati cui si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;

e) "firma elettronica qualificata", una firma elettronica avanzata che sia basata su di un certificato qualificato creato mediante un dispositivo sicuro per la creazione della firma;

f) "firmatario", una persona che ha accesso al dispositivo per la creazione di una firma e agisce per conto proprio o per conto della persona fisica o giuridica o dell'entità che rappresenta;

g) "dati per la creazione di una firma", dati peculiari, come codici o chiavi crittografiche private, utilizzati dal firmatario per creare una firma elettronica;

h) "dispositivo per la creazione di una firma", un software configurato o un hardware usato per utilizzare i dati per la creazione di una firma;

i) "dispositivo sicuro per la creazione di una firma", un dispositivo per la creazione di una firma che soddisfa i requisiti di cui all'articolo 7;

l) "dati per la verifica della firma", dati, come codici o chiavi crittografiche pubbliche, utilizzati per verificare una firma elettronica;

m) "servizio di firma e certificazione", la messa a disposizione di prodotti e procedure necessarie per la firma, l'emissione, il rinnovo e la gestione di certificati, servizi elenchi, servizi di revoca, servizi di registrazione e servizi di time stamping, nonché servizi informatici e di consulenza correlati alle firme elettroniche;

n) "dispositivo di verifica della firma", un software configurato o un hardware usato per utilizzare i dati di verifica della firma, secondo le raccomandazioni di cui al successivo articolo 8;

o) "certificato", un attestato elettronico che collega i dati di verifica della firma ad un titolare e conferma l'identità di tale titolare;

p) "certificato qualificato", un certificato elettronico conforme ai requisiti di cui all'articolo 4 rilasciato da un prestatore di servizi di certificazione che risponde ai requisiti di cui all'articolo 5;

q) "prestatore di servizi di certificazione" o "certificatore", un organismo o una persona fisica o giuridica che rilascia certificati o fornisce altri servizi connessi alle firme elettroniche;

r) "prodotto di firma elettronica", hardware o software, oppure i componenti pertinenti dei medesimi, destinati ad essere utilizzati da un prestatore di servizi di certificazione per la prestazione di servizi di firma elettronica oppure per la creazione o la verifica di firme

elettroniche;

s) "validazione temporale" o "time stamping", il risultato della procedura informatica, con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile a terzi;

t) "servizio di time stamping", una attestazione recante la firma elettronica di un certificatore che comprova l'esistenza di determinati dati elettronici in un determinato momento (data ed orario).

Art. 2

(Documento informatico e sua validità)

1. Gli atti, dati e documenti formati dalla Pubblica Amministrazione con strumenti informatici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione su supporto informatico e trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge, purché firmati e validati ai sensi della presente 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 pubbliche amministrazioni provvedono a definire e a rendere disponibili per via telematica moduli e formulari elettronici validi ad ogni effetto di legge.

4. Le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici saranno stabilite con specifici regolamenti tecnici da emanare mediante decreto reggenziale. [1]

Art. 3

(Effetti giuridici delle firme elettroniche)

1. L'uso di una firma elettronica apposta o associata mediante certificato revocato o scaduto equivale alla mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione da parte dei prestatori di servizi di certificazione.

2. La trasmissione del documento informatico per via telematica, firmato elettronicamente ai sensi dei regolamenti previsti dalla presente legge, con modalità che assicurino l'avvenuta consegna, equivale alla spedizione per mezzo posta raccomandata con avviso di ricevimento. [2]

---

[1] **Testo originario LEGGE 20 luglio 2005 n.115**

Art. 2, comma 1

1. Gli atti, dati e documenti formati dalla Pubblica Amministrazione e dai privati con strumenti informatici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione su supporto informatico e trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge, purché firmati e validati ai sensi della presente legge.

Modifiche legislative:

LEGGE 29 maggio 2013 N.58

Art. 30 (Abrogazioni)

Le parole “e dai privati” dell’articolo 2, comma 1 della Legge 20 luglio 2005 n.115 sono soppresse.

Sono abrogate tutte le disposizioni in contrasto con la presente legge.

[2] **Testo originario LEGGE 20 luglio 2005 n.115, Art. 3**

(Effetti giuridici delle firme elettroniche)

1. L'uso di una firma elettronica apposta o associata mediante certificato revocato o scaduto equivale alla mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione da parte dei prestatori di servizi di certificazione.

2. La trasmissione del documento informatico per via telematica, firmato elettronicamente ai sensi dei regolamenti previsti dalla presente legge, con modalità che assicurino l'avvenuta consegna, equivale alla spedizione per mezzo posta.

3. Le firme elettroniche qualificate basate su un certificato qualificato e create mediante un dispositivo sicuro per la creazione di una firma:

a) posseggono i requisiti legali di una firma in relazione ai dati in forma elettronica così come una firma autografa li possiede per i dati cartacei;
b) sono ammesse come prova in giudizio.

4. La firma elettronica non può essere considerata legalmente inefficace e inammissibile come prova in giudizio unicamente a causa del fatto che è:

-in forma elettronica, o
-non basata su un certificato qualificato, o
-non basata su un certificato qualificato rilasciato da un prestatore di servizi di certificazione accreditato, ovvero
-non creata da un dispositivo sicuro per la creazione di una firma. [3]

5. 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 ai regolamenti tecnici previsti dalla presente legge.

6. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente, si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se conformi ai regolamenti tecnici previsti dalla presente legge.

Art. 4

(Requisiti relativi ai certificati qualificati)

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

a) l'indicazione che il certificato rilasciato è un certificato qualificato;
b) l'identificazione del prestatore di servizi di certificazione e lo Stato in cui ha la propria sede;
c) il nome del firmatario o uno pseudonimo identificato come tale;
d) l'indicazione di un attributo specifico del firmatario, da includere se pertinente, a seconda dello scopo per cui il certificato è richiesto;

---

3. Le firme elettroniche qualificate basate su un certificato qualificato e create mediante un dispositivo sicuro per la creazione di una firma:

a) posseggono i requisiti legali di una firma in relazione ai dati in forma elettronica così come una firma autografa li possiede per i dati cartacei;
b) sono ammesse come prova in giudizio.

4. La firma elettronica non può essere considerata legalmente inefficace e inammissibile come prova in giudizio unicamente a causa del fatto che è:

-in forma elettronica, o
-non basata su un certificato qualificato, o
-non basata su un certificato qualificato rilasciato da un prestatore di servizi di certificazione accreditato, ovvero
-non creata da un dispositivo sicuro per la creazione di una firma.

5. 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 ai regolamenti tecnici previsti dalla presente legge.

6. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente, si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se conformi ai regolamenti tecnici previsti dalla presente legge.

Modifiche legislative:

DECRETO DELEGATO 21 marzo 2023 n.51, Art. 26, comma 2

2. Al termine dell'articolo 3, comma 2 della Legge n.115/2005 è aggiunta la seguente espressione "raccomandata con avviso di ricevimento".

[3] Vedi anche **DECRETO DELEGATO 30 gennaio 2020 n.9, art. 9 comma 6**

6. I documenti elettronici formati, acquisiti e gestiti da software in uso nell'Amministrazione che non prevedano l'utilizzo della firma elettronica qualificata bensì di firma elettronica semplice o avanzata, hanno il valore giuridico e probatorio di cui all'articolo 3, comma 4 della Legge n.115/2005 e, pertanto, sono liberamente valutabili in giudizio in relazione alle loro caratteristiche di sicurezza, integrità e immodificabilità.

e) i dati per la verifica della firma corrispondenti ai dati per la creazione della firma sotto il controllo del firmatario;
f) un'indicazione dell'inizio e del termine del periodo di validità del certificato;
g) il codice d'identificazione del certificato;
h) la firma elettronica qualificata del prestatore di servizi di certificazione che ha rilasciato il certificato;
i) i limiti d'uso del certificato, ove applicabili;
l) i limiti del valore dei negozi per i quali il certificato può essere usato, ove applicabili.

Art. 5

(Requisiti relativi al prestatore di servizi di certificazione che rilascia certificati qualificati)

1. Il prestatore di servizi di certificazione che rilascia certificati qualificati deve:
   a) dimostrare l'affidabilità organizzativa tecnica e finanziaria necessaria per fornire servizi di certificazione;
   b) assicurare il funzionamento di un servizio di gestione delle informazioni puntuale e sicuro e garantire un servizio di revoca sicuro e immediato;
   c) utilizzare nei certificati qualificati e per i servizi elenchi e per i servizi di revoca un time stamping di qualità garantita, e comunque assicurare la localizzazione temporale dell'emissione e della revoca di un certificato qualificato;
   d) verificare con mezzi appropriati, l'identità e, eventualmente, le specifiche caratteristiche della persona cui viene rilasciato un certificato qualificato;
   e) impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle qualifiche necessarie per i servizi forniti, in particolare la competenza a livello gestionale, la conoscenza specifica nel settore della tecnologia delle firme elettroniche e la dimestichezza con procedure di sicurezza appropriate; essi devono inoltre applicare procedure e metodi amministrativi e di gestione adeguati e corrispondenti a norme riconosciute;
   f) utilizzare sistemi affidabili e prodotti protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti di cui sono oggetto;
   g) adottare misure contro la contraffazione dei certificati e, nei casi in cui il prestatore di servizi di certificazione generi dati per la creazione di una firma, garantire la riservatezza, l'integrità e la sicurezza nel corso della generazione di tali dati;
   h) disporre di risorse finanziarie sufficienti ad operare secondo i requisiti previsti dalla legge, in particolare per sostenere il rischio di responsabilità per danni, ad esempio stipulando un'apposita assicurazione di responsabilità civile;
   i) tenere una registrazione di tutte le informazioni pertinenti relative ad un certificato qualificato per un periodo di almeno 10 anni, in particolare al fine di fornire la prova della certificazione in eventuali procedimenti giudiziari. Tali registrazioni possono essere elettroniche;
   l) non conservare né copiare i dati per la creazione della firma della persona cui il prestatore di servizi di certificazione ha fornito i servizi di gestione della chiave;
   m) prima di avviare un rapporto contrattuale con una persona che richieda un certificato a sostegno della sua firma elettronica, informarla con un mezzo di comunicazione durevole, degli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso e le procedure di reclamo e di risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte e utilizzare un linguaggio comprensibile. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato;
   n) utilizzare sistemi affidabili per memorizzare i certificati in modo verificabile e far sì che:
      I. soltanto le persone autorizzate possano effettuare inserimenti e modifiche;
      II. l'autenticità delle informazioni sia verificabile;

III. i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato;
IV. l'operatore possa rendersi conto di qualsiasi modifica tecnica che comprometta i requisiti di sicurezza.

Art. 6
(Responsabilità)

1. Il prestatore di servizi di certificazione che rilascia al pubblico un certificato come certificato qualificato o che garantisce al pubblico l'affidabilità di tale certificato, è responsabile per danni provocati a entità o persone fisiche o giuridiche che facciano ragionevole affidamento su detto certificato:
   a) per quanto riguarda l'esattezza di tutte le informazioni contenute nel certificato qualificato dal momento del rilascio e il fatto che esso contenga tutti i dati prescritti per un certificato qualificato,
   b) per la garanzia che, al momento del rilascio del certificato, il firmatario identificato nel certificato qualificato detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato,
   c) per la garanzia che i dati per la creazione della firma e i dati per la verifica della firma possano essere usati in modo complementare, nei casi in cui il fornitore di servizi di certificazione generi entrambi,

a meno che il prestatore di servizi di certificazione provi di aver agito senza negligenza.
2. Il prestatore di servizi di certificazione che rilascia al pubblico un certificato come certificato qualificato è responsabile, nei confronti di entità o di persone fisiche o giuridiche che facciano affidamento sul certificato, dei danni provocati, per la mancata registrazione della revoca del certificato, a meno che provi di aver agito senza negligenza.
3. Un prestatore di servizi di certificazione ha la facoltà di indicare, in un certificato qualificato, i limiti d'uso di detto certificato, purché tali limiti siano riconoscibili da parte dei terzi. Il prestatore di servizi di certificazione è esentato dalla responsabilità per i danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti nello stesso.
4. Un prestatore di servizi di certificazione ha la facoltà di indicare nel certificato qualificato un valore limite per i negozi per i quali può essere usato il certificato, purché tali limiti siano riconoscibili da parte dei terzi. Il prestatore di servizi di certificazione non è responsabile dei danni risultanti dal superamento di detto limite massimo.
5. Il prestatore di servizi di certificazione deve poter fornire, su richiesta, la marcatura temporale (time stamping), di adeguata precisione, di cui assicurerà la tenuta della registrazione per un congruo numero di anni come indicato da decreto reggenziale di cui all'articolo 2, punto 4.
6. 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 5; 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 reggenziale, saranno 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.

Art. 7
(Requisiti relativi ai dispositivi per la creazione di una firma elettronica qualificata)

1. I dispositivi per la creazione di una firma elettronica qualificata, mediante mezzi tecnici e procedurali appropriati, devono garantire almeno che:

a) i dati per la creazione della firma utilizzati nella generazione della stessa possono comparire in pratica solo una volta e che è garantita la loro riservatezza;
b) i dati per la creazione della firma utilizzati nella generazione della stessa non possono, entro i limiti di sicurezza previsti, essere derivati e la firma è protetta da contraffazioni compiute con l'impiego di tecnologia attualmente disponibile;
c) i dati per la creazione della firma utilizzati nella generazione della stessa sono sufficientemente protetti dal firmatario legittimo contro l'uso da parte di terzi.

2. I dispositivi sicuri per la creazione di una firma non devono alterare i dati da firmare né impedire che tali dati siano presentati al firmatario prima dell'operazione di firma; deve inoltre essere richiesta, senza ambiguità, la volontà di generare la firma.

Art. 8
(Raccomandazioni per la verifica della firma elettronica qualificata)

1. Durante il processo relativo alla verifica della firma elettronica qualificata occorre garantire, entro limiti di certezza, che:

a) i dati utilizzati per la verifica della firma corrispondono ai dati comunicati al verificatore;
b) la firma è verificata in modo affidabile e i risultati della verifica correttamente comunicati;
c) il verificatore può, all'occorrenza, stabilire in modo attendibile i contenuti dei dati firmati;
d) l'autenticità e la validità del certificato necessario al momento della verifica della firma sono verificate in modo attendibile;
e) i risultati della verifica e dell'identità del firmatario sono comunicati correttamente;
f) l'uso di uno pseudonimo è chiaramente indicato;
g) qualsiasi modifica che incida sulla sicurezza può essere individuata.

Art. 9
(Settore Pubblico)

1. All'interno della Pubblica Amministrazione e Settore Pubblico Allargato e per le comunicazioni tra organismi statali e persone fisiche o giuridiche, l'uso della firma elettronica può essere soggetto a requisiti specifici che saranno individuati dal regolamento tecnico da emanare mediante il decreto reggenziale di cui all'articolo 2, punto 4.

Art. 10
(Organismo tecnico)

1. Le competenze tecniche di attuazione della presente legge vengono espletate dall'Autorità per l'Informatica di cui alla Legge 23 maggio 1995 n.70, che si avvale del supporto tecnico dell'Ufficio Programmazione Economica Centro Elaborazione Dati e Statistica ed eventualmente della consulenza di persone o società esperte nelle problematiche concernenti la firma elettronica.

Art. 11
(Compiti affidati all'Autorità per l'Informatica)

1. E' compito dell'Autorità per l'Informatica promuovere i regolamenti tecnici da emanare con il decreto reggenziale di cui all'articolo 2, punto 4. Tali regolamenti dovranno tener conto degli standard emergenti a livello internazionale.
2. Almeno ogni due anni, a partire dalla pubblicazione del regolamento tecnico, l'Autorità per

l'Informatica provvede ad esaminare i progressi tecnologici, l'evoluzione del mercato e gli sviluppi giuridici a livello internazionale e provvede, se del caso, ad apportare le opportune modifiche al regolamento tecnico.
3. Ogni sei mesi, a partire dalla pubblicazione del regolamento tecnico, l'Autorità per l'Informatica provvede a pubblicare una lista degli Stati terzi la cui normativa sulla firma elettronica risulta conforme ai requisiti indicati nella presente legge e del regolamento tecnico.
4. E' compito dell'Autorità per l'Informatica, con il supporto tecnico dell'Ufficio Programmazione Economica Centro Elaborazione Dati e Statistica ed eventualmente della consulenza di persone o società esperte nelle problematiche concernenti la firma elettronica, svolgere funzioni di vigilanza e controllo sulle attività di certificazione e rilascio dei certificati svolte da parte del prestatore di servizi di certificazione.

Art. 12
(Aspetti internazionali)

1. Al fine di agevolare servizi di certificazione transfrontalieri con Paesi terzi e il riconoscimento giuridico delle firme elettroniche qualificate che hanno origine in Paesi terzi, l'Autorità per l'Informatica presenta, se del caso, proposte miranti all'effettiva attuazione di norme e di accordi internazionali applicabili ai servizi di certificazione.

Art. 13
(Protezione dei dati)

1. Il prestatore di servizi di certificazione e gli organismi responsabili dell'accreditamento o della supervisione si devono conformare alla Legge 23 maggio 1995 n. 70 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali.
2. È consentito a un prestatore di servizi di certificazione che rilascia certificati al pubblico di raccogliere dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono.

Art. 14
(Riesame)

1. Ogni due anni, a partire dall'entrata in vigore della presente legge, l'Autorità per l'Informatica riesamina l'applicazione della presente legge e presenta una relazione in merito al Consiglio Grande e Generale.
2. Nel riesame si valuta, tra l'altro, se l'ambito di applicazione della presente legge debba essere modificato per tener conto dei progressi tecnologici, dell'evoluzione del mercato e degli sviluppi giuridici. La relazione è corredata, se del caso, di proposte legislative.

Art. 15
(Entrata in vigore)

1. La presente legge entra in vigore il quinto giorno successivo a quello della sua legale pubblicazione.

DECRETO 8 novembre 2005 N.156 - REGOLE TECNICHE PER LA FORMAZIONE, LA TRASMISSIONE, LA CONSERVAZIONE, LA DUPLICAZIONE, LA RIPRODUZIONE E LA VALIDAZIONE, ANCHE TEMPORALE, DEI DOCUMENTI INFORMATICI.

TITOLO I
DISPOSIZIONI GENERALI

Art.1
(Definizioni)

1. Ai fini del presente regolamento si intende per:

a) CHIAVI, la coppia di chiavi asimmetriche crittografiche, una privata ed una pubblica correlate fra di loro, utilizzate nell'ambito dei sistemi di validazione di documenti informatici;
b) IMPRONTA di una sequenza di simboli binari (bit), la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash;
c) FUNZIONE DI HASH, una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) per le quali la funzione generi impronte uguali;
d) EVIDENZA INFORMATICA, una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica;
e) RIFERIMENTO TEMPORALE, informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici;
f) VALIDAZIONE TEMPORALE, il risultato della procedura informatica, con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi;
g) MARCA TEMPORALE, un'evidenza informatica che consente la validazione temporale;
h) PRESTATORE DI SERVIZI DI CERTIFICAZIONE o CERTIFICATORE, un organismo od una persona fisica o giuridica che rilascia certificati o fornisce altri servizi connessi alle firme elettroniche;
i) FIRMA DIGITALE, una particolare forma di firma elettronica qualificata basata su di un sistema di chiavi asimmetriche, una pubblica ed una privata;
l) CHIAVI ASIMMETRICHE, la coppia di chiavi crittografiche, una privata ed una pubblica, correlate fra di loro, utilizzate nell'ambito dei sistemi di validazione di documenti informatici;
m) CHIAVE PRIVATA, l'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto al soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;
n) CHIAVE PUBBLICA, l'elemento della coppia di chiavi asimmetriche destinate ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche.

Art.2
(Ambito di applicazione)

1. Il presente regolamento stabilisce, ai sensi dell'articolo 2, comma 4, della Legge 20 luglio 2005 n.115, le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.

2. Ai certificatori che rilasciano al pubblico certificati qualificati ai sensi della Legge 20 luglio 2005 n.115 si applicano le disposizioni del Titolo II.
3. I certificatori devono disporre di un sistema di validazione temporale conforme alle disposizioni di cui al Titolo III.
4. Al titolo IV vengono date disposizioni circa l'archiviazione elettronica dei documenti.
5. Al titolo V vengono indicati gli standard di riferimento della firma digitale.

Art.2 *bis*
(Firma elettronica remota)

1. Sino alla revisione della Legge 20 luglio 2005 n.115 e del presente decreto delegato, come già modificato con Decreto Delegato 30 gennaio 2020 n.9, gli effetti giuridici che le predette norme di rango primario attribuiscono alle firme elettroniche qualificate basate su un certificato qualificato e create mediante un dispositivo sicuro per la creazione di una firma, sono riconosciuti anche alla "firma remota", così come definita e disciplinata dal Decreto del Presidente del Consiglio dei Ministri (DPCM) 22 febbraio 2013 della Repubblica Italiana (in G.U.R.I. s.g. n.117 del 21/05/2013) e dai successivi futuri aggiornamenti e modifiche dello stesso.[4]

TITOLO II
REGOLE TECNICHE DI BASE

Art.3
(Norme tecniche di riferimento)

1. I prodotti di firma digitale, i dispositivi sicuri di firma elettronica, gli algoritmi di generazione e di verifica delle firme digitali e le funzioni di hash, devono essere conformi alle norme generalmente riconosciute a livello internazionale od individuate dalla Commissione Europea.
2. Il documento informatico sottoscritto con firma digitale od altro tipo di firma elettronica avanzata basata su un certificato qualificato e generata mediante un dispositivo sicuro per la creazione di una firma elettronica non produce gli effetti di cui all'articolo 3, comma 3, della Legge 20 luglio 2005 n.115, se contiene macroistruzioni o codici eseguibili, tali da attivare funzionalità che

[4] **Testo originario DECRETO DELEGATO 29 ottobre 2021 n.184, Art.15**
(Firma elettronica remota)
1. Dopo l'articolo 85 del Decreto 8 novembre 2005 n.156 e successive modifiche è aggiunto il seguente articolo:
"Art.85-*bis*
(Norme transitorie in materia di firma elettronica remota)
1. Sino alla revisione della Legge 20 luglio 2005 n.115 e del presente decreto delegato, come già modificato con Decreto Delegato 30 gennaio 2020 n.9, gli effetti giuridici che le predette norme di rango primario attribuiscono alle firme elettroniche qualificate basate su un certificato qualificato e create mediante un dispositivo sicuro per la creazione di una firma, sono riconosciuti anche alla "firma remota", così come definita e disciplinata dal Decreto del Presidente del Consiglio dei Ministri (DPCM) 22 febbraio 2013 della Repubblica Italiana (in G.U.R.I. s.g. n.117 del 21/05/2013) e dai successivi futuri aggiornamenti e modifiche dello stesso.".
Modifiche legislative:
DECRETO DELEGATO 21 marzo 2023 n.51, Art.26 comma 5
5. La numerazione e la rubrica dell'articolo 85bis del Decreto n.156/2005, come modificato dal CAPO IV FIRMA ELETTRONICA REMOTA e dall'articolo 15 Decreto Delegato n.184/2021, è così modificata: "Art.2bis (Firma elettronica remota)".

possano modificare gli atti, i fatti o i dati nello stesso rappresentati.

Art. 3-*bis*
(Formazione del documento elettronico)

1. Il documento elettronico è formato mediante una delle seguenti principali modalità:
a) redazione tramite l'utilizzo di appositi strumenti software;
b) acquisizione di un documento elettronico per via telematica o su supporto elettronico, acquisizione della copia per immagine su supporto elettronico di un documento analogico, acquisizione della copia informatica di un documento analogico;
c) registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
d) 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.
2. Le modalità di formazione di cui al comma 1 e le successive disposizioni di cui al presente articolo ed al Titolo IV-*bis* si applicano anche al documento amministrativo elettronico. Il diritto di accesso ai documenti amministrativi, così come regolato dalle norme in materia, si applica anche al documento amministrativo elettronico.
3. Il documento elettronico, identificato in modo univoco e persistente, è memorizzato in un sistema di gestione informatica dei documenti o di conservazione la cui tenuta può anche essere delegata a terzi.
4. Laddove non sia presente, al documento elettronico immodificabile è associato un riferimento temporale.
5. La data e l'ora di formazione del documento elettronico sono sempre opponibili ai terzi se, in via alternativa:
a) vi è apposta una validazione temporale attraverso una marca temporale di cui al Titolo III;
b) vi è associato il riferimento temporale contenuto nella segnatura di protocollo di cui al Regolamento 30 dicembre 2013 n. 9 attraverso il processo di archiviazione elettronica;
c) vi è associato il riferimento temporale attraverso i processi di conservazione sostitutiva e di riversamento sostitutivo di cui al Titolo IV;
d) vi è associato il riferimento temporale ottenuto attraverso l'utilizzo di un servizio elettronico di recapito certificato di cui all'articolo 8-*bis* del Decreto Delegato 11 aprile 2016 n. 46, così come introdotto dal Decreto Delegato 26 luglio 2018 n. 92, con attestazione di avvenuta accettazione;
e) vi è associato il riferimento temporale attraverso l'utilizzo di marcatura postale elettronica ai sensi dell'articolo 14, comma 1, punto 1.4 della Convenzione Postale Universale, come modificata dalle decisioni adottate dal XXIII Congresso dell'Unione Postale Universale.
6. L'utilizzo del dispositivo di firma elettronica qualificata si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria.
7. Il documento elettronico assume la caratteristica di immodificabilità se prodotto in modo che forma e contenuti non siano alterabili durante le fasi di tenuta ed accesso e ne sia garantita la staticità nella fase di conservazione.
8. Nel caso di documento elettronico formato ai sensi del comma 1, lettera a), le caratteristiche di immodificabilità e di integrità sono determinate da una o più delle seguenti operazioni:
a) la sottoscrizione con firma elettronica qualificata;
b) l'apposizione di una validazione temporale;
c) il trasferimento a soggetti terzi a mezzo di un servizio elettronico di recapito certificato di cui all'articolo 8-*bis* del Decreto Delegato n. 46/2016, così come introdotto dal Decreto Delegato n. 92/2018, con attestazione di avvenuta accettazione;
d) il trasferimento a soggetti terzi a mezzo di un servizio elettronico di recapito certificato qualificato avente i requisiti di cui all'articolo 44 del Regolamento eIDAS;

e) la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza e di protezione del dato;
f) il versamento ad un sistema di conservazione.

9. Nel caso di documento elettronico formato ai sensi del comma 1, lettera b), le caratteristiche di immodificabilità e di integrità sono determinate dall'operazione di memorizzazione in un sistema di gestione informatica dei documenti che garantisca l'inalterabilità del documento o in un sistema di conservazione.

10. Nel caso di documento elettronico formato ai sensi del comma 1, lettere c) e d), le caratteristiche di immodificabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di 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.

11. Nel caso di documento amministrativo elettronico le caratteristiche di immodificabilità e di integrità, oltre che con le modalità di cui ai commi 8, 9 e 10 sono determinate anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nei sistemi di gestione informatica dei documenti utilizzati dalla Pubblica Amministrazione e dagli Enti ed Aziende Autonome di Stato ed individuati dall'Unità Organizzativa (UO) Istituti Culturali e dalla Direzione Generale della Funzione Pubblica (DGFP).

12. L'evidenza informatica corrispondente al documento elettronico immodificabile è prodotta in uno dei formati contenuti nell'Allegato 1 in modo da assicurare l'indipendenza dalle piattaforme tecnologiche, l'interoperabilità tra sistemi informatici e la durata nel tempo dei dati in termini di accesso e di leggibilità. Formati diversi possono essere scelti nei casi in cui la natura del documento elettronico lo richieda per un utilizzo specifico nel suo contesto tipico.

13. Fermo restando quanto stabilito al comma 12, eventuali ulteriori formati possono essere utilizzati dalla Pubblica Amministrazione e dagli Enti ed Aziende Autonome di Stato in relazione a specifici contesti operativi individuati dall'UO Informatica, Tecnologia, Dati e Statistica (UITDS) e dalla DGFP su espressa e motivata richiesta degli uffici ed organi competenti.

14. Al documento elettronico sono associati i metadati che sono stati generati durante la sua formazione. L'insieme minimo dei metadati, come definiti nell'Allegato 2, è costituito da:
a) l'identificativo univoco e persistente;
b) il riferimento temporale di cui al comma 4;
c) l'oggetto;
d) il soggetto che ha formato il documento;
e) l'eventuale destinatario;
f) l'impronta del documento elettronico.

15. Eventuali ulteriori metadati rispetto a quelli indicati al comma 14 sono definiti in funzione del contesto e delle necessità gestionali e conservative. Con riferimento al documento amministrativo elettronico, possono essere associati eventuali ulteriori metadati rilevanti ai fini amministrativi ed individuati dall'UO UITDS e dalla DGFP su espressa e motivata richiesta degli uffici ed organi competenti, con riferimento ad ogni tipologia di documento e tenendo conto del contesto a cui esso si riferisce.

16. ABROGATO. [5]

[5] **Testo originario: Decreto Delegato 30 gennaio 2020 n.9, Art.3**
(Norme sulla formazione del documento elettronico)
1. Dopo l'articolo 3 del Decreto n. 156/2005 è aggiunto il seguente articolo:
"Art. 3-bis
(Formazione del documento elettronico)
1. Il documento elettronico è formato mediante una delle seguenti principali modalità:
a) redazione tramite l'utilizzo di appositi strumenti software;

b) acquisizione di un documento elettronico per via telematica o su supporto elettronico, acquisizione della copia per immagine su supporto elettronico di un documento analogico, acquisizione della copia informatica di un documento analogico;
c) registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
d) 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.
2. Le modalità di formazione di cui al comma 1 e le successive disposizioni di cui al presente articolo ed al Titolo IV-bis si applicano anche al documento amministrativo elettronico. Il diritto di accesso ai documenti amministrativi, così come regolato dalle norme in materia, si applica anche al documento amministrativo elettronico.
3. Il documento elettronico, identificato in modo univoco e persistente, è memorizzato in un sistema di gestione informatica dei documenti o di conservazione la cui tenuta può anche essere delegata a terzi.
4. Laddove non sia presente, al documento elettronico immodificabile è associato un riferimento temporale.
5. La data e l'ora di formazione del documento elettronico sono sempre opponibili ai terzi se, in via alternativa:
a) vi è apposta una validazione temporale attraverso una marca temporale di cui al Titolo III;
b) vi è associato il riferimento temporale contenuto nella segnatura di protocollo di cui al
Regolamento 30 dicembre 2013 n. 9 attraverso il processo di archiviazione elettronica;
c) vi è associato il riferimento temporale attraverso i processi di conservazione sostitutiva e di riversamento sostitutivo di cui al Titolo IV;
d) vi è associato il riferimento temporale ottenuto attraverso l'utilizzo di un servizio elettronico di recapito certificato di cui all'articolo 8-bis del Decreto Delegato 11 aprile 2016 n. 46, così come introdotto dal Decreto Delegato 26 luglio 2018 n. 92, con attestazione di avvenuta accettazione;
e) vi è associato il riferimento temporale attraverso l'utilizzo di marcatura postale elettronica ai sensi dell'articolo 14, comma 1, punto 1.4 della Convenzione Postale Universale, come modificata dalle decisioni adottate dal XXIII Congresso dell'Unione Postale Universale.
6. L'utilizzo del dispositivo di firma elettronica qualificata si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria.
7. Il documento elettronico assume la caratteristica di immodificabilità se prodotto in modo che forma e contenuti non siano alterabili durante le fasi di tenuta ed accesso e ne sia garantita la staticità nella fase di conservazione.
8. Nel caso di documento elettronico formato ai sensi del comma 1, lettera a), le caratteristiche di immodificabilità e di integrità sono determinate da una o più delle seguenti operazioni:
a) la sottoscrizione con firma elettronica qualificata;
b) l'apposizione di una validazione temporale;
c) il trasferimento a soggetti terzi a mezzo di un servizio elettronico di recapito certificato di cui all'articolo 8-bis del Decreto Delegato n. 46/2016, così come introdotto dal Decreto Delegato n. 92/2018, con attestazione di avvenuta accettazione;
d) il trasferimento a soggetti terzi a mezzo di un servizio elettronico di recapito certificato qualificato avente i requisiti di cui all'articolo 44 del Regolamento eIDAS;
e) la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza e di protezione del dato;
f) il versamento ad un sistema di conservazione.
9. Nel caso di documento elettronico formato ai sensi del comma 1, lettera b), le caratteristiche di immodificabilità e di integrità sono determinate dall'operazione di memorizzazione in un sistema di gestione informatica dei documenti che garantisca l'inalterabilità del documento o in un sistema di conservazione.
10. Nel caso di documento elettronico formato ai sensi del comma 1, lettere c) e d), le caratteristiche di immodificabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di 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.
11. Nel caso di documento amministrativo elettronico le caratteristiche di immodificabilità e di integrità, oltre che con le modalità di cui ai commi 8, 9 e 10 sono determinate anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nei sistemi di gestione informatica dei documenti utilizzati dalla Pubblica Amministrazione e dagli Enti ed Aziende Autonome di Stato ed individuati dall'Unità Organizzativa (UO) Istituti Culturali e dalla Direzione Generale della Funzione Pubblica (DGFP).
12. L'evidenza informatica corrispondente al documento elettronico immodificabile è prodotta in uno dei formati contenuti nell'Allegato 1 in modo da assicurare l'indipendenza dalle piattaforme tecnologiche, l'interoperabilità tra

Art.4

(Caratteristiche generali delle chiavi per la creazione e la verifica della firma elettronica)

1. Una coppia di chiavi per la creazione e la verifica della firma elettronica deve essere attribuita ad un solo titolare.
2. Se il titolare appone la sua firma elettronica per mezzo di una procedura automatica, deve utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso.
3. Se la procedura automatica fa uso di più dispositivi per apporre la firma elettronica del medesimo titolare, deve essere utilizzata una coppia di chiavi diversa per ciascun dispositivo.
4. Ai fini del presente regolamento, le chiavi di creazione e verifica della firma elettronica, ed i correlati servizi, si distinguono secondo le tipologie:

a) chiavi di sottoscrizione, destinate alla generazione e verifica delle firme elettroniche apposte od associate ai documenti;

b) chiavi di certificazione, destinate alla generazione e verifica delle firme elettroniche apposte od associate ai certificati qualificati, alle liste di revoca (CRL) e sospensione (CSL), ovvero alla sottoscrizione dei certificati relativi a chiavi di marcatura temporale;

c) chiavi di marcatura temporale, destinate alla generazione e verifica delle marche temporali.

5. Non è consentito l'uso di una coppia di chiavi per funzioni diverse da quelle previste, per ciascuna tipologia, dal precedente comma 4.
6. La robustezza delle chiavi deve essere tale da garantire un adeguato livello di sicurezza in rapporto allo stato delle conoscenze scientifiche e tecnologiche in tale materia.

Art.5

(Generazione delle chiavi)

---

sistemi informatici e la durata nel tempo dei dati in termini di accesso e di leggibilità. Formati diversi possono essere scelti nei casi in cui la natura del documento elettronico lo richieda per un utilizzo specifico nel suo contesto tipico.

13. Fermo restando quanto stabilito al comma 12, eventuali ulteriori formati possono essere utilizzati dalla Pubblica Amministrazione e dagli Enti ed Aziende Autonome di Stato in relazione a specifici contesti operativi individuati dall'UO Informatica, Tecnologia, Dati e Statistica (UITDS) e dalla DGFP su espressa e motivata richiesta degli uffici ed organi competenti.

14. Al documento elettronico sono associati i metadati che sono stati generati durante la sua formazione. L'insieme minimo dei metadati, come definiti nell'Allegato 2, è costituito da:

a) l'identificativo univoco e persistente;
b) il riferimento temporale di cui al comma 4;
c) l'oggetto;
d) il soggetto che ha formato il documento;
e) l'eventuale destinatario;
f) l'impronta del documento elettronico.

15. Eventuali ulteriori metadati rispetto a quelli indicati al comma 14 sono definiti in funzione del contesto e delle necessità gestionali e conservative. Con riferimento al documento amministrativo elettronico, possono essere associati eventuali ulteriori metadati rilevanti ai fini amministrativi ed individuati dall'UO UITDS e dalla DGFP su espressa e motivata richiesta degli uffici ed organi competenti, con riferimento ad ogni tipologia di documento e tenendo conto del contesto a cui esso si riferisce.

16. Le imposte di bollo relative ai documenti amministrativi elettronici e alla loro riproduzione su diversi tipi di supporto sono assolte con le modalità definite dalla DGFP, sentita l'UO Ufficio del Registro e Conservatoria.".

MODIFICHE LEGISLATIVE: DECRETO DELEGATO 29 marzo 2021 n.61, Art. 10

-omissis-

4. Sono abrogati:

-omissis-

i) l'articolo 3bis, comma 16 del Decreto 8 novembre 2005 n.156 come modificato dall'articolo 3 del Decreto Delegato 2 luglio 2019 n.113 [RATIF. con Decreto Delegato 30 gennaio 2020 n.9]

1. La generazione della coppia di chiavi deve essere effettuata mediante dispositivi e procedure che assicurino, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata.
2. Il sistema di generazione della coppia di chiavi deve comunque assicurare:
a) la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;
b) l'equiprobabilità di generazione di tutte le coppie possibili;
c) l'identificazione del soggetto che attiva la procedura di generazione.

Art.6
(Modalità di generazione delle chiavi)

1. Le chiavi di certificazione debbono essere generate esclusivamente dal responsabile del servizio.
2. Le chiavi di sottoscrizione possono essere generate dal titolare o dal certificatore.
3. La generazione delle chiavi di sottoscrizione effettuata autonomamente dal titolare deve avvenire all'interno del dispositivo sicuro per la generazione delle firme, che deve essere rilasciato od indicato dal certificatore.
4. Il certificatore deve assicurarsi che il dispositivo sicuro per la generazione delle firme, da lui fornito od indicato, presenti le caratteristiche ed i requisiti di cui all'articolo 5 della Legge 20 luglio 2005 n.115 ed all'articolo 9 del presente decreto.
5. Il titolare è tenuto ad utilizzare esclusivamente il dispositivo fornito dal certificatore ovvero un dispositivo scelto tra quelli indicati dal certificatore stesso.

Art.7
(Conservazione delle chiavi)

1. È vietata la duplicazione della chiave privata e dei dispositivi che la contengono.
2. Per fini particolari di sicurezza, è consentito che le chiavi di certificazione vengano esportate purché ciò avvenga con modalità tali da non ridurre il livello di sicurezza.
3. Il titolare della coppia di chiavi deve:
a) conservare con la massima diligenza la chiave privata od il dispositivo che la contiene al fine di garantirne l'integrità e la massima riservatezza;
b) conservare le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo contenente la chiave;
c) richiedere immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma elettronica difettosi o di cui abbia perduto il possesso.

Art.8
(Generazione delle chiavi al di fuori del dispositivo di firma elettronica)

1. Se la generazione delle chiavi avviene su un sistema diverso da quello destinato all'uso della chiave privata, il sistema di generazione deve assicurare:
a) l'impossibilità di intercettazione o recupero di qualsiasi informazione, anche temporanea, prodotta durante l'esecuzione della procedura;
b) il trasferimento della chiave privata, in condizioni di massima sicurezza, nel dispositivo di firma elettronica in cui verrà utilizzata.
2. Il sistema di generazione deve essere isolato, dedicato esclusivamente a questa attività ed adeguatamente protetto contro i rischi di interferenze ed intercettazioni.
3. L'accesso al sistema deve essere controllato e ciascun utente preventivamente identificato.

Ogni sessione di lavoro deve essere registrata nel giornale di controllo.
4. Prima della generazione di una nuova coppia di chiavi, l'intero sistema deve procedere alla verifica della propria configurazione, dell'autenticità ed integrità del software installato e dell'assenza di programmi non previsti dalla procedura.

Art.9

(Dispositivi sicuri e procedure per la generazione della firma elettronica)

1. In aggiunta a quanto previsto all'articolo 5 della Legge 20 Luglio 2005 n.115, la generazione della firma elettronica deve avvenire all'interno di un dispositivo sicuro di firma elettronica, così che non sia possibile l'intercettazione della chiave privata utilizzata.
2. Il dispositivo sicuro di firma elettronica deve poter essere attivato esclusivamente dal titolare prima di procedere alla generazione della firma elettronica.
3. I dispositivi sicuri di firma elettronica sono sottoposti alla valutazione e certificazione di sicurezza secondo i criteri indicati all'articolo 45.
4. La personalizzazione del dispositivo sicuro di firma elettronica deve almeno garantire:
a) l'acquisizione da parte del certificatore dei dati identificativi del dispositivo di firma elettronica utilizzato e la loro associazione al titolare;
b) la registrazione nel dispositivo di firma elettronica del certificato qualificato relativo alle chiavi di sottoscrizione del titolare.
5. La personalizzazione del dispositivo sicuro di firma elettronica può prevedere, per l'utilizzo nelle procedure di verifica della firma elettronica, la registrazione, nel dispositivo di firma elettronica, del certificato elettronico relativo alla chiave pubblica del certificatore la cui corrispondente privata è stata utilizzata per sottoscrivere il certificato qualificato relativo alle chiavi di sottoscrizione del titolare.
6. La personalizzazione del dispositivo di firma elettronica è registrata nel giornale di controllo.
7. Il certificatore deve adottare, nel processo di personalizzazione del dispositivo sicuro per la generazione delle firme elettroniche, procedure atte ad identificare il titolare di un dispositivo sicuro di firma elettronica e dei certificati in esso contenuti.

Art.10

(Verifica delle firme digitali)

1. I certificatori che rilasciano certificati qualificati devono fornire ovvero indicare almeno un sistema che consenta di effettuare la verifica delle firme digitali.

Art.11

(Informazioni riguardanti i certificatori)

1. I certificatori che rilasciano al pubblico certificati qualificati ai sensi della Legge 20 luglio 2005 n.115 devono fornire le seguenti informazioni e documenti:
a) dati anagrafici ovvero denominazione o ragione sociale;
b) residenza ovvero sede legale;
c) sedi operative;
d) rappresentante legale;
e) certificati delle chiavi di certificazione;
f) piano per la sicurezza contenuto in busta sigillata;
g) manuale operativo di cui al successivo articolo 51;
i) dichiarazione di conformità ai requisiti previsti nel presente decreto;
l) relazione sulla struttura organizzativa;
m) copia di una polizza assicurativa di copertura dei rischi dell'attività e dei danni causati a terzi.

Art.12

(Modalità di segnalazione di inizio attività da parte dei certificatori nazionali)

1. I certificatori stabiliti nella Repubblica di San Marino che intendono rilasciare al pubblico certificati qualificati devono darne avviso all'Autorità per l'Informatica, almeno sessanta giorni prima dell'inizio dell'attività.
2. L'avviso di inizio attività, firmato dal rappresentante legale, trasmesso all'Autorità per l'Informatica mediante un sistema che ne attesti l'avvenuta ricezione, deve contenere le informazioni di cui all'articolo 11.

All'avviso deve essere inoltre allegata la seguente documentazione:

a) autorizzazione preventiva all'accesso alle strutture dedicate alle operazioni di certificazione, da parte dell'Autorità per l'Informatica o di persone da questa incaricate, per la verifica del mantenimento della rispondenza ai requisiti tecnico-organizzativi di cui alla documentazione allegata alla domanda;
b) copia del manuale operativo, di cui al successivo articolo 51;
c) copia del piano per la sicurezza, di cui al successivo articolo 40;
d) una relazione dettagliata sulla struttura organizzativa;
e) dichiarazione di impegno a comunicare tempestivamente all'Autorità per l'Informatica ogni variazione significativa delle soluzioni tecnico-organizzative adottate.

3. L'Autorità per l'Informatica ha facoltà di richiedere ulteriore documentazione utile a valutare le modalità con cui il certificatore intende operare. La richiesta di ulteriore documentazione sospende il termine di sessanta giorni di cui al punto 1.
4. Entro il suddetto termine di sessanta giorni l'Autorità per l'Informatica ha facoltà di negare al certificatore l'autorizzazione ad operare, qualora la documentazione fornita non risulti rispondente ai requisiti previsti dal presente regolamento tecnico.
5. Trascorsi sessanta giorni dal ricevimento della segnalazione di inizio attività, nel silenzio dell'Autorità per l'Informatica, il certificatore è autorizzato ad operare.

Art.13

(Riconoscimento dei certificatori esteri)

1. Sono equiparati ai certificati nazionali i certificati emessi da un certificatore avente sede in uno dei Paesi della Comunità Europea, che soddisfi i requisiti applicabili al rilascio di certificati nel paese nel quale il certificatore ha sede, e la cui validità può essere verificata nel territorio nazionale.
2. I certificati qualificati di tali certificatori producono i medesimi effetti giuridici dei certificati qualificati nazionali.
3. I certificati emessi da certificatori di paesi terzi vengono equiparati a quelli nazionali se:

a) rispondono a tutte le norme previste dalla Legge 20 luglio 2005 n.115 ed al presente decreto;
b) che si sia verificato quanto previsto dall'articolo 12 della Legge 20 luglio 2005 n.115.

Art.14

(Equivalenza internazionale dei certificati)

1. I certificati rilasciati dai prestatori di servizi di certificazione costituiti in uno Stato non membro dello Comunità Europea in conformità con la legislazione di quello Stato, sono equiparati a quelli nazionali, se adempiono ad almeno una delle seguenti condizioni:

a) che il prestatore di servizi di certificazione abbia i requisiti stabiliti dalla normativa della Comunità Europea in materia di firma elettronica per il rilascio di certificati riconosciuti, e sia stato accreditato in conformità al sistema volontario di accreditamento stabilito in uno Stato membro della Comunità Europea;

b) che il certificato sia garantito da un prestatore di servizi di certificazione costituito nello Spazio economico europeo che adempia i requisiti definiti dalla normativa della Comunità Europea in materia di firma elettronica per il rilascio di certificati riconosciuti;
c) che il certificato o il prestatore di servizi di certificazione siano riconosciuti in virtù di un accordo bilaterale o multilaterale fra la Comunità Europea e paesi terzi o organizzazioni internazionali;
d) che il certificato o il prestatore di servizi di certificazione siano riconosciuti nel proprio paese pubblicato nella lista prevista dal paragrafo 11, comma 3, della Legge 20 luglio 2005 n.115.

Art.15
(Modalità di richiesta di certificati qualificati)

1. Il prestatore di servizi di certificazione verifica che la richiesta di rilascio del certificato qualificato sia effettuata tramite documento elettronico sul quale deve essere apposta la firma digitale, o tramite documento scritto su supporto cartaceo, con firma autografa, secondo quanto disposto dagli articoli 16 e 17 del presente decreto.
2. Il prestatore di servizi di certificazione verifica l'identità del richiedente, tramite mezzo legalmente riconosciuto, verificando, nel caso i cui la richiesta sia sottoscritta da terzi, i poteri sufficienti del richiedente per la riferita sottoscrizione.

Art.16
(Richiesta di emissione del certificato qualificato da persona singola)

1. La richiesta di emissione, quando effettuata da persona singola in qualità di titolare del certificato qualificato, deve contenere, fra gli altri, i seguenti elementi:
a) nome completo;
b) indicazione di eventuale pseudonimo come titolare;
c) numero ISS, data e ente di emissione o qualsiasi altro elemento che permette l'identificazione univoca;
d) indirizzo e altre forme di contatto;
e) eventuale indicazione di una qualità specifica in funzione all'utilizzo della richiesta;
f) indicazione riguardo alle eventuali restrizioni di uso del certificato;
g) altre informazioni relative ai poteri di rappresentazione, alla qualifica professionale od altri attributi.
2. Se la richiesta di emissione è effettuata da terzi, e non dalla persona singola in qualità di titolare del certificato qualificato, la stessa, oltre agli elementi riferiti nel numero anteriore, e a seconda che sia presentata da persona singola o collettiva, deve contenere i seguenti elementi relativi al richiedente:
a) nome o denominazione legale;
b) numero ISS, data e ente di emissione, o qualsiasi altro elemento che permetta l'identificazione univoca, o numero di operatore economico;
c) residenza o sede;
d) scopo sociale, nome dei titolari degli organismi sociali e di altre persone che vi esercitano potere;
e) indirizzo e altra forma di contatto.
3. La richiesta di inclusione nel certificato qualificato dei dati personali della persona singola in qualità di titolare dovrà essere espressamente autorizzata dalla stessa.
4. Nella situazione prevista al comma 2 del presente articolo, la richiesta è anche accompagnata dalla dichiarazione della persona singola come titolare del certificato in cui si vincola agli obblighi in quanto titolare.

Art.17

(Richiesta di emissione del certificato qualificato da persona giuridica)

1. La richiesta di emissione, qualora effettuata da persona giuridica in qualità di titolare del certificato qualificato, deve essere sottoscritta dai suoi rappresentanti legali e deve contenere, fra gli altri, i seguenti elementi:
a) denominazione legale;
b) numero di operatore economico, sede, scopo sociale, nome dei titolari degli organismi sociali e di altre persone che vi esercitano potere e numero di immatricolazione nei registri pubblici;
c) nome completo, numero ISS o di qualsiasi altro elemento che permetta l'identificazione univoca delle persone singole che la rappresentano legalmente o statutariamente;
d) indirizzo e altre forme di contatto;
e) indicazione delle eventuali restrizioni di uso del certificato e di eventuali limiti del valore delle transazioni per le quali il certificato è valido;
f) eventuale riferimento a una qualità specifica, in funzione dell'utilizzo del certificato;
g) altre informazioni relative ai poteri di rappresentazione, alla qualifica professionale o altri attributi.
2. Nel caso in cui la richiesta di emissione sia presentata da terzi, e non dalla persona collettiva in qualità di titolare del certificato, alla stessa, oltre a quanto disposto nel numero precedente, si applica con gli adattamenti del caso, quanto previsto nei commi 2, punti a), b), c), d) ed e), e 4 dell'articolo 16.

Art.18
(Registro delle richieste di certificati qualificati)

1. Il prestatore di servizi di certificazione riceve la richiesta, ne convalida i dati e procede al registro.
2. Il registro comprende:
a) l'identificazione del certificatore che ha ricevuto la richiesta;
b) i dati di cui consta la richiesta;
c) i documenti di prova che accompagnano la richiesta;
d) la descrizione dei metodi utilizzati nella verifica della richiesta;
e) l'identificazione del contratto riferito nell'articolo 62;
f) altre informazioni utili relativi all'utilizzo del certificato.
3. I dati del registro non possono essere utilizzati per fini diversi da quelli necessari all'utilizzo del certificato.
4. L'ente di certificazione mantiene in archivio, per almeno venti anni, i dati del registro, i documenti che li comprovano e una copia del contratto.

Art.19
(Generazione delle chiavi di certificazione)

1. La generazione delle chiavi di certificazione deve avvenire in modo conforme a quanto previsto dal presente Titolo.
2. Per ciascuna chiave di certificazione il certificatore deve generare un certificato sottoscritto con la chiave privata della coppia cui il certificato si riferisce.
3. I valori contenuti nei singoli campi del certificato delle chiavi di certificazione devono essere codificati in modo da non generare equivoci relativi al nome, ragione o denominazione sociale del certificatore.

Art.20
(Generazione dei certificati qualificati)

1. In aggiunta agli obblighi previsti per il certificatore dall'articolo 6 della Legge 20 luglio 2005 n.115, prima di emettere il certificato qualificato il certificatore deve:
a) accertarsi dell'autenticità della richiesta;
b) verificare il possesso della chiave privata e il corretto funzionamento della coppia di chiavi.
2. Il certificato qualificato deve essere generato con un sistema conforme a quanto previsto dall'articolo 37.
3. L'emissione dei certificati qualificati deve essere registrata nel giornale di controllo con la specificazione della data e dell'ora della generazione.
4. Il momento della generazione dei certificati deve essere attestato tramite un riferimento temporale.

Art.21
(Informazioni contenute nei certificati qualificati)

1. Fatto salvo quanto previsto dall'articolo 4 della Legge 20 luglio 2005 n.115, i certificati qualificati devono contenere almeno le seguenti informazioni:
a) codice identificativo del titolare presso il certificatore;
b) tipologia della coppia di chiavi in base all'uso cui sono destinate.
2. I valori contenuti nei singoli campi del certificato qualificato devono essere codificati in modo da non generare equivoci relativi al nome, ragione o denominazione sociale del certificatore.
3. Il certificatore determina il periodo di validità dei certificati qualificati in funzione della robustezza delle chiavi di creazione e verifica impiegate e dei servizi cui essi sono destinati.
4. Il certificatore custodisce le informazioni di cui all'articolo 5, punto i), della Legge 20 luglio 2005 n.115, per un periodo non inferiore a dieci anni dalla data di scadenza o revoca del certificato qualificato.

Art.22
(Rilascio dei certificati qualificati)

1. L'ente di certificazione garantisce che, durante la procedura di rilascio, i dati di registro del titolare siano trattati in forma sicura e che la chiave pubblica relativa al certificato sia connessa alla corrispondente chiave privata del titolare.
2. L'ente di certificazione attribuisce un identificatore unico per ciascun titolare, per l'uso nel certificato.
3. L'ente di certificazione assicura la protezione della riservatezza e l'integrità dei dati del registro in tutte le procedure di rilascio.
4. Il termine di validità del certificato non può oltrepassare il termine di validità degli algoritmi utilizzati e dei parametri corrispondenti.
5. Il termine di validità del certificato accompagnante non può superare il termine di validità del certificato cui si riferisce.
6. L'ente di certificazione mantiene il registro dei certificati rilasciati, dalla data del rispettivo rilascio durante tutto il periodo di validità, e li conserva per un periodo non inferiore a venti anni, a partire dal termine del periodo di validità.
7. L'ente di certificazione emette un certificato per la persona giuridica solo quando può garantire che la creazione della firma digitale, mediante dispositivo di creazione della firma digitale, esige l'intervento di persone singole, statutariamente o legalmente, che rappresentano la persona giuridica titolare di questo certificato.

Art.23
(Distribuzione dei certificati qualificati)

1. L’ente di certificazione, nella distribuzione dei certificati, deve utilizzare sistemi sicuri che ne permettano la conservazione e disponibilità ai fini di verifica, e assicurare che:
a) il certificato sia messo a disposizione del titolare, in forma integrale, da parte di chi lo ha rilasciato;
b) il certificato sia accessibile alla consultazione pubblica solo previo consenso del titolare;
c) al destinatario vengano trasmesse le condizioni cui si vincola, e in particolare:
   i. verificare la validità, sospensione o revoca del certificato a ogni comunicazione o transizione;
   ii. verificare che il certificato sia utilizzato conformemente alle condizioni emesse dall’ente di certificazione.

Art.24

(Rinnovo e aggiornamento dei certificati qualificati)

1. Nel caso di rinnovo o aggiornamento dei certificati in seguito a una modifica degli attributi del titolare, l’ente di certificazione deve:
a) controllare che tutte le informazioni utilizzate per verificare l’identità e gli attributi del titolare siano ancora valide;
b) comunicare anticipatamente al titolare tutte le alterazioni dei termini e delle condizioni di rilascio del certificato;
c) assicurare che le chiavi della firma digitale siano aggiornate prima del termine del loro periodo di validità e che le chiavi pubbliche a esse connesse garantiscano, come minimo, lo stesso livello di sicurezza che offrivano nel certificato iniziale.
d) assicurare che il rilascio di un nuovo certificato, che utilizzi la chiave pubblica certificata precedentemente, sia effettuato solo se è garantita la sicurezza crittografica di questa chiave durante il termine di validità del nuovo certificato.

Art.25

(Revoca e sospensione del certificato qualificato)

1. Fatto salvo quanto previsto dall’articolo 7 della Legge 20 luglio 2005 n.115, il certificato qualificato deve essere revocato o sospeso dal certificatore, ove quest’ultimo abbia notizia della compromissione della chiave privata o del dispositivo per la creazione della firma elettronica.

Art.26

(Revoca dei certificati qualificati relativi a chiavi di sottoscrizione)

1. La revoca del certificato qualificato relativo a chiavi di sottoscrizione viene effettuata dal certificatore mediante l’inserimento del suo codice identificativo in una delle liste di certificati revocati e sospesi (CRL/CSL).
2. Se la revoca avviene a causa della possibile compromissione della segretezza della chiave privata, il certificatore deve procedere tempestivamente alla pubblicazione dell'aggiornamento della lista di revoca.
3. La revoca dei certificati è annotata nel giornale di controllo con la specificazione della data e dell’ora della pubblicazione della nuova lista.

Art.27

(Revoca su iniziativa del certificatore)

1. Salvo i casi di motivata urgenza, il certificatore che intende revocare un certificato

qualificato deve darne preventiva comunicazione al titolare, specificando i motivi della revoca nonché la data e l'ora a partire dalla quale la revoca è efficace.

Art.28
(Revoca su richiesta del titolare)

1. La richiesta di revoca deve essere inoltrata al certificatore munita della sottoscrizione del titolare e con la specificazione della sua decorrenza.
2. Le modalità di inoltro della richiesta devono essere indicate dal certificatore nel manuale operativo di cui al successivo articolo 51.
3. Il certificatore deve verificare l'autenticità della richiesta e procedere alla revoca entro il termine richiesto. Sono considerate autentiche le richieste inoltrate con le modalità previste dal comma 2.
4. Se il certificatore non ha la possibilità di accertare in tempo utile l'autenticità della richiesta, procede alla sospensione del certificato.

Art.29
(Revoca su richiesta del terzo interessato)

1. La richiesta di revoca da parte del terzo interessato da cui derivano i poteri di rappresentanza del titolare deve essere inoltrata al certificatore munita di sottoscrizione e con la specificazione della sua decorrenza.
2. Il certificatore deve notificare la revoca al titolare.
3. Se il certificatore non ha la possibilità di accertare in tempo utile l'autenticità della richiesta, procede alla sospensione del certificato.

Art.30
(Sospensione dei certificati qualificati)

1. La sospensione del certificato qualificato è effettuata dal certificatore attraverso l’inserimento di tale certificato in una delle liste dei certificati revocati e sospesi (CRL/CSL).
2. La sospensione dei certificati è annotata nel giornale di controllo con l’indicazione della data e dell’ora di esecuzione dell’operazione.

Art.31
(Sospensione su iniziativa del certificatore)

1. Salvo casi d’urgenza, che il certificatore è tenuto a motivare contestualmente alla notifica di cui al comma 2, il certificatore che intende sospendere un certificato qualificato deve darne preventiva comunicazione al titolare specificando i motivi della sospensione e la sua durata.
2. L'avvenuta sospensione del certificato qualificato deve essere tempestivamente notificata al titolare specificando la data e l'ora a partire dalla quale il certificato qualificato risulta sospeso.
3. Se la sospensione è causata da una richiesta di revoca motivata dalla possibile compromissione della chiave privata, il certificatore deve procedere tempestivamente alla pubblicazione della sospensione.

Art.32
(Sospensione su richiesta del titolare)

1. La richiesta di sospensione deve essere inoltrata al certificatore munita della sottoscrizione del titolare e con la specificazione della sua durata.

2. Le modalità di inoltro della richiesta devono essere indicate dal certificatore nel manuale operativo.
3. Il certificatore deve verificare l'autenticità della richiesta e procedere alla sospensione entro il termine richiesto.

Art.33
(Sospensione su richiesta del terzo interessato)

1. La richiesta di sospensione da parte del terzo interessato da cui derivano i poteri di rappresentanza del titolare deve essere inoltrata al certificatore munita di sottoscrizione del titolare e con la specificazione della sua durata.
2. Il certificatore deve notificare la sospensione al titolare.

Art.34
(Sostituzione delle chiavi di certificazione)

1. Almeno novanta giorni prima della scadenza del certificato relativo a chiavi di certificazione, il certificatore deve avviare la procedura di sostituzione, generando, con le modalità previste dall'articolo 19, una nuova coppia di chiavi.
2. Il certificatore deve generare un certificato relativo alla nuova chiave pubblica sottoscritto con la chiave privata della vecchia coppia ed uno relativo alla vecchia chiave pubblica sottoscritto con la chiave privata della nuova coppia.

Art.35
(Revoca dei certificati relativi a chiavi di certificazione)

1. La revoca del certificato relativo ad una coppia di chiavi di certificazione è consentita solo nei seguenti casi:
a) compromissione della chiave privata, intesa come diminuita affidabilità nelle caratteristiche di sicurezza della chiave privata.
b) guasto del dispositivo di firma elettronica;
c) cessazione dell'attività.
2. La revoca deve essere notificata entro ventiquattro ore a tutti i titolari di certificati qualificati firmati con la chiave privata appartenente alla coppia revocata.
3. I certificati qualificati per i quali risulti compromessa la chiave privata con cui sono stati sottoscritti devono essere revocati.

Art.36
(Requisiti di sicurezza dei sistemi operativi)

1. Il sistema operativo dei sistemi di elaborazione utilizzati nelle attività di certificazione per la generazione delle chiavi, la generazione dei certificati qualificati e la gestione del registro dei certificati qualificati devono essere conformi quanto meno alle specifiche previste dalla classe ITSEC F-C2/E2 o equivalenti.
2. Il requisito di cui al comma 1 non si applica al sistema operativo dei dispositivi di firma digitale.

Art.37
(Sistema di generazione dei certificati qualificati)

1. La generazione dei certificati qualificati deve avvenire su un sistema utilizzato

esclusivamente per la generazione di certificati, situato in locali adeguatamente protetti.
2. L'entrata e l'uscita dai locali protetti deve essere registrata sul giornale di controllo.
3. L'accesso ai sistemi di elaborazione deve essere consentito, limitatamente alle funzioni assegnate, esclusivamente al personale autorizzato, identificato attraverso un'opportuna procedura di riconoscimento da parte del sistema al momento di apertura di ciascuna sessione.
4. L'inizio e la fine di ciascuna sessione devono essere registrate sul giornale di controllo.

Art.38
(Accesso del pubblico ai certificati)

1. Le liste dei certificati revocati e sospesi devono essere rese pubbliche.
2. I certificati qualificati, su richiesta del titolare, possono essere accessibili alla consultazione del pubblico, ovvero comunicati a terzi, esclusivamente nei casi consentiti dal titolare del certificato.

Art.39
(Implementazione di sicurezza)

1. L'ente di certificazione assicura che le installazioni, i procedimenti, il personale, le attrezzature ed i prodotti siano conformi alle norme di sicurezza applicabili nell'esercizio della sua attività, dovendo in particolare:
a) disporre di un piano di sicurezza implementato secondo quanto disposto dalla norma internazionale ISO/IEC 17799;
b) utilizzare sistemi e prodotti affidabili, protetti da alterazioni;
c) disporre di un revisore di sicurezza;
d) elaborare rapporti sugli incidenti dovuti a errori operativi o di sicurezza, e adottare rapidamente le adeguate misure correttive.
2. L'ente di certificazione assicura che i procedimenti utilizzati per garantire i livelli di sicurezza operativi, fisici e dei sistemi, nei termini delle norme adottate, siano documentati, implementati e aggiornati e mantiene un inventario dei beni con la rispettiva classificazione, in modo da caratterizzare le sue esigenze di protezione.

Art.40
(Piano per la sicurezza)

1. Il certificatore deve definire un piano per la sicurezza nel quale devono essere contenuti almeno i seguenti elementi:
a) struttura generale, modalità operativa e struttura logistica;
b) descrizione dell'infrastruttura di sicurezza per ciascun immobile rilevante ai fini della sicurezza;
c) allocazione dei servizi e degli uffici negli immobili;
d) elenco del personale e sua allocazione negli uffici;
e) attribuzione delle responsabilità;
f) algoritmi crittografici o altri sistemi utilizzati;
g) descrizione delle procedure utilizzate nell'attività di certificazione;
h) descrizione dei dispositivi installati;
i) descrizione dei flussi di dati;
l) procedura di gestione delle copie di sicurezza dei dati;
m) procedura di gestione dei disastri;
n) analisi dei rischi;
o) descrizione delle contromisure;
p) specificazione dei controlli.

Art.41
(Piano contingente)

1. L’ente di certificazione, per far fronte all’insorgere di eventuali disastri o incidenti che potrebbero mettere in causa il normale funzionamento di prestazione dei servizi di certificazione, elabora un piano contingente che contempla:
a) la possibilità di modifica o di accesso non autorizzato alle chiavi private dell’ente di certificazione;
b) una pianificazione della ripresa delle operazioni in un intervallo di tempo precedentemente definito;
c) la forma in cui richiedenti, titolari, destinatari e altri enti di certificazione con i quali esiste un accordo, saranno informati dell’insorgere di qualsiasi evento che mette in causa l’utilizzo sicuro dei certificati e lo stato di revoca;
d) la manutenzione dell’integrità e autenticità dell’informazione relativa allo stato di revoca.
2. L’ente di certificazione assicura che i servizi di distribuzione, revoca e stato di revoca dei certificati siano permanentemente disponibili, in caso di incidente, garantisce i procedimenti che permettono la continuazione dei servizi grazie a sistemi di recupero alternativi, facendo in modo che la migrazione dai sistemi primari ai sistemi di recupero non metta a rischio la sicurezza dei sistemi.

Art.42
(Giornale di controllo)

1. Il giornale di controllo è costituito dall'insieme delle registrazioni effettuate automaticamente dai dispositivi installati presso il certificatore, allorché si verificano le condizioni previste dal presente regolamento.
2. Le registrazioni possono essere effettuate indipendentemente anche su supporti distinti e di tipo diverso.
3. A ciascuna registrazione deve essere associato un riferimento temporale.
4. Il giornale di controllo deve essere tenuto in modo da garantire l'autenticità delle annotazioni e consentire la ricostruzione con la necessaria accuratezza di tutti gli eventi rilevanti ai fini della sicurezza.
5. L'integrità del giornale di controllo deve essere verificata con frequenza almeno mensile.
6. Le registrazioni contenute nel giornale di controllo devono essere conservate per un periodo non inferiore a dieci anni.

Art.43
(Sistema di qualità del certificatore)

1. Entro un anno dall'avvio dell'attività di certificazione, il certificatore deve dichiarare la conformità del proprio sistema di qualità alle norme ISO 9000, successive evoluzioni o a norme equivalenti.
2. Il manuale della qualità deve essere reso disponibile presso il certificatore.

Art.44
(Affidabilità hardware e software)

1. Il certificatore deve garantire che tutti i sistemi, l’hardware e il software utilizzati siano sicuri, affidabili e protetti contro le alterazioni e la contraffazione.
2. Gli strumenti e il software utilizzati in relazione alle firme elettroniche soddisfano ai requisiti specificati nel comma 1 se conformi alle norme pubblicate nella Gazzetta Ufficiale dell’Unione Europea.

Art.45
(Verifiche di sicurezza)

1. Il verificatore di sicurezza è una persona fisica o giuridica, indipendente dall'ente di certificazione, riconosciuta come idonea, con esperienza e qualifiche comprovate nell'area della sicurezza dell'informazione, dell'esecuzione di verifiche di sicurezza e dell'attuazione della norma ISO/IEC 17799, e riconosciuta dall'Autorità per l'Informatica.
2. L'ente di certificazione prova attraverso il rapporto annuale di verifica di sicurezza, effettuata da verificatore di sicurezza accreditato, di aver realizzato una valutazione dei rischi e di avere identificato e implementato i controlli necessari alla sicurezza dell'informazione.
3. Le verifiche di sicurezza sono effettuate in base alla norma ISO/IEC 17799, dovendo la rispettiva relazione del verificatore essere inviata all'Autorità per l'Informatica entro il 31 marzo di ogni anno.
4. Il verificatore di sicurezza garantisce che i suoi collaboratori agiscano in modo imparziale e non discriminatorio e non abbiano prestato servizi di consulenza a enti di certificazione nei tre anni precedenti, né mantengano con questi alcun accordo o vincolo contrattuale.
5. In caso di subappalto, il verificatore deve:

a) informare previamente un ente di certificazione e ottenere da questo l'approvazione per un subappalto;
b) garantire l'esistenza di un contratto in forma scritta nel quale siano chiaramente identificate le funzioni delegate e in cui siano stabiliti gli obblighi fra le parti, in particolare riguardo la riservatezza e l'indipendenza degli interessi commerciali o di altro tipo, oltre alla garanzie dell'assenza di qualsiasi tipo di vincolo con un ente di certificazione sottoposto a verifica;
c) garantire di essere atto a comprovare la competenza tecnica, idoneità ed estraneità dall'ente subappaltatore, e che questo adempia al disposto del punto precedente;
d) assumere la piena responsabilità delle funzioni date in subappalto e del rapporto finale di verifica.

Art.46
(Organizzazione del personale del certificatore)

1. L'organizzazione del personale del certificatore deve prevedere almeno le seguenti funzioni:

a) responsabile della sicurezza;
b) responsabile della generazione e custodia delle chiavi;
c) responsabile della personalizzazione dei dispositivi di firma elettronica;
d) responsabile della generazione dei certificati;
e) responsabile della gestione del registro dei certificati;
f) responsabile della registrazione degli utenti;
g) responsabile della sicurezza dei dati;
h) responsabile della crittografia o di altro sistema utilizzato;
i) responsabile dei servizi tecnici;
l) responsabile delle verifiche e delle ispezioni (auditing);
m) responsabile del sistema di riferimento temporale.

2. È possibile attribuire al medesimo soggetto più funzioni tra quelle previste dal comma 1 purché tra loro compatibili; sono in ogni caso compatibili tra loro le funzioni specificate nei sotto indicati raggruppamenti:

a) generazione e custodia delle chiavi, generazione dei certificati, personalizzazione dei dispositivi di firma elettronica, crittografia, sicurezza dei dati;
b) registrazione degli utenti, gestione del registro dei certificati, crittografia, sicurezza dei dati, sistema di riferimento temporale.

Art.47
(Requisiti di competenza ed esperienza del personale)

1. Il personale cui sono attribuite le funzioni previste dall'articolo 46 deve aver maturato una esperienza almeno quinquennale nella analisi, progettazione e conduzione di sistemi informatici.
2. Per ogni aggiornamento apportato al sistema di certificazione deve essere previsto un apposito corso di addestramento.

Art.48
(Formato dei certificati qualificati)

1. I certificati qualificati e le informazioni relative alle procedure di sospensione e di revoca devono essere conformi alla norma ISO/IEC 9594-8:2001 e successive evoluzioni.

Art.49
(Formato della firma digitale)

1. Alla firma digitale deve essere allegato il certificato qualificato corrispondente alla chiave pubblica da utilizzare per la verifica.

Art.50
(Codice di emergenza)

1. Per ciascun certificato qualificato emesso il certificatore deve fornire al titolare almeno un codice riservato, da utilizzare in caso di emergenza per confermare l'autenticità della eventuale richiesta di sospensione del certificato.
2. In caso di emergenza è possibile richiedere la sospensione immediata di un certificato qualificato utilizzando il codice previsto al comma 1. La richiesta deve essere successivamente confermata utilizzando una delle modalità previste dal certificatore.
3. Il codice d'emergenza deve essere mantenuto segreto dal certificatore il quale adotterà le idonee specifiche misure di sicurezza.

Art.51
(Manuale operativo)

1. Il manuale operativo definisce le procedure applicate dal certificatore che rilascia certificati qualificati nello svolgimento della sua attività.
2. Il manuale operativo deve essere pubblicato a cura del certificatore in modo da essere consultabile per via telematica.
3. Il manuale deve contenere almeno le seguenti informazioni:

a) dati identificativi del certificatore;
b) dati identificativi della versione del manuale operativo;
c) responsabile del manuale operativo;
d) definizione degli obblighi del certificatore, del titolare e dei richiedenti la verifica delle firme elettroniche;
e) definizione delle responsabilità e delle eventuali limitazioni agli indennizzi;
f) indirizzo del sito web del certificatore ove sono pubblicate le tariffe;
g) modalità di identificazione e registrazione degli utenti;
h) modalità di generazione delle chiavi per la creazione e la verifica della firma digitale;
i) modalità di emissione dei certificati;

l) modalità con cui viene espletato quanto previsto all'articolo 4 punto a) della Legge 20 luglio 2005 n.115;
m) modalità di sospensione e revoca dei certificati;
n) modalità di sostituzione delle chiavi;
o) modalità di gestione del registro dei certificati;
p) modalità di accesso al registro dei certificati;
q) modalità di protezione della riservatezza;
r) modalità per l'apposizione e la definizione del riferimento temporale;
s) modalità operative per l'utilizzo del sistema di verifica delle firme elettroniche di cui all'articolo 10;
t) modalità operative per la generazione della firma digitale.

Art.52

(Responsabilità dei prestatori di servizi di certificazione)

Oltre quanto previsto dall'articolo 6 della Legge 20 luglio 2005 n.115, si ha:

a) I prestatori di servizi di certificazione saranno responsabili per i danni che possano derivare a qualsiasi persona nell'esercizio della loro attività quando non adempiano gli obblighi imposti dalla Legge 20 luglio 2005 n. 115 e il presente regolamento tecnico. La responsabilità del prestatore di servizi di certificazione sarà esigibile in conformità alle norme generali in materia di responsabilità contrattuale o extracontrattuale, ove ne sussistano i presupposti, anche se rimarrà a carico del prestatore di servizi di certificazione dimostrare di non aver agito con negligenza.
b) I prestatori di servizi di certificazione saranno altresì responsabili per i danni derivanti a qualsiasi persona che utilizzi o si fidi di certificati riconosciuti rilasciati da un prestatore di servizi di certificazione costituito in uno Stato non appartenente alla Comunità Europea di cui avesse dato garanzia al pubblico in conformità all'articolo 14, punto b).
c) I prestatori di servizi di certificazione si assumeranno ogni responsabilità nei confronti di terzi per la condotta di persone cui abbiano delegato l'esecuzione di una o più funzioni necessarie alla prestazione dei servizi di certificazione.

Art.53

(Responsabilità e risarcimento dei danni)

1. Il certificatore che offre al pubblico certificati qualificati ha l'obbligo di risarcire i danni a chiunque abbia fondati motivi per ritenere di avere subito danni o perdite attribuibili a dette autenticazioni, dovuti ai seguenti motivi:

a) i dati riportati sul certificato qualificato erano sbagliati al momento del rilascio del certificato stesso;
b) il certificato qualificato non contiene le informazioni di cui all'articolo 21, comma 2;
c) la persona indicata nel certificato qualificato non era, al momento del rilascio del certificato, in possesso dei dati utilizzati per la creazione della firma digitale e corrispondenti ai dati di controllo della stessa dichiarati o indicati nel certificato;
d) l'insieme dei dati utilizzati per la creazione e la verifica della firma digitale creata dal certificatore non sono compatibili;
e) il certificatore non ha annullato il certificato qualificato seguendo le modalità indicate negli articoli 25, 26, 27, 28, 29, 30, 31, 32, 33, 34 e 35.

2. Il certificatore non ha alcun obbligo di risarcimento dei danni nel caso in cui sia in grado di dimostrare che le perdite o i danni non sono attribuibili a negligenza propria o di chiunque altro al quale abbia richiesto assistenza.

3. Il certificatore può limitare le proprie responsabilità mediante accordi specifici. Il

certificatore non è responsabile delle perdite causate da usi in contrasto con quelli consentiti.

Art.54

(Limitazioni della responsabilità dei prestatori di servizi di certificazione)

1. Il prestatore di servizi di certificazione non sarà responsabile per i danni derivanti al firmatario o a terzi in buona fede, per l'inadempimento dei seguenti doveri inerenti alla condizione di firmatario:

a) per l'inadempimento da parte del firmatario di dare al prestatore di servizi di certificazione informazioni veritiere, complete ed esatte circa i dati che devono risultare sul certificato o che siano necessari al suo rilascio, revoca o sospensione, quando al certificatore non sia stato possibile individuare la loro inesattezza, in conformità a quanto previsto agli articoli 16 e 17;
b) per l'inadempimento da parte del firmatario di dare comunicazione tempestiva al prestatore di servizi di certificazione di qualsiasi modifica delle circostanze riflesse nel certificato. Nel caso dei certificati che facciano riferimento a procura a rappresentare del firmatario, tanto questi quanto la persona rappresentata hanno l'onere di richiedere la revoca del certificato;
c) per l'inadempimento da parte del firmatario di conservare con diligenza i dati di creazione della firma digitale allo scopo di garantirne la segretezza e di proteggerli da qualsiasi accesso o rivelazione;
d) per l'inadempimento da parte del firmatario di richiedere la sospensione o la revoca del certificato nel caso di dubbi circa il mantenimento della segretezza dei dati corrispondenti alla creazione della firma digitale;
e) per l'inadempimento da parte del firmatario di astenersi dall'utilizzo dei dati di creazione della firma digitale dal momento in cui sia scaduto il periodo di validità del certificato o il prestatore di servizi di certificazione dia comunicazione della perdita di validità o della sospensione;
f) per l'inadempimento da parte del firmatario di attenersi alle condizioni limite che compaiono nel certificato, relativamente agli usi consentiti ed all'ammontare delle transazioni che possano essere condotte con esso, ed utilizzarlo in conformità alle condizioni stabilite e comunicate al firmatario dal prestatore di servizi di certificazione.

2. Il prestatore di servizi di certificazione non sarà neppure responsabile per danni e pregiudizi derivanti al firmatario o a terzi in buona fede, se il destinatario dei documenti firmati elettronicamente non adempie qualsiasi dei seguenti doveri di diligenza:

a) verificare e prendere atto delle restrizioni che compaiono nel certificato relativamente agli usi consentiti ed all'importo specificato delle transazioni possibili con esso;
b) assicurarsi della validità del certificato, mediante consultazione del servizio di pubblicazione dei certificati che il certificatore mantenga e verificare la firma digitale.

3. Il prestatore di servizi di certificazione non sarà responsabile per danni e pregiudizi derivanti al firmatario o a terzi in buona fede per l'inesattezza dei dati che risultino sul certificato, se questi sono stati a lui accreditati a mezzo di documento pubblico notarile, giudiziale o amministrativo.

Art.55

(Responsabilità in materia di uso non autorizzato dei dati utilizzati per la creazione delle firme elettroniche)

1. Il certificatore è responsabile dell'uso non autorizzato dei dati utilizzati per la creazione delle firme elettroniche unicamente nel caso in cui egli abbia fornito tali dati a terzi o non abbia rispettato l'obbligo di notifica al titolare.

2. Il certificatore non è responsabile dell'uso non autorizzato dei dati utilizzati per la creazione delle firme elettroniche nei casi in cui tali dati siano stati utilizzati dopo il ricevimento della comunicazione di perdita del titolo su tali dati.

Art.56
(Uso della banca dati sulla popolazione)

1. Il certificatore è autorizzato, dietro espresso consenso del richiedente un certificato, ad acquisire e verificare i dati personali forniti dal richiedente rispetto a quelli contenuti nella banca dati sulla popolazione.

Art.57
(Diritto di richiedere informazioni)

1. Indipendentemente dalle norme sulla riservatezza contenute nelle leggi vigenti, l'Autorità per l'Informatica ha il diritto di ottenere dai certificatori operanti sul territorio nazionale tutti i dati necessari a verificare il corretto adempimento delle disposizioni presenti nella Legge 20 luglio 2005 n.115 e nel presente decreto.

Art.58
(Obbligo di riservatezza)

1. È fatto divieto a chiunque nello svolgimento dei compiti stabiliti dal presente regolamento e dalla Legge 20 luglio 2005 n.115 venga a conoscenza di notizie commerciali o professionali riservate, di rivelarle a terzi o di utilizzarle a proprio vantaggio.

Art.59
(Obblighi di informazione)

1. Nell'esercizio della sua attività il prestatore di servizi di certificazione è tenuto a divulgare le seguenti informazioni:
a) prezzo dei servizi offerti;
b) dichiarazione delle pratiche di certificazione;
c) termini, condizioni e ambito di utilizzo dei suoi certificati;
d) mezzo di comunicazione, permanentemente disponibile, per procedere alla richiesta di sospensione e/o revoca del certificato;
e) che l'informazione registrata, necessaria all'utilizzo del certificato, non sia utilizzata per altri fini;
f) periodo di tempo durante il quale mantiene in archivio l'informazione prestata al richiedente e il riferimento per l'utilizzo dei certificati corrispondenti;
g) che, in caso di cessazione dell'attività, l'informazione riferita nel comma precedente sia trasmessa, nei termini previsti dal regolamento, ad un altro ente qualificato;
h) meccanismi utilizzati per la risoluzione dei conflitti;
i) legislazione applicabile all'attività di certificazione.

Art.60
(Obblighi del titolare)

1. Il titolare del certificato si impegna, adottando le misure necessarie, a non causare danni a terzi e a tutelare la riservatezza dell'informazione trasmessa, ed è obbligato a:
a) utilizzare le chiavi crittografiche nei limiti stabiliti dalla rispettiva politica di certificazione;
b) garantire la riservatezza della chiave privata;
c) utilizzare l'algoritmo e la lunghezza della chiave a norma degli articoli 5 e 6, nel caso crei le sue proprie chiavi;
d) usare un dispositivo sicuro di creazione della firma elettronica, se così richiesto dalla politica di

certificazione;
e) creare le chiavi all'interno di un dispositivo sicuro di creazione della firma digitale, se richiesto dalla politica di certificazione;
f) informare immediatamente l'ente di certificazione, nel caso di perdita di controllo della chiave privata o di inesattezza o alterazione dell'informazione contenuta nel certificato, durante il periodo di validità dello stesso.

Art.61
(Obblighi del richiedente)

1. Gli obblighi del richiedente a nome proprio sono gli stessi obblighi del titolare di cui all'articolo precedente.
2. Il richiedente a nome altrui ha l'obbligo di informare il titolare riguardo ai termini e alle condizioni di utilizzo dei certificati e alle conseguenze dell'inadempimento.

Art.62
(Contratto)

1. Il contratto fra l'ente di certificazione e il richiedente deve essere redatto in forma scritta, in linguaggio chiaro e accessibile, su un supporto fisico durevole e sottoscritto dalle parti mediante firma elettronica qualificata, se si tratta di un documento elettronico, o mediante firma autografa, se è su supporto cartaceo.
2. Le clausole del contratto stabilito fra l'ente di certificazione e il richiedente, devono contenere:
a) gli obblighi dell'ente di certificazione;
b) gli obblighi del richiedente.
3. Il contratto fra l'ente di certificazione e il richiedente deve essere registrato e archiviato dall'ente di certificazione per un periodo minimo di venti anni.

Art.63
(Riferimenti temporali)

1. I riferimenti temporali debbono essere realizzati in conformità con quanto disposto dal Titolo III.
2. I riferimenti temporali debbono essere apposti dal fornitore di servizi sul giornale di controllo.
3. L'ora assegnata ai riferimenti temporali di cui al precedente comma 2, deve corrispondere alla scala di tempo UTC(IEN), con una differenza non superiore ad un minuto primo.

Art.64
(Sospensione dell'attività del certificatore)

1. Nel caso di sospensione della propria attività, oltre a darne comunicazione all'Autorità per l'Informatica, il certificatore dovrà revocare i certificati validi o adoperarsi affinché almeno i suoi servizi elenchi e servizi di revoca vengano rilevati da un altro certificatore. Andranno comunque informati senza indugio i firmatari circa la sospensione dell'attività e la revoca o il rilievo dei servizi. Il certificatore deve garantire, anche in caso di revoca dei certificati, la prosecuzione dei servizi di revoca.

Art.65
(Documentazione del certificatore)

1. Un certificatore deve documentare le misure di sicurezza adottate per il rispetto della Legge 20 luglio 2005 n.115 e dei relativi regolamenti, nonché l'emissione e l'eventuale blocco o revoca di certificati. I dati, la loro integrità e il momento del loro inserimento nel sistema di verbalizzazione devono essere verificabili in qualsiasi momento.
2. Un certificatore deve consegnare la documentazione di cui al precedente comma su richiesta del Tribunale Unico o dell'Autorità per l'Informatica.

Art.66
(Rappresentazione del documento informatico)

1. Il certificatore deve indicare nel manuale operativo i formati del documento informatico e le modalità operative a cui il titolare deve attenersi per ottemperare a quanto prescritto dall'articolo 3, comma 2 del presente decreto.

Art.67
(Limitazioni d'uso)

1. Il certificatore, su richiesta del titolare o del terzo interessato, è tenuto a inserire nel certificato qualificato eventuali limitazioni d'uso.

TITOLO III
REGOLE PER LA VALIDAZIONE TEMPORALE E PER LA PROTEZIONE DEI DOCUMENTI INFORMATICI

Art.68
(Validazione temporale)

1. Una evidenza informatica è sottoposta a validazione temporale con la generazione di una marca temporale che le si applichi.
2. Le marche temporali sono generate da un apposito sistema elettronico sicuro in grado di:
a) mantenere la data e l'ora conformemente a quanto richiesto dal presente regolamento;
b) generare la struttura di dati secondo quanto specificato negli articoli 69 e 72;
c) sottoscrivere digitalmente la struttura di dati di cui al precedente punto b).

Art.69
(Informazioni contenute nella marca temporale)

1. Una marca temporale deve contenere almeno le seguenti informazioni:
a) identificativo dell'emittente;
b) numero di serie della marca temporale;
c) algoritmo di sottoscrizione della marca temporale;
d) identificativo del certificato relativo alla chiave di verifica della marca;
e) data ed ora di generazione della marca;
f) identificatore dell'algoritmo di hash utilizzato per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale;
g) valore dell'impronta dell'evidenza informatica.
2. La marca temporale può inoltre contenere un identificatore dell'oggetto a cui appartiene l'impronta di cui al precedente comma 1, punto g).

Art.70
(Chiavi di marcatura temporale)

1. Ogni coppia di chiavi utilizzata per la validazione temporale deve essere univocamente associata ad un sistema di validazione temporale.
2. Al fine di limitare il numero di marche temporali generate con la medesima coppia, le chiavi di marcatura temporale devono essere sostituite ed un nuovo certificato deve essere emesso dopo non più di un mese di utilizzazione, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente certificato.
3. Per la sottoscrizione dei certificati relativi a chiavi di marcatura temporale devono essere utilizzate chiavi di certificazione appositamente generate.
4. Le chiavi di certificazione e di marcatura temporale possono essere generate esclusivamente dai responsabili dei rispettivi servizi.

Art.71
(Gestione dei certificati e delle chiavi)

1. Alle chiavi di certificazione utilizzate ai sensi dell'articolo 70, comma 3, per sottoscrivere i certificati relativi a chiavi di marcatura temporale, si applica quanto previsto per le chiavi di certificazione utilizzate per sottoscrivere certificati relativi a chiavi di sottoscrizione.
2. I certificati relativi ad una coppia di chiavi di marcatura temporale, oltre ad essere conformi alla norma ISO/IEC 9594-8:2001 e successive evoluzioni, devono contenere l'identificativo del sistema di marcatura temporale che utilizza le chiavi.

Art.72
(Precisione dei sistemi di validazione temporale)

1. L'ora assegnata ad una marca temporale deve corrispondere, con una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC(IEN), al momento della sua generazione.
2. La data e l'ora contenute nella marca temporale sono specificate con riferimento al Tempo Universale Coordinato (UTC).

Art.73
(Sicurezza dei sistemi di validazione temporale)

1. Ogni sistema di validazione temporale deve produrre un registro operativo su di un supporto non riscrivibile nel quale siano automaticamente registrati gli eventi per i quali tale registrazione è richiesta dal presente regolamento.
2. Qualsiasi anomalia o tentativo di manomissione che possa modificare il funzionamento dell'apparato in modo da renderlo incompatibile con i requisiti del presente regolamento, ed in particolare con quello di cui all'articolo 72, comma 1, deve essere annotato sul registro operativo e causare il blocco del sistema.
3. Il blocco del sistema di validazione temporale può essere rimosso esclusivamente con l'intervento di personale espressamente autorizzato.
4. La conformità ai requisiti di sicurezza specificati nel presente articolo deve essere verificata secondo criteri di sicurezza almeno equivalenti a quelli previsti dal livello di valutazione E2 e robustezza dei meccanismi HIGH dell'ITSEC, o dal livello EAL 3 della norma ISO/IEC 15408 o superiori. Sono ammessi livelli di valutazione internazionalmente riconosciuti come equivalenti.

Art.74

(Registrazione delle marche generate)

1. Tutte le marche temporali emesse da un sistema di validazione sono conservate in un apposito archivio digitale non modificabile per un periodo non inferiore a dieci anni ovvero, su richiesta dell'interessato, per un periodo maggiore, alle condizioni previste dal certificatore.
2. La marca temporale è valida per l'intero periodo di conservazione a cura del fornitore del servizio.

Art.75
(Richiesta di validazione temporale)

1. Il certificatore stabilisce, pubblicandole nel manuale operativo, le procedure per l'inoltro della richiesta di validazione temporale.
2. La richiesta deve contenere l'evidenza informatica alla quale le marche temporali debbono fare riferimento.
3. L'evidenza informatica può essere sostituita da una o più impronte, calcolate con funzioni di hash previste dal manuale operativo. Debbono essere comunque accettate le funzioni di hash basate sugli algoritmi dedicated hash-function 3, corrispondente alla funzione SHA-1 e dedicated hash-function 1, corrispondente alla funzione RIPEMD-160, definiti nella norma ISO/IEC 10118-3:1998.
4. Il certificatore ha facoltà di implementare il sistema di validazione temporale in modo che sia possibile richiedere l'emissione di più marche temporali per la stessa evidenza informatica. In tal caso debbono essere restituite marche temporali generate con chiavi diverse.
5. La generazione delle marche temporali deve garantire un tempo di risposta, misurato come differenza tra il momento della ricezione della richiesta e l'ora riportata nella marca temporale, non superiore al minuto primo.

Art.76
(Estensione della validità del documento informatico)

1. La validità di un documento informatico, i cui effetti si protraggano nel tempo oltre il limite della validità della chiave di sottoscrizione, può essere estesa mediante l'associazione di una o più marche temporali.

TITOLO IV
ARCHIVIAZIONE ELETTRONICA

Art.77
(Definizioni)

1. Ai fini del presente regolamento si intende per:
a) DOCUMENTO: rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica;
b) DOCUMENTO ANALOGICO: documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiche, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video). Si distingue in documento originale e copia;
c) DOCUMENTO ANALOGICO ORIGINALE: documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;
d) DOCUMENTO INFORMATICO: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

e) SUPPORTO OTTICO DI MEMORIZZAZIONE: mezzo fisico che consente la memorizzazione di documenti informatici mediante l'impiego della tecnologia laser (quali, ad esempio, dischi ottici, magneto-ottici, DVD);
f) MEMORIZZAZIONE: processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici, anche sottoscritti ai sensi della Legge 20 luglio 2005 n.115;
g) ARCHIVIAZIONE ELETTRONICA: processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti, così come individuati nel precedente punto f), univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione;
h) DOCUMENTO ARCHIVIATO: documento informatico, anche sottoscritto, così come individuato nel precedente punto f), sottoposto al processo di archiviazione elettronica;
i) CONSERVAZIONE SOSTITUTIVA: processo effettuato con le modalità di cui agli articoli 79 ed 80;
l) DOCUMENTO CONSERVATO: documento sottoposto al processo di conservazione sostitutiva;
m) ESIBIZIONE: operazione che consente di visualizzare un documento conservato e di ottenerne copia;
n) RIVERSAMENTO DIRETTO: processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione informatica. Per tale processo non sono previste particolari modalità;
o) RIVERSAMENTO SOSTITUTIVO: processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, modificando la loro rappresentazione informatica. Per tale processo sono previste le modalità descritte nell'articolo 79, comma 2, e nell'articolo 80, comma 4, del presente decreto;
p) RIFERIMENTO TEMPORALE: informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici;
q) PUBBLICO UFFICIALE: il notaio, salvo quanto previsto dall'articolo 81, comma 4 del presente decreto e nei casi per i quali possono essere chiamate in causa le altre figure previste per l’autenticazione di copie conformi con l’originale (notaio, cancelliere od altro funzionario incaricato);
r) EVIDENZA INFORMATICA: una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica;
s) IMPRONTA: la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l’applicazione alla prima di una opportuna funzione di hash;
t) FUNZIONE DI HASH: una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali.

Art.78

(Obblighi di conservazione sostitutiva)

1. Gli obblighi di conservazione sostitutiva dei documenti, previsti dalla legislazione vigente sia per le pubbliche amministrazioni sia per i privati, sono soddisfatti a tutti gli effetti, fatto salvo quanto indicato dall’articolo 83, qualora il processo di conservazione venga effettuato con le modalità di cui agli articoli 79 ed 80.
2. I documenti informatici, anche sottoscritti, così come individuati nel precedente articolo 77, punto f), possono essere archiviati elettronicamente prima di essere sottoposti al processo di conservazione. Per l'archiviazione elettronica non sussistono gli obblighi di cui al presente decreto.

Art.79

(Conservazione sostitutiva di documenti informatici)

1. Il processo di conservazione sostitutiva di documenti informatici, anche sottoscritti, così come individuati nel precedente articolo 77, punto f), ed, eventualmente, anche delle loro impronte, avviene mediante memorizzazione su supporti ottici e termina con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta il corretto svolgimento del processo.
2. Il processo di riversamento sostitutivo di documenti informatici conservati avviene mediante memorizzazione su altro supporto ottico e termina con l'apposizione sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta il corretto svolgimento del processo. Qualora il processo riguardi documenti informatici sottoscritti, così come individuati nell'articolo 77, punto f), è inoltre richiesta l'apposizione del riferimento temporale e della firma digitale, da parte di un pubblico ufficiale, per attestare la conformità di quanto riversato al documento d'origine.

Art.80

(Conservazione sostitutiva di documenti analogici)

1. Il processo di conservazione sostitutiva di documenti analogici avviene mediante memorizzazione della relativa immagine direttamente sui supporti ottici, eventualmente, anche della relativa impronta, e termina con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta così il corretto svolgimento del processo.
2. Il processo di conservazione sostitutiva di documenti analogici originali unici si conclude con l'ulteriore apposizione del riferimento temporale e della firma digitale da parte di un pubblico ufficiale per attestare la conformità di quanto memorizzato al documento d'origine.
3. La distruzione di documenti analogici, di cui è obbligatoria la conservazione, è consentita soltanto dopo il completamento della procedura di conservazione sostitutiva, fatto salvo il parere dell'Archivio Pubblico.
4. Il processo di riversamento sostitutivo di documenti analogici conservati avviene mediante memorizzazione su altro supporto ottico. Il responsabile della conservazione, al termine del riversamento, ne attesta il corretto svolgimento con l'apposizione del riferimento temporale e della firma digitale sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi. Qualora il processo riguardi documenti originali unici di cui al precedente comma 2, è richiesta l'ulteriore apposizione del riferimento temporale e della firma digitale da parte di un pubblico ufficiale per attestare la conformità di quanto riversato al documento d'origine.

Art.81

(Responsabile della conservazione)

1. Il responsabile del procedimento di conservazione sostitutiva:
a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conservare, della quale tiene evidenza. Organizza conseguentemente il contenuto dei supporti ottici e gestisce le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato;
b) archivia e rende disponibili, con l'impiego di procedure elaborative, relativamente ad ogni

supporto di memorizzazione utilizzato, le seguenti informazioni:

I) descrizione del contenuto dell'insieme dei documenti;
II) estremi identificativi del responsabile della conservazione;
III) estremi identificativi delle persone eventualmente delegate dal responsabile della conservazione, con l'indicazione dei compiti alle stesse assegnati;
IV) indicazione delle copie di sicurezza.

c) mantiene e rende accessibile un archivio del software dei programmi in gestione nelle eventuali diverse versioni;
d) verifica la corretta funzionalità del sistema e dei programmi in gestione;
e) adotta le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione sostitutiva e delle copie di sicurezza dei supporti di memorizzazione;
f) richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
g) definisce e documenta le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
h) verifica periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.

2. Il responsabile del procedimento di conservazione sostitutiva può delegare, in tutto o in parte, lo svolgimento delle proprie attività ad una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni ad esse delegate.
3. Il procedimento di conservazione sostitutiva può essere affidato, in tutto o in parte, ad altri soggetti, pubblici o privati, i quali sono tenuti ad osservare quanto previsto dal presente decreto.
4. Nelle amministrazioni pubbliche il ruolo di pubblico ufficiale è svolto dal dirigente dell'ufficio responsabile della conservazione dei documenti o da altri dallo stesso formalmente designati, fatta eccezione per quanto previsto dall'articolo 79, comma 2, e dall'articolo 80, commi 2 e 4, casi nei quali si richiede l'intervento di soggetto diverso della stessa amministrazione.

Art.82
(Obbligo di esibizione)

1. Il documento conservato deve essere reso leggibile in qualunque momento presso il sistema di conservazione sostitutiva e disponibile, a richiesta, su supporto cartaceo.
2. Il documento conservato può essere esibito anche per via telematica.
3. Qualora un documento conservato venga esibito su supporto cartaceo fuori dall'ambiente in cui è installato il sistema di conservazione sostitutiva, deve esserne dichiarata la conformità da parte di un pubblico ufficiale se si tratta di documenti per la cui conservazione è previsto il suo intervento.

Art.83
(Procedure operative)

1. A qualsiasi soggetto pubblico o privato che intenda avvalersi del processo di conservazione sostitutiva dei documenti è consentita l'adozione di accorgimenti e procedure integrative, nel rispetto di quanto stabilito nel presente regolamento.
2. Le pubbliche amministrazioni comunicano preliminarmente all'Autorità per l'Informatica le procedure integrative che intendono adottare ai sensi del precedente comma 1.

Art.84
(Altri supporti di memorizzazione)

Tenuto conto dell'evoluzione tecnologica, è data facoltà alle pubbliche amministrazioni ed ai privati, ove non ostino particolari motivazioni, di utilizzare, nei processi di conservazione sostitutiva e di riversamento sostitutivo, un qualsiasi supporto di memorizzazione, anche non ottico, comunque idoneo a garantire la conformità dei documenti agli originali, nel rispetto delle modalità previste dal presente decreto.

TITOLO IV-*BIS*
NORME SULLA DUPLICAZIONE E RIPRODUZIONE DEI DOCUMENTI ANALOGICI ED ELETTRONICI [6]

[6] **TESTO ORIGINARIO Decreto Delegato 30 gennaio 2020 n.9, Art. 4**
(Introduzione del Titolo IV-bis al Decreto n.156/2005)
1. Dopo il Titolo IV del Decreto n. 156/2005 è aggiunto il seguente Titolo IV-bis:
"TITOLO IV-BIS - NORME SULLA DUPLICAZIONE E RIPRODUZIONE DEI DOCUMENTI ANALOGICI ED ELETTRONICI
Art. 85-bis
(Copia informatica di documento analogico)
1. La copia informatica di documento analogico è il documento elettronico avente contenuti identici a quelli del documento analogico da cui è tratto.
2. I documenti elettronici contenenti copia di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo formati in origine su supporto analogico, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali oppure da altro pubblico impiegato autorizzato ad attribuirgli fede pubblica, hanno la stessa efficacia probatoria dell'originale da cui sono tratti, se la loro conformità è attestata dai predetti soggetti.
Laddove richiesta dalla natura dell'attività, l'attestazione di conformità può:
a) essere inserita nel documento elettronico contenente la copia informatica. Il documento
a) elettronico così formato è sottoscritto con firma elettronica qualificata del notaio, del pubblico ufficiale ovvero di altro pubblico impiegato autorizzato ad attribuirgli fede pubblica, oppure,
b) essere prodotta come documento elettronico separato contenente un riferimento temporale e l'impronta di ogni copia informatica. Il documento elettronico così formato è sottoscritto con firma elettronica qualificata del notaio, del pubblico ufficiale ovvero di altro pubblico impiegato autorizzato ad attribuirgli fede pubblica.
3. La copia informatica di un documento analogico è prodotta mediante processi e strumenti che assicurino la corrispondenza dei contenuti della copia elettronica alle informazioni del documento analogico di origine previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza dei contenuti dell'originale e della copia.
4. Le copie formate ai sensi del presente articolo sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal seguente comma 5.
5. Con delibera del Congresso di Stato, adottata su proposta dell'Unità Organizzativa (UO) Istituti Culturali possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale ovvero da altro pubblico impiegato autorizzato ad attribuirgli fede pubblica, con dichiarazione da questi firmata digitalmente ed allegata al documento elettronico.

Art. 85-ter
(Copia per immagine su supporto elettronico di documento analogico)
1. La copia per immagine su supporto elettronico di documento analogico è il documento elettronico avente contenuti e forma identici a quelli del documento analogico da cui è tratto.
2. Le copie per immagine su supporto elettronico di documenti originali formati in origine su supporto analogico sono prodotte mediante processi e strumenti che assicurino che il documento elettronico abbia contenuti e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e dei contenuti dell'originale e della copia.
3. Le copie per immagine su supporto elettronico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da notaio o da

pubblico ufficiale ovvero da altro pubblico impiegato autorizzato ad attribuirgli fede pubblica. Laddove richiesta dalla natura dell'attività, l'attestazione di conformità può:

a) essere inserita nel documento elettronico contenente la copia per immagine. Il documento elettronico così formato è sottoscritto con firma elettronica qualificata del notaio, del pubblico ufficiale ovvero di altro pubblico impiegato autorizzato ad attribuirgli fede pubblica, oppure,

b) essere prodotta come documento elettronico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento elettronico così formato è sottoscritto con firma elettronica qualificata del notaio, del pubblico ufficiale ovvero di altro pubblico impiegato autorizzato ad attribuirgli fede pubblica.

4. Le copie per immagine su supporto elettronico di documenti originali formati in origine su supporto analogico hanno, in assenza dell'attestazione di conformità di cui al comma 3, la stessa efficacia probatoria degli originali da cui sono estratte, qualora la loro conformità all'originale non sia espressamente disconosciuta.

5. Le copie formate ai sensi del presente articolo sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal seguente comma 6.

6. Con delibera del Congresso di Stato, adottata su proposta dell'Unità Organizzativa (UO) Istituti Culturali possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale ovvero da altro pubblico impiegato autorizzato ad attribuirgli fede pubblica, con dichiarazione da questi firmata digitalmente ed allegata al documento elettronico.

Art. 85 - quater
(Copia analogica di documento elettronico)

1. Le copie e gli estratti su supporto analogico di documento elettronico, anche sottoscritto con firma elettronica avanzata o qualificata, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un notaio, da un pubblico ufficiale ovvero da un altro pubblico impiegato autorizzato ad attribuirgli fede pubblica secondo quanto previsto dall'articolo 20 della Legge 5 ottobre 2011 n. 159.

2. L'attestazione di conformità di cui al comma 1 consiste nella dichiarazione della conformità della copia analogica al documento elettronico originale. Tale dichiarazione è redatta in calce alla copia analogica e deve recare l'indicazione della data e del luogo in cui è eseguita, nonché del nome, del cognome e della qualifica rivestita da colui che la esegue. Se il documento è formato da più pagine la dichiarazione è redatta in calce all'ultima pagina della copia con l'indicazione del numero dei fogli o delle pagine impiegati; colui che esegue l'autenticazione deve apporre la propria firma autografa sul margine di ogni pagina intermedia.

3. Le copie e gli estratti su supporto analogico del documento elettronico hanno la stessa efficacia probatoria dell'originale, in assenza dell'attestazione di cui ai commi 1 e 2, se la loro conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale elettronico.

4. Sulle copie ed estratti su supporto analogico di documenti elettronici può essere apposto a stampa un contrassegno tramite il quale è possibile accedere al documento elettronico, ovvero verificare la corrispondenza allo stesso della copia o estratto analogici. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa del pubblico ufficiale e non può essere richiesta la produzione di altra copia o estratto analogici con sottoscrizione autografa del medesimo documento elettronico. La verifica della autenticità del documento tramite il contrassegno avviene a mezzo applicativi software resi disponibili gratuitamente dai soggetti che procedono all'apposizione del contrassegno medesimo.

5. Le caratteristiche tecniche del contrassegno di cui al comma 4 sono stabilite con Regolamento del Congresso di Stato; con riferimento al contrassegno da utilizzare per i documenti informatici generati dal Registro pubblico dei domicili digitali e dal servizio elettronico di recapito certificato, la specifica tecnica è stabilita dal Regolamento 22 novembre 2018 n. 7.

6. Qualora il destinatario di comunicazioni e provvedimenti dell'Amministrazione sia sprovvisto del domicilio digitale di cui all'articolo 5 del Decreto Delegato 11 aprile 2016 n. 46, come modificato dal Decreto Delegato 26 luglio 2018 n. 92, l'Amministrazione può predisporre le comunicazioni ai soggetti privati a mezzo di documenti elettronici sottoscritti con firma elettronica qualificata, da conservare nei propri archivi, e trasmettere ai soggetti stessi, per posta ordinaria o raccomandata con avviso di ricevimento, copia o estratto su supporto analogico del documento elettronico originale.

Art. 85-quinquies
(Duplicati informatici)

Art. 85-*bis*

(Copia informatica di documento analogico)

1. La copia informatica di documento analogico è il documento elettronico avente contenuti identici a quelli del documento analogico da cui è tratto.
2. I documenti elettronici contenenti copia di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo formati in origine su supporto analogico, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali oppure da altro pubblico impiegato autorizzato ad attribuirgli fede pubblica, hanno la stessa efficacia probatoria dell'originale da cui sono tratti, se la loro conformità è attestata dai predetti soggetti.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità può:

a) essere inserita nel documento elettronico contenente la copia informatica. Il documento
a) elettronico così formato è sottoscritto con firma elettronica qualificata del notaio, del pubblico ufficiale ovvero di altro pubblico impiegato autorizzato ad attribuirgli fede pubblica, oppure,
b) essere prodotta come documento elettronico separato contenente un riferimento temporale e l'impronta di ogni copia informatica. Il documento elettronico così formato è sottoscritto con firma elettronica qualificata del notaio, del pubblico ufficiale ovvero di altro pubblico impiegato autorizzato ad attribuirgli fede pubblica.

3. La copia informatica di un documento analogico è prodotta mediante processi e strumenti che assicurino la corrispondenza dei contenuti della copia elettronica alle informazioni del documento analogico di origine previo raffronto dei documenti o attraverso certificazione di

---

1. Il duplicato elettronico è il documento elettronico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.
2. Il duplicato elettronico ha il medesimo valore giuridico, ad ogni effetto di legge, del documento elettronico da cui è tratto, se prodotto mediante processi e strumenti che assicurino che il documento elettronico ottenuto sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la stessa sequenza di bit del documento elettronico di origine.

Art. 85 - sexies

(Copie ed estratti informatici di documenti elettronici)

1. Le copie e gli estratti informatici del documento elettronico, se prodotti in conformità al comma 2, hanno la stessa efficacia probatoria dell'originale da cui sono tratti nei seguenti casi alternativi:

a) la loro conformità all'originale, in tutti le sue componenti, sia attestata da un notaio, da un pubblico ufficiale ovvero da altro pubblico impiegato autorizzato ad attribuirgli fede pubblica tramite sottoscrizione con firma elettronica qualificata;

b) in assenza dell'attestazione di cui alla lettera a), qualora siano sottoscritti con firma elettronica qualificata da chi effettua la copia o l'estratto, salvo che la conformità all'originale non sia espressamente disconosciuta.

2. La copia e gli estratti informatici di un documento elettronico sono prodotti attraverso l'utilizzo di uno dei formati idonei di cui all'Allegato 1, mediante processi e strumenti che assicurino la corrispondenza dei contenuti della copia o dell'estratto elettronico alle informazioni del documento elettronico di origine previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza dei contenuti dell'originale e della copia.

3. Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie o dell'estratto elettronico di un documento elettronico di cui al comma 1, lettera a), può:

a) essere inserita nel documento elettronico contenente la copia o l'estratto. Il documento elettronico così formato è sottoscritto con firma elettronica qualificata del notaio, del pubblico ufficiale ovvero di altro pubblico impiegato autorizzato ad attribuirgli fede pubblica, oppure,

b) essere prodotta come documento elettronico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto elettronico. Il documento elettronico così formato è sottoscritto con firma elettronica qualificata del notaio, del pubblico ufficiale ovvero di altro pubblico impiegato autorizzato ad attribuirgli fede pubblica.

4. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale elettronico.

processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza dei contenuti dell'originale e della copia.

4. Le copie formate ai sensi del presente articolo sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal seguente comma 5.

5. Con delibera del Congresso di Stato, adottata su proposta dell'Unità Organizzativa (UO) Istituti Culturali possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale ovvero da altro pubblico impiegato autorizzato ad attribuirgli fede pubblica, con dichiarazione da questi firmata digitalmente ed allegata al documento elettronico.

Art. 85-*ter*

(Copia per immagine su supporto elettronico di documento analogico)

1. La copia per immagine su supporto elettronico di documento analogico è il documento elettronico avente contenuti e forma identici a quelli del documento analogico da cui è tratto.

2. Le copie per immagine su supporto elettronico di documenti originali formati in origine su supporto analogico sono prodotte mediante processi e strumenti che assicurino che il documento elettronico abbia contenuti e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e dei contenuti dell'originale e della copia.

3. Le copie per immagine su supporto elettronico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da notaio o da pubblico ufficiale ovvero da altro pubblico impiegato autorizzato ad attribuirgli fede pubblica. Laddove richiesta dalla natura dell'attività, l'attestazione di conformità può:

a) essere inserita nel documento elettronico contenente la copia per immagine. Il documento elettronico così formato è sottoscritto con firma elettronica qualificata del notaio, del pubblico ufficiale ovvero di altro pubblico impiegato autorizzato ad attribuirgli fede pubblica, oppure,
b) essere prodotta come documento elettronico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento elettronico così formato è sottoscritto con firma elettronica qualificata del notaio, del pubblico ufficiale ovvero di altro pubblico impiegato autorizzato ad attribuirgli fede pubblica.

4. [abrogato] [7]

5. Le copie formate ai sensi del presente articolo sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal seguente comma 6.

6. Con delibera del Congresso di Stato, adottata su proposta dell'Unità Organizzativa (UO)

[7] **Testo originario (Decreto n.156/2005, come introdotto dall'articolo 4 del Decreto Delegato n.9/2020)**
Art. 85-*ter* comma 4
4. Le copie per immagine su supporto elettronico di documenti originali formati in origine su supporto analogico hanno, in assenza dell'attestazione di conformità di cui al comma 3, la stessa efficacia probatoria degli originali da cui sono estratte, qualora la loro conformità all'originale non sia espressamente disconosciuta
Modifiche legislative:
Decreto Delegato 21 marzo 2023 n.51, art. 26 comma 8
8. Sono abrogati:
-*omissis*-
e) l'articolo 85 ter, comma 4 del Decreto n.156/2005, come introdotto dall'articolo 4 del Decreto Delegato n.9/2020;
-*omissis*-

Istituti Culturali possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale ovvero da altro pubblico impiegato autorizzato ad attribuirgli fede pubblica, con dichiarazione da questi firmata digitalmente ed allegata al documento elettronico.

Art. 85 - *quater*
(Copia analogica di documento elettronico)

1. Le copie e gli estratti su supporto analogico di documento elettronico, anche sottoscritto con firma elettronica avanzata o qualificata, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un notaio, da un pubblico ufficiale ovvero da un altro pubblico impiegato autorizzato ad attribuirgli fede pubblica secondo quanto previsto dall'articolo 20 della Legge 5 ottobre 2011 n. 159.
2. L'attestazione di conformità di cui al comma 1 consiste nella dichiarazione della conformità della copia analogica al documento elettronico originale. Tale dichiarazione è redatta in calce alla copia analogica e deve recare l'indicazione della data e del luogo in cui è eseguita, nonché del nome, del cognome e della qualifica rivestita da colui che la esegue. Se il documento è formato da più pagine la dichiarazione è redatta in calce all'ultima pagina della copia con l'indicazione del numero dei fogli o delle pagine impiegati; colui che esegue l'autenticazione deve apporre la propria firma autografa sul margine di ogni pagina intermedia.
3. Le copie e gli estratti su supporto analogico del documento elettronico hanno la stessa efficacia probatoria dell'originale, in assenza dell'attestazione di cui ai commi 1 e 2, se la loro conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale elettronico.
4. Sulle copie ed estratti su supporto analogico di documenti elettronici può essere apposto a stampa un contrassegno tramite il quale è possibile accedere al documento elettronico, ovvero verificare la corrispondenza allo stesso della copia o estratto analogici. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa del pubblico ufficiale e non può essere richiesta la produzione di altra copia o estratto analogici con sottoscrizione autografa del medesimo documento elettronico. La verifica della autenticità del documento tramite il contrassegno avviene a mezzo applicativi software resi disponibili gratuitamente dai soggetti che procedono all'apposizione del contrassegno medesimo.
5. Le caratteristiche tecniche del contrassegno di cui al comma 4 sono stabilite con Regolamento del Congresso di Stato; con riferimento al contrassegno da utilizzare per i documenti informatici generati dal Registro pubblico dei domicili digitali e dal servizio elettronico di recapito certificato, la specifica tecnica è stabilita dal Regolamento 22 novembre 2018 n. 7.
6. Qualora il destinatario di comunicazioni e provvedimenti dell'Amministrazione sia sprovvisto del domicilio digitale di cui all'articolo 5 del Decreto Delegato 11 aprile 2016 n. 46, come modificato dal Decreto Delegato 26 luglio 2018 n. 92, l'Amministrazione può predisporre le comunicazioni ai soggetti privati a mezzo di documenti elettronici sottoscritti con firma elettronica qualificata, da conservare nei propri archivi, e trasmettere ai soggetti stessi, per posta ordinaria o raccomandata con avviso di ricevimento, copia o estratto su supporto analogico del documento elettronico originale.

Art. 85-*quinquies*
(Duplicati informatici)

1. Il duplicato elettronico è il documento elettronico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del

documento originario.
2. Il duplicato elettronico ha il medesimo valore giuridico, ad ogni effetto di legge, del documento elettronico da cui è tratto, se prodotto mediante processi e strumenti che assicurino che il documento elettronico ottenuto sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la stessa sequenza di bit del documento elettronico di origine.

Art. 85 - *sexies*
(Copie ed estratti informatici di documenti elettronici)

1. Le copie e gli estratti informatici del documento elettronico, se prodotti in conformità al comma 2, hanno la stessa efficacia probatoria dell'originale da cui sono tratti nei seguenti casi alternativi:
a) la loro conformità all'originale, in tutti le sue componenti, sia attestata da un notaio, da un pubblico ufficiale ovvero da altro pubblico impiegato autorizzato ad attribuirgli fede pubblica tramite sottoscrizione con firma elettronica qualificata;
b) in assenza dell'attestazione di cui alla lettera a), qualora siano sottoscritti con firma elettronica qualificata da chi effettua la copia o l'estratto, salvo che la conformità all'originale non sia espressamente disconosciuta.
2. La copia e gli estratti informatici di un documento elettronico sono prodotti attraverso l'utilizzo di uno dei formati idonei di cui all'Allegato 1, mediante processi e strumenti che assicurino la corrispondenza dei contenuti della copia o dell'estratto elettronico alle informazioni del documento elettronico di origine previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza dei contenuti dell'originale e della copia.
3. Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie o dell'estratto elettronico di un documento elettronico di cui al comma 1, lettera a), può:
a) essere inserita nel documento elettronico contenente la copia o l'estratto. Il documento elettronico così formato è sottoscritto con firma elettronica qualificata del notaio, del pubblico ufficiale ovvero di altro pubblico impiegato autorizzato ad attribuirgli fede pubblica, oppure,
b) essere prodotta come documento elettronico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto elettronico. Il documento elettronico così formato è sottoscritto con firma elettronica qualificata del notaio, del pubblico ufficiale ovvero di altro pubblico impiegato autorizzato ad attribuirgli fede pubblica.
4. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale elettronico.

TITOLO V
DISPOSIZIONI FINALI E TRANSITORIE

Art.85
(Standard di riferimento)

1. Secondo quanto previsto dall'articolo 3 del presente decreto, gli standard per la firma digitale riconosciuti dalla Commissione Europea relativi ai prestatori di servizi di certificazione che rilasciano certificati qualificati sono:
a) CWA 14167-1, del Marzo 2003: "Security requirements for trustworthy systems managing certificates for electronic signatures - Part 1: System Security Requirements";
b) CWA 14167-2, del Marzo 2002: "Security requirements for trustworthy systems managing certificates for electronic signatures - Part 2: cryptographic module for CSP signing operations - Protection Profile (MCSO-PP)".
2. Secondo quanto previsto dall'articolo 3 gli standard per la firma digitale riconosciuti dalla Commissione Europea relativi ai requisiti relativi ai dispositivi per la creazione di una firma

elettronica sicura sono:

a) CWA 14169, del Marzo 2002: “Secure signature-creation devices”.

3. I servizi elenchi ed i servizi di revoca devono essere tenuti in formato riconosciuto a livello internazionale. Per l’accesso ai servizi elenchi e servizi di revoca si applicano in particolare le seguenti norme internazionali:

a) 1988 CCITT (ITU-T) X.500 / ISO IS9594;

b) RCF2587 Internet X.509 Public Key Infrastructure LDAP v2 Schema;

c) RCF 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile;

d) RCF 2589 Lightweight Directory Access Protocol (LDAP v3) Extensions for Dynamic Directory Services.

4. I suddetti standard di riferimento possono essere soggetti a revisione periodica in funzione dell’evoluzione tecnologica. In particolare l’Autorità per l’Informatica provvederà a valutare la necessità di adeguamento degli standard entro un periodo di due anni a partire dalla pubblicazione del presente regolamento tecnico.

[Art.85-*bis*

(Norme transitorie in materia di firma elettronica remota)]

VEDERE **Art.2 bis**

(Firma elettronica remota) [8]

[8] **Testo originario DECRETO DELEGATO 29 ottobre 2021 n.184, Art.15**

(Firma elettronica remota)

1. Dopo l’articolo 85 del Decreto 8 novembre 2005 n.156 e successive modifiche è aggiunto il seguente articolo: “Art.85-*bis*

(Norme transitorie in materia di firma elettronica remota)

1. Sino alla revisione della Legge 20 luglio 2005 n.115 e del presente decreto delegato, come già modificato con Decreto Delegato 30 gennaio 2020 n.9, gli effetti giuridici che le predette norme di rango primario attribuiscono alle firme elettroniche qualificate basate su un certificato qualificato e create mediante un dispositivo sicuro per la creazione di una firma, sono riconosciuti anche alla “firma remota”, così come definita e disciplinata dal Decreto del Presidente del Consiglio dei Ministri (DPCM) 22 febbraio 2013 della Repubblica Italiana (in G.U.R.I. s.g. n.117 del 21/05/2013) e dai successivi futuri aggiornamenti e modifiche dello stesso.”.

Modifiche legislative:

DECRETO DELEGATO 21 marzo 2023 n.51, Art.26 comma 5

5. La numerazione e la rubrica dell’articolo 85bis del Decreto n.156/2005, come modificato dal CAPO IV FIRMA ELETTRONICA REMOTA e dall’articolo 15 Decreto Delegato n.184/2021, è così modificata: “Art.2bis (Firma elettronica remota)”.

DECRETO DELEGATO 11 aprile 2016 n.46 – ABROGATO [9]

DISPOSIZIONI PER L'UTILIZZO DI SERVIZI ELETTRONICI DI RECAPITO CERTIFICATO QUALIFICATI

CAPO I
DISPOSIZIONI GENERALI
Art. 1
(Finalità e ambito di applicazione)

1. Il presente decreto delegato disciplina l'utilizzo di servizi elettronici di recapito certificato qualificati, così come definiti a mente dell'articolo 2, comma 2, in attuazione della delega legislativa di cui all'articolo 79 della Legge 22 dicembre 2010 n. 194.

Art. 2
(Definizioni)

1. Ai fini del presente decreto
delegato i seguenti termini ed espressioni assumono i sotto indicati significati:

a) per "Amministrazione", "Settore Pubblico Allargato", "Pubblica Amministrazione" e "Enti": quanto rispettivamente definito dalle lettere a), b), c) e d) dell'articolo 3 comma 1, della Legge 5 dicembre 2011 n. 188;

b) per "documento o atto amministrativo" e per "documento o atto pubblico": quanto rispettivamente definito dai commi 2 e 3 dell'articolo 2 della Legge 5 ottobre 2011 n. 159.
Rientrano, pertanto, nella definizione di "documento o atto amministrativo" le istanze nonché gli atti e documenti di cui rispettivamente agli articoli 10 e 15, comma 1, lettera c) della Legge 5 ottobre 2011 n. 160;

c) per "documento informatico": quanto definito dall'articolo 1, comma 1, lettera b) della Legge 20 luglio 2005 n. 115. Il documento informatico firmato elettronicamente ai sensi della Legge n. 115/2005 e trasmesso mediante un servizio elettronico di recapito certificato qualificato è valido e rilevante a tutti gli effetti di legge; [soppresso].
Al di fuori dei casi sopra indicati, il documento informatico sprovvisto di firma elettronica ha l'efficacia probatoria della riproduzione meccanica;

d) [abrogata];

e) per "corrispondente":
1) il soggetto privato che si sia identificato ai sensi dell'articolo 5, comma 1 ai fini della trasmissione e/o ricezione di documenti o atti amministrativi, mediante un servizio elettronico di recapito certificato qualificato, con gli effetti giuridici di cui all'articolo 6;
2) gli organi e le Autorità dell'Amministrazione, le Unità Organizzative ed i Dipartimenti della Pubblica Amministrazione, le articolazioni organizzative degli Enti che si siano identificati ai sensi dell'articolo 5, comma 2 ai fini della trasmissione e ricezione di documenti o atti amministrativi, mediante un servizio elettronico di recapito certificato qualificato, con gli effetti giuridici di cui all'articolo 6.

e *bis*) per "domicilio digitale": l'indirizzo elettronico dichiarato dal soggetto interessato ed associato ai dati di identificazione delle persone fisiche e delle persone giuridiche.

2. Ai fini del presente decreto delegato, si intendono, altresì, integralmente recepite le definizioni di cui al Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, non in contrasto con quelle dettate nel

---

[9] **Modifiche legislative:**
DECRETO DELEGATO 21 marzo 2023 n.51
Art. 26, comma 3
3. Laddove il Decreto n.156/2005 e successive modifiche e le vigenti norme che prevedano l'utilizzo del SERC facciano riferimento al Decreto Delegato 11 aprile 2016 n.46 e successive modifiche ed al Decreto Delegato 26 luglio 2018 n. 92 ovvero a specifici articoli degli stessi, il richiamo deve intendersi effettuato al presente decreto delegato.
DECRETO DELEGATO 21 marzo 2023 n.51, Art.26 comma 8
8. Sono abrogati:
a) il Decreto Delegato 11 aprile 2016 n.46;
- *omissis* -

presente e nei successivi articoli.[10]

Art. 3
(Ambito e modalità di applicazione)

[10] **Testo originario**: **(D.D. n. 46/2016):**
Art. 2 *(Definizioni)*
1. Ai fini del presente decreto delegato i seguenti termini ed espressioni assumono i sotto indicati significati:
   a) per "Amministrazione", "Settore Pubblico Allargato", "Pubblica Amministrazione" e "Enti": quanto rispettivamente definito dalle lettere a), b), c) e d) dell'articolo 3 comma 1, della Legge 5 dicembre 2011 n. 188;
   b) per "documento o atto amministrativo" e per "documento o atto pubblico": quanto rispettivamente definito dai commi 2 e 3 dell'articolo 2 della Legge 5 ottobre 2011 n. 159.
   Rientrano, pertanto, nella definizione di "documento o atto amministrativo" le istanze nonché gli atti e documenti di cui rispettivamente agli articoli 10 e 15, comma 1, lettera c) della Legge 5 ottobre 2011 n. 160;
   c) per "documento informatico": quanto definito dall'articolo 1, comma 1, lettera b) della Legge 20 luglio 2005 n. 115. Il documento informatico firmato elettronicamente ai sensi della Legge n. 115/2005 e trasmesso mediante un servizio elettronico di recapito certificato qualificato è valido e rilevante a tutti gli effetti di legge; la medesima validità e rilevanza a tutti gli effetti di legge è riconosciuta, esclusivamente nel procedimento amministrativo in cui è acquisito, al documento informatico sprovvisto di firma elettronica ma trasmesso, mediante un servizio elettronico di recapito certificato qualificato, all'Amministrazione che abbia provveduto ad autenticarlo ai sensi dell'articolo 20, comma 2, lettera b) della Legge 5 ottobre 2011 n. 159. Al di fuori dei casi sopra indicati, il documento informatico sprovvisto di firma elettronica ha l'efficacia probatoria della riproduzione meccanica;
   d) per "messaggio elettronico": un documento informatico sprovvisto di firma elettronica ed avente perciò, fatto salvo quanto previsto dalla precedente lettera c), l'efficacia probatoria della riproduzione meccanica;
   e) per "corrispondente":
   1) il soggetto privato che si sia identificato ai sensi dell'articolo 5, comma 1 ai fini della trasmissione e/o ricezione di documenti o atti amministrativi, mediante un servizio elettronico di recapito certificato qualificato, con gli effetti giuridici di cui all'articolo 6;
   2) gli organi e le Autorità dell'Amministrazione, le Unità Organizzative ed i Dipartimenti della Pubblica Amministrazione, le articolazioni organizzative degli Enti che si siano identificati ai sensi dell'articolo 5, comma 2 ai fini della trasmissione e ricezione di documenti o atti amministrativi, mediante un servizio elettronico di recapito certificato qualificato, con gli effetti giuridici di cui all'articolo 6.
2. Ai fini del presente decreto delegato si intendono, altresì, integralmente recepite le definizioni di cui al Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno
Modifiche legislative: DECRETO DELEGATO 26 luglio 2018 n.92, Art. 2
1. All'articolo 2, comma 1, lettera c) del Decreto Delegato n.46/2016 è soppressa la seguente espressione: "la medesima validità e rilevanza a tutti gli effetti di legge è riconosciuta, esclusivamente nel procedimento amministrativo in cui è acquisito, al documento informatico sprovvisto di firma elettronica ma trasmesso, mediante un servizio elettronico di recapito certificato qualificato, all'Amministrazione che abbia provveduto ad autenticarlo ai sensi dell'articolo 20, comma 2, lettera b) della Legge 5 ottobre 2011 n. 159.".
2. All'articolo 2, comma 1, del Decreto Delegato n.46/2016 è aggiunta la seguente lettera:
"e *bis)* per "domicilio digitale": l'indirizzo elettronico dichiarato dal soggetto interessato ed associato ai dati di identificazione delle persone fisiche e delle persone giuridiche.".
3. L'articolo 2, comma 2, del Decreto Delegato n.46/2016 è così modificato:
"2. Ai fini del presente decreto delegato, si intendono, altresì, integralmente recepite le definizioni di cui al Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, non in contrasto con quelle dettate nel presente e nei successivi articoli.".
4. L'espressione "comma 1 o comma 2" contenuta all'articolo 6, comma 1, lettere b) e c) del Decreto Delegato n.46/2016 è soppressa.
Modifiche legislative: Decreto Delegato 30 gennaio 2020 n.9, Art. 9 comma 8
8. L'articolo 22, comma 8, della Legge 31 ottobre 2018 n.137 e gli articoli 2, comma 1, lettera d) e 7, comma 2 del Decreto Delegato n.46/2016 sono abrogati. L'espressione "nonché dei documenti informatici nel loro formato originale" di cui all'articolo 7, comma 1 del Decreto Delegato n.46/2016 è soppressa.

1. L’utilizzo di servizi elettronici di recapito certificato qualificati per la trasmissione di documenti e atti amministrativi informatici in relazione alla quale l’Amministrazione debba acquisire la certezza dell’invio e della consegna al destinatario, avviene fra i seguenti soggetti, secondo i termini sotto specificati:

a) fra Pubblica Amministrazione ed Enti: obbligatoriamente;
b) fra Amministrazione e persone pubbliche o private che erogano un pubblico servizio: secondo modalità e termini definiti con appositi protocolli operativi, da redigersi previa acquisizione del parere vincolante della Commissione Tecnica per l’Innovazione Tecnologica;
c) fra Amministrazione e soggetti privati:
    1) obbligatoriamente, fra Amministrazione e soggetti operatori economici;
    2) volontariamente, fra Amministrazione e soggetti non operatori economici;
d) fra persone pubbliche o private che erogano un pubblico servizio e soggetti privati: secondo quanto previsto dai rispettivi regolamenti o norme interne, da redigersi previa acquisizione del parere vincolante della Commissione Tecnica per l’Innovazione Tecnologica.

CAPO II
DISPOSIZIONI RELATIVE ALLA TRASMISSIONE DI MESSAGGI ELETTRONICI MEDIANTE SERVIZI ELETTRONICI DI RECAPITO CERTIFICATO QUALIFICATI

Art. 4
(Requisiti relativi ai servizi elettronici di recapito certificato qualificati)

1. I servizi elettronici di recapito certificato qualificati utilizzabili ai fini del presente decreto delegato sono individuati dalla Commissione Tecnica per l’Innovazione Tecnologica mediante propria deliberazione.
2. I servizi elettronici di recapito certificato qualificati soddisfano i seguenti requisiti cumulativi:

a) sono forniti da uno o più prestatori di servizi fiduciari qualificati;
b) l’autenticità delle ricevute di invio e di consegna dei dati è garantita da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificati;
c) qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente ed al destinatario dei dati stessi;
d) la data e l’ora di invio e di consegna e qualsiasi modifica dei dati sono indicate da una validazione temporale elettronica qualificata;
e) sono tenuti a garantire l’integrità dei dati contenuti nel documento elettronico oggetto di trasmissione.

3. Qualora i messaggi elettronici siano trasferiti fra due o più prestatori di servizi fiduciari qualificati, i requisiti di cui al comma 2 devono sussistere in capo a tutti i predetti prestatori.

Art. 5
(Registro pubblico dei domicili digitali)

1. È istituito il Registro pubblico dei domicili digitali, brevemente denominato “Registro”. Il Registro può integrarsi con altri elenchi, anagrafi e registri già in uso presso l’Amministrazione.
2. Il Registro è tenuto dall’Unità Organizzativa (UO) Informatica, Tecnologia, Dati e Statistica. Il Registro può, tuttavia, su decisione del Congresso di Stato, essere concesso, in tutto o in parte, in gestione ad Enti a partecipazione maggioritaria o totalitaria pubblica, secondo i termini definiti nel provvedimento di concessione.
3. Ad un soggetto privato, persona fisica o giuridica, può corrispondere un solo domicilio digitale individuato con le modalità di cui al comma 4. I domicili digitali utilizzati dall’Amministrazione sono individuati con le modalità di cui al comma 5.
4. Il soggetto privato corrispondente di un messaggio scambiato tramite un servizio elettronico di recapito certificato, qualificato o non qualificato, si intende identificato quando sussistano le seguenti condizioni cumulative:

a) il suo domicilio digitale sia contenuto nel Registro;
b) abbia prestato, obbligatoriamente o volontariamente secondo quanto previsto dall’articolo 3, comma 1, lettera c), il proprio consenso in forma scritta a ricevere dall’Amministrazione documenti o atti amministrativi di proprio interesse mediante un servizio elettronico di recapito certificato, qualificato o non qualificato, nonché abbia, eventualmente e su base volontaria, dichiarato di avvalersi della modalità di trasmissione per via telematica di documenti informatici all’Amministrazione a mente dell’articolo 10 della Legge n. 159/2011 e dell’articolo 10 della Legge n. 160/2011;
c) il suo domicilio digitale, inserito nel Registro, sia associato ai dati di identificazione personale tramite una dichiarazione sostitutiva di atto di notorietà di cui all’articolo 13 della Legge n. 159/2011.

5. I domicili digitali della Pubblica Amministrazione, degli Enti e delle Aziende del Settore Pubblico Allargato e dei gestori di pubblici servizi sono pubblicati sui rispettivi portali e siti web. La trasmissione e ricezione di atti e documenti amministrativi informatici tramite un servizio elettronico di recapito certificato, qualificato o non qualificato,

avviene avvalendosi esclusivamente di tali domicili digitali.

6 È obbligo del pubblico dipendente, all'atto di ogni trasmissione e ricezione di atti e documenti amministrativi informatici mediante un servizio elettronico di recapito certificato, qualificato o non qualificato, eseguire l'autenticazione dei domicili digitali tramite la verifica della rispondenza fra il corrispondente del messaggio ed il domicilio digitale riportato nel Registro ovvero, qualora il corrispondente sia anch'esso soggetto dell'Amministrazione o di gestore di pubblico servizio, pubblicato sul portale o sito web.

7. Il Registro è reso accessibile all'Amministrazione al fine di consentire l'autenticazione dei domicili digitali dei corrispondenti. Tale accesso è consentito, per i medesimi fini, anche alle persone pubbliche o private che erogano un pubblico servizio secondo i termini definiti mediante i protocolli operativi di cui all'articolo 3, comma 1, lettera b). [11]

---

[11] **Testo originario**: **(D.D. n. 46/2016): Art. 5**

(Identificazione del corrispondente)

1. Il soggetto privato corrispondente di un documento elettronico scambiato tramite un servizio elettronico di recapito certificato qualificato si intende identificato quando sussistano le seguenti condizioni cumulative:
   a) abbia prestato, obbligatoriamente o volontariamente secondo quanto previsto dall'articolo 3, comma 1, lettera c), il proprio consenso in forma scritta a ricevere dall'Amministrazione documenti o atti amministrativi di proprio interesse mediante il predetto servizio elettronico di recapito nonché abbia, eventualmente e su base volontaria, dichiarato di avvalersi della modalità di trasmissione per via telematica di documenti informatici all'Amministrazione a mente dell'articolo 10 della Legge n. 159/2011 e dell'articolo 10 della Legge n. 160/2011;
   b) il suo indirizzo di posta elettronica è contenuto in apposito registro gestito dall'Unità Organizzativa Informatica, Tecnologia, Dati e Statistica, suddiviso in due sezioni di cui una relativa agli operatori economici, l'altra relativa ai non operatori economici;
   c) il suo indirizzo di posta elettronica è associato ai dati di identificazione personale tramite una dichiarazione sostitutiva di atto di notorietà di cui all'articolo 13 della Legge n. 159/2011.
2. Il soggetto pubblico dell'Amministrazione corrispondente di un messaggio elettronico scambiato con un servizio elettronico di recapito certificato qualificato è identificato tramite la pubblicazione su portale web degli indirizzi di posta elettronica dell'Amministrazione abilitati a trasmettere ed a ricevere atti e documenti amministrativi informatici tramite i predetti servizi elettronici.
3. E' obbligo del pubblico dipendente verificare, all'atto di ogni trasmissione e ricezione di documenti informatici mediante i servizi elettronici di recapito certificato qualificati, la rispondenza fra il corrispondente del messaggio elettronico e l'indirizzo di posta elettronica indicato nel registro ovvero, qualora il corrispondente sia anch'esso dipendente dell'Amministrazione, pubblicato sul portale web.
4. Il registro di cui al comma 1, lettera b) è reso accessibile all'interno dell'Amministrazione al fine di consentire di verificare la rispondenza dell'indirizzo di posta elettronica del soggetto privato corrispondente con quello contenuto nel registro. Tale accesso è consentito, per i medesimi fini, anche alle persone pubbliche o private che erogano un pubblico servizio secondo i termini definiti mediante i protocolli operativi di cui all'articolo 3, comma 1, lettera b).

Modifiche legislative: DECRETO DELEGATO 26 luglio 2018 n.92, Art. 3

1. L'articolo 5 del Decreto Delegato n.46/2016 è così sostituito:

"Art.5

(Registro pubblico dei domicili digitali)

1. È istituito il Registro pubblico dei domicili digitali, brevemente denominato "Registro". Il Registro può integrarsi con altri elenchi, anagrafi e registri già in uso presso l'Amministrazione.
2. Il Registro è tenuto dall'Unità Organizzativa (UO) Informatica, Tecnologia, Dati e Statistica. Il Registro può, tuttavia, su decisione del Congresso di Stato, essere concesso, in tutto o in parte, in gestione ad Enti a partecipazione maggioritaria o totalitaria pubblica, secondo i termini definiti nel provvedimento di concessione.
3. Ad un soggetto privato, persona fisica o giuridica, può corrispondere un solo domicilio digitale individuato con le modalità di cui al comma 4. I domicili digitali utilizzati dall'Amministrazione sono individuati con le modalità di cui al comma 5.
4. Il soggetto privato corrispondente di un messaggio scambiato tramite un servizio elettronico di recapito certificato, qualificato o non qualificato, si intende identificato quando sussistano le seguenti condizioni cumulative:

a) il suo domicilio digitale sia contenuto nel Registro;

b) abbia prestato, obbligatoriamente o volontariamente secondo quanto previsto dall'articolo 3, comma 1, lettera c), il proprio consenso in forma scritta a ricevere dall'Amministrazione documenti o atti amministrativi di proprio interesse mediante un servizio elettronico di recapito certificato, qualificato o non qualificato, nonché abbia, eventualmente e su base volontaria, dichiarato di avvalersi della modalità di trasmissione per via telematica di documenti informatici all'Amministrazione a mente dell'articolo 10 della Legge n. 159/2011 e dell'articolo 10 della Legge n. 160/2011;

c) il suo domicilio digitale, inserito nel Registro, sia associato ai dati di identificazione personale tramite una dichiarazione sostitutiva di atto di notorietà di cui all'articolo 13 della Legge n. 159/2011.

Art. 6

(Effetti giuridici relativi alla trasmissione di messaggi elettronici mediante un servizio elettronico di recapito certificato qualificato)

1. Le trasmissioni di documenti elettronici tramite un servizio elettronico di recapito certificato qualificato godono:
a) della presunzione di integrità dei dati in essi contenuti;
b) della certezza dell'invio da parte del mittente identificato a mente dell'articolo 5, [soppresso];
c) della certezza della loro consegna al destinatario identificato a mente dell'articolo 5, [soppresso]. [Soppresso].
2. La trasmissione di documento elettronico[12] tramite un servizio elettronico di recapito certificato qualificato equivale alla spedizione per mezzo di posta raccomandata con avviso di ricevimento in quanto costituisce forma di comunicazione tramite canale informatico sicuro in conformità all'articolo 10, comma 4 della Legge n. 159/2011.
3. Le ricevute di invio e consegna convalidate dal prestatore di servizi fiduciari qualificati sono valide e rilevanti a tutti gli effetti di legge e possono essere opposte a terzi in giudizio. [13]

---

5. I domicili digitali della Pubblica Amministrazione, degli Enti e delle Aziende del Settore Pubblico Allargato e dei gestori di pubblici servizi sono pubblicati sui rispettivi portali e siti web. La trasmissione e ricezione di atti e documenti amministrativi informatici tramite un servizio elettronico di recapito certificato, qualificato o non qualificato, avviene avvalendosi esclusivamente di tali domicili digitali.
6 È obbligo del pubblico dipendente, all'atto di ogni trasmissione e ricezione di atti e documenti amministrativi informatici mediante un servizio elettronico di recapito certificato, qualificato o non qualificato, eseguire l'autenticazione dei domicili digitali tramite la verifica della rispondenza fra il corrispondente del messaggio ed il domicilio digitale riportato nel Registro ovvero, qualora il corrispondente sia anch'esso soggetto dell'Amministrazione o di gestore di pubblico servizio, pubblicato sul portale o sito web.
7. Il Registro è reso accessibile all'Amministrazione al fine di consentire l'autenticazione dei domicili digitali dei corrispondenti. Tale accesso è consentito, per i medesimi fini, anche alle persone pubbliche o private che erogano un pubblico servizio secondo i termini definiti mediante i protocolli operativi di cui all'articolo 3, comma 1, lettera b).".

[12] **DECRETO DELEGATO 30 gennaio 2020 n.9, Art. 9 comma 2**

2. L'espressione "messaggio" di cui all'articolo 5 del Decreto Delegato n.46/2016 e successive modifiche, l'espressione "messaggio elettronico" di cui all'articolo 6 e l'espressione "messaggi elettronici" di cui all'articolo 7, comma 1 del medesimo decreto delegato e successive modifiche è sostituita con "documento elettronico".

[13] **Testo originario DECRETO DELEGATO 11 aprile 2016 n.46,**

Art. 6 *(Effetti giuridici relativi alla trasmissione di messaggi elettronici mediante un servizio elettronico di recapito certificato qualificato)*

I messaggi elettronici trasmessi mediante un servizio elettronico di recapito certificato qualificato godono:
a) della presunzione di integrità dei dati in essi contenuti;
b) della certezza dell'invio da parte del mittente identificato a mente dell'articolo 5, comma 1 o comma 2;
c) della certezza della loro consegna al destinatario identificato a mente dell'articolo 5, comma 1 o comma 2. Tale presunzione sussiste indipendentemente dal fatto che il soggetto privato destinatario riceva il messaggio elettronico su casella di posta sulla quale sia attivo o meno un servizio di recapito certificato qualificato.
2. La trasmissione di messaggi elettronici tramite un servizio elettronico di recapito certificato qualificato equivale alla spedizione per mezzo di posta raccomandata con avviso di ricevimento in quanto costituisce forma di comunicazione tramite canale informatico sicuro in conformità all'articolo 10, comma 4 della Legge n. 159/2011.
3. Le ricevute di invio e consegna convalidate dal prestatore di servizi fiduciari qualificati sono valide e rilevanti a tutti gli effetti di legge e possono essere opposte a terzi in giudizio.

Modifiche legislative: DECRETO DELEGATO 26 luglio 2018 n.92, Art. 2

-omissis-

4. L'espressione "comma 1 o comma 2" contenuta all'articolo 6, comma 1, lettere b) e c) del Decreto Delegato n.46/2016 è soppressa.

DECRETO DELEGATO 30 gennaio 2020 n.9, Art. 9 Comma 3

3. L'alinea dell'articolo 6, comma 1 del Decreto Delegato n.46/2016 è così modificato: "Le trasmissioni di documenti elettronici tramite un servizio elettronico di recapito certificato qualificato godono:".

DECRETO DELEGATO 30 gennaio 2020 n.9, Art. 9 comma 4

4. All'articolo 6, comma 1, lettera c) del Decreto Delegato n.46/2016 è soppresso il seguente periodo: "Tale presunzione sussiste indipendentemente dal fatto che il soggetto privato destinatario riceva il messaggio elettronico su casella di posta sulla quale sia attivo o meno un servizio di recapito certificato qualificato."

Art. 7
(Archiviazione e conservazione)

1. L'archiviazione e conservazione di documento elettronico e relative ricevute [soppressa] avviene in conformità alla Legge 11 maggio 2012 n. 50 e, in particolare, all'articolo 14 della stessa.
2. [abrogato]. [14]

CAPO III
DISPOSIZIONI TRANSITORIE SULL'UTILIZZO DI SERVIZI ELETTRONICI DI RECAPITO CERTIFICATO [15]

---

[14] **Testo originario DECRETO DELEGATO 11 aprile 2016 n.46, Art. 7** *(Archiviazione e conservazione)*
1. L'archiviazione e conservazione di messaggi elettronici e relative ricevute nonché dei documenti informatici nel loro formato originale avviene in conformità alla Legge 11 maggio 2012 n. 50 e, in particolare, all'articolo 14 della stessa.
2. L'Amministrazione può verificare in qualunque momento l'integrità dei messaggi elettronici ricevuti utilizzando gli strumenti di verifica messi a disposizione dal prestatore di servizi fiduciari qualificati.
Modifiche legislative:
DECRETO DELEGATO 30 gennaio 2020 n.9, Art. 9 comma 2
2. L'espressione "messaggio" di cui all'articolo 5 del Decreto Delegato n.46/2016 e successive modifiche, l'espressione "messaggio elettronico" di cui all'articolo 6 e l'espressione "messaggi elettronici" di cui all'articolo 7, comma 1 del medesimo decreto delegato e successive modifiche è sostituita con "documento elettronico".
DECRETO DELEGATO 30 gennaio 2020 n.9, Art. 9 comma 8
8. L'articolo 22, comma 8, della Legge 31 ottobre 2018 n.137 e gli articoli 2, comma 1, lettera d) e 7, comma 2 del Decreto Delegato n.46/2016 sono abrogati. L'espressione "nonché dei documenti informatici nel loro formato originale" di cui all'articolo 7, comma 1 del Decreto Delegato n.46/2016 è soppressa.

[15] **Testo originario**: **Testo originario DECRETO DELEGATO 11 aprile 2016 n.46,**
CAPO III
DISPOSIZIONE ATTUATIVA
Art. 8
(Disposizione attuativa)
1. Tenuto conto dell'esigenza di ultimare la fase di individuazione dell'uno o più prestatori di servizi fiduciari qualificati cui l'Amministrazione affiderà il servizio elettronico di recapito certificato qualificato nonché dei necessari adeguamenti organizzativi, l'efficacia delle norme di cui all'articolo 3 è subordinata all'adozione di direttive della Commissione Tecnica per l'Innovazione Tecnologica con le quali saranno definiti i termini di decorrenza delle predette disposizioni.
2. Il Congresso di Stato, su eventuale proposta della Commissione Tecnica per l'Innovazione Tecnologica, adotta il regolamento di attuazione del presente decreto delegato.
Modifiche legislative: DECRETO DELEGATO 26 luglio 2018 n.92, Art. 4
1. Il Capo III del Decreto Delegato n.46/2016 è così modificato:
"Capo III
DISPOSIZIONI TRANSITORIE SULL'UTILIZZO DI SERVIZI ELETTRONICI DI RECAPITO CERTIFICATO
Art. 8
(Ambito e modalità di applicazione)
1. Le disposizioni del presente Capo regolano l'utilizzo di servizi elettronici di recapito certificato, nelle more della piena applicabilità delle norme di cui al Capo II la cui attuazione è subordinata alla preventiva adozione, da parte delle competenti autorità dell'Unione Europea, di atti esecutivi del Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014.
2. L'ambito e le modalità di applicazione delle norme di cui al presente Capo sono i medesimi di quelli previsti dall'articolo 3.
Art. 8-*bis*
(Requisiti relativi ai servizi elettronici di recapito certificato)
1. Un servizio elettronico di recapito certificato consente la trasmissione di dati fra soggetti per via elettronica e fornisce prove relative al trattamento dei dati trasmessi proteggendoli dal rischio di perdita, furto, danni o modifiche non autorizzate.
2. I servizi elettronici di recapito certificato soddisfano i seguenti requisiti:
a) garantiscono, con un elevato livello di sicurezza, l'identificazione del mittente;

Art. 8
(Ambito e modalità di applicazione)

1. Le disposizioni del presente Capo regolano l'utilizzo di servizi elettronici di recapito certificato, nelle more della piena applicabilità delle norme di cui al Capo II la cui attuazione è subordinata alla preventiva adozione, da parte delle competenti autorità dell'Unione Europea, di atti esecutivi del Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014.
2. L'ambito e le modalità di applicazione delle norme di cui al presente Capo sono i medesimi di quelli previsti dall'articolo 3.

Art. 8-*bis*
(Requisiti relativi ai servizi elettronici di recapito certificato)

1. Un servizio elettronico di recapito certificato consente la trasmissione di dati fra soggetti per via elettronica e fornisce prove relative al trattamento dei dati trasmessi proteggendoli dal rischio di perdita, furto, danni o modifiche non autorizzate.
2. I servizi elettronici di recapito certificato soddisfano i seguenti requisiti:
   a) garantiscono, con un elevato livello di sicurezza, l'identificazione del mittente;
   b) garantiscono l'identificazione del destinatario prima della consegna dei dati;
   c) l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato per la firma digitale, in modo da escludere la possibilità di modifiche non rilevabili dei dati;
   d) qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente e al destinatario dei dati stessi;
   e) la data e l'ora di invio e di ricezione e qualsiasi modifica dei dati sono indicate da una validazione temporale elettronica qualificata.
3. I servizi elettronici di recapito certificato utilizzabili ai fini del presente decreto delegato sono individuati dalla Commissione Tecnica per l'Innovazione Tecnologica mediante propria deliberazione, su parere conforme dell'Agenzia dello Sviluppo Digitale di cui al Decreto Delegato 9 dicembre 2015 n. 179.

---

b) garantiscono l'identificazione del destinatario prima della consegna dei dati;
c) l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato per la firma digitale, in modo da escludere la possibilità di modifiche non rilevabili dei dati;
d) qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente e al destinatario dei dati stessi;
e) la data e l'ora di invio e di ricezione e qualsiasi modifica dei dati sono indicate da una validazione temporale elettronica qualificata.
3. I servizi elettronici di recapito certificato utilizzabili ai fini del presente decreto delegato sono individuati dalla Commissione Tecnica per l'Innovazione Tecnologica mediante propria deliberazione, su parere conforme dell'Agenzia dello Sviluppo Digitale di cui al Decreto Delegato 9 dicembre 2015 n. 179.
Art. 8-*ter*
(Effetti giuridici relativi alla trasmissione di messaggi elettronici mediante un servizio elettronico di recapito certificato)
1. I dati trasmessi mediante un servizio elettronico di recapito certificato godono del medesimo valore giuridico e probatorio stabilito per i servizi elettronici di recapito certificato qualificato dall'articolo 6, commi 2 e 3; i predetti dati sono assistititi dalla certezza dell'invio e della consegna, secondo i medesimi termini di cui all'articolo 6, comma 1, lettere b) e c). I dati trasmessi mediante servizio elettronico di recapito certificato non godono, tuttavia, della presunzione di integrità di cui all'articolo 6, comma 1, lettera a), pur non essendo agli stessi negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della loro forma elettronica o perché non soddisfano i requisiti del servizio elettronico di recapito certificato qualificato.
2. I dati inviati mediante un servizio elettronico di recapito certificato si intendono spediti dal mittente se inviati al prestatore del servizio elettronico di recapito certificato e si intendono consegnati se resi disponibili al domicilio digitale del destinatario, salva la prova che la mancata consegna sia dovuta a fatto non imputabile al destinatario medesimo.
Art. 8-*quater*
(Archiviazione e conservazione dei messaggi elettronici trasmessi mediante un servizio elettronico di recapito certificato)
1. All'archiviazione e conservazione dei dati trasmessi mediante un servizio elettronico di recapito certificato si applicano le medesime disposizioni di cui all'articolo 7.".

Art. 8-*ter*

(Effetti giuridici relativi alla trasmissione di messaggi elettronici mediante un servizio elettronico di recapito certificato)

1. Le trasmissioni di documenti elettronici mediante un servizio elettronico di recapito certificato godono del medesimo valore giuridico e probatorio stabilito dall'articolo 6, commi 2 e 3 in relazione alle trasmissioni effettuate tramite i servizi elettronici di recapito certificato qualificato.
Le predette trasmissioni sono, pertanto, assistite dalla certezza dell'invio e della consegna, secondo i medesimi termini di cui all'articolo 6, comma 1, lettere b) e c). Le trasmissioni effettuate con servizio elettronico di recapito certificato non godono, tuttavia, della presunzione di integrità dei dati in esse contenuti prevista dall'articolo 6, comma 1, lettera a).
2. I dati inviati mediante un servizio elettronico di recapito certificato si intendono spediti dal mittente se inviati al prestatore del servizio elettronico di recapito certificato e si intendono consegnati se resi disponibili al domicilio digitale del destinatario, salva la prova che la mancata consegna sia dovuta a fatto non imputabile al destinatario medesimo. [16]

Art. 8-*quater*

(Archiviazione e conservazione dei messaggi elettronici trasmessi mediante un servizio elettronico di recapito certificato)

1. All'archiviazione e conservazione dei dati trasmessi mediante un servizio elettronico di recapito certificato si applicano le medesime disposizioni di cui all'articolo 7.

Capo III – *bis* [17]
DISPOSIZIONI ATTUATIVE

Art. 8-*quinquies*

---

[16] **Modifiche legislative DECRETO DELEGATO 30 gennaio 2020 n.9, art.9 comma 5**
5. L'articolo 8-*ter*, comma 1 del Decreto Delegato n.46/2016 e successive modifiche è così ulteriormente modificato:
"1. Le trasmissioni di documenti elettronici mediante un servizio elettronico di recapito certificato godono del medesimo valore giuridico e probatorio stabilito dall'articolo 6, commi 2 e 3 in relazione alle trasmissioni effettuate tramite i servizi elettronici di recapito certificato qualificato.
Le predette trasmissioni sono, pertanto, assistite dalla certezza dell'invio e della consegna, secondo i medesimi termini di cui all'articolo 6, comma 1, lettere b) e c). Le trasmissioni effettuate con servizio elettronico di recapito certificato non godono, tuttavia, della presunzione di integrità dei dati in esse contenuti prevista dall'articolo 6, comma 1, lettera a).".

[17] **Testo originario DECRETO DELEGATO 26 luglio 2018 n.92, Art. 5**
Art. 5
1. Al Decreto Delegato n.46/2016 è aggiunto il seguente Capo:
"Capo III - *bis*
DISPOSIZIONI ATTUATIVE
Art. 8-*quinquies*
1. Tenuto conto dell'esigenza di ultimare la fase di individuazione dell'uno o più prestatori di servizi fiduciari cui l'Amministrazione affiderà il servizio elettronico di recapito certificato, qualificato o non qualificato, nonché dei necessari adeguamenti organizzativi, l'efficacia delle norme di cui al presente decreto delegato è subordinata all'adozione di direttive della Commissione
Tecnica per l'Innovazione Tecnologica con le quali saranno definiti i termini di decorrenza delle predette disposizioni.
2. L'individuazione dei prestatori di servizi fiduciari di cui al comma 1 avviene, in via prioritaria, attraverso le modalità di cui all'articolo 17, comma 5, lettera e) del Decreto Delegato 2 marzo 2015 n.26 e prevedendo la costituzione di associazione temporanea di impresa. In ragione del perseguimento di obiettivi di economicità, uniformità e sicurezza nella gestione dei dati, l'Amministrazione ha facoltà di mettere a disposizione del prestatore del servizio elettronico di recapito certificato, qualificato o non qualificato, individuato a mente del comma 1 e di quanto previsto al precedente periodo, il proprio centro elaborazione dati, secondo termini e modalità definiti negli atti e contratti disciplinanti l'erogazione del servizio.
3. Il Congresso di Stato, su proposta della Commissione Tecnica per l'Innovazione Tecnologica, adotta regolamenti di attuazione del presente decreto delegato, con particolare riferimento alla tenuta del Registro.
4. Le modalità di archiviazione e conservazione dei messaggi trasmessi mediante un servizio elettronico di recapito certificato, qualificato o non qualificato, sono disciplinate nei Piani di Gestione Documentaria della Pubblica Amministrazione e degli Enti e delle Aziende del Settore Pubblico Allargato di cui all'articolo 7 del Decreto Delegato 8 luglio 2013 n.81.".

1. Tenuto conto dell'esigenza di ultimare la fase di individuazione dell'uno o più prestatori di servizi fiduciari cui l'Amministrazione affiderà il servizio elettronico di recapito certificato, qualificato o non qualificato, nonché dei necessari adeguamenti organizzativi, l'efficacia delle norme di cui al presente decreto delegato è subordinata all'adozione di direttive della Commissione Tecnica per l'Innovazione Tecnologica con le quali saranno definiti i termini di decorrenza delle predette disposizioni.
2. L'individuazione dei prestatori di servizi fiduciari di cui al comma 1 avviene, in via prioritaria, attraverso le modalità di cui all'articolo 17, comma 5, lettera e) del Decreto Delegato 2 marzo 2015 n.26 e prevedendo la costituzione di associazione temporanea di impresa. In ragione del perseguimento di obiettivi di economicità, uniformità e sicurezza nella gestione dei dati, l'Amministrazione ha facoltà di mettere a disposizione del prestatore del servizio elettronico di recapito certificato, qualificato o non qualificato, individuato a mente del comma 1 e di quanto previsto al precedente periodo, il proprio centro elaborazione dati, secondo termini e modalità definiti negli atti e contratti disciplinanti l'erogazione del servizio.
3. Il Congresso di Stato, su proposta della Commissione Tecnica per l'Innovazione Tecnologica, adotta regolamenti di attuazione del presente decreto delegato, con particolare riferimento alla tenuta del Registro.
4. Le modalità di archiviazione e conservazione dei messaggi trasmessi mediante un servizio elettronico di recapito certificato, qualificato o non qualificato, sono disciplinate nei Piani di Gestione Documentaria della Pubblica Amministrazione e degli Enti e delle Aziende del Settore Pubblico Allargato di cui all'articolo 7 del Decreto Delegato 8 luglio 2013 n.81.

DECRETO DELEGATO 30 gennaio 2020 n.9 - MODIFICHE AL DECRETO 8 NOVEMBRE 2005 N.156 E DISPOSIZIONI SULL'UTILIZZO DI SERVIZI ELETTRONICI DI RECAPITO CERTIFICATO E DI POSTA ELETTRONICA CERTIFICATA

CAPO I
NORME GENERALI

Art. 1
(Finalità)

1. Il presente decreto delegato integra le disposizioni del Decreto 8 novembre 2005 n. 156 in attuazione della Legge 20 luglio 2005 n. 115 relativamente alle regole tecniche per la formazione, la trasmissione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti elettronici.
2. Il presente decreto disciplina, altresì, nell'esercizio della delega di cui all'articolo 18, comma 2, lettere b) e c) della Legge 30 maggio 2019 n.88:
a) l'estensione degli effetti giuridici di cui all'articolo 8ter del Decreto Delegato 11 aprile 2016 n.46 e successive modifiche alle trasmissioni di documenti elettronici effettuate, mediante servizio elettronico di recapito certificato, fra i soggetti privati, persona fisica o giuridica, sammarinesi o residenti;
b) gli effetti giuridici nell'ordinamento sammarinese delle trasmissioni di documenti elettronici effettuate mediante la posta elettronica certificata (PEC) disciplinata dall'ordinamento della Repubblica Italiana.

Art. 2
(Recepimento di norme)

1. Sono recepite integralmente nell'ordinamento sammarinese le definizioni contenute all'articolo 3 del Regolamento (UE) n.910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (Regolamento eIDAS).
2. Le definizioni di cui al comma 1 prevalgono, in caso di contrasto, sulle definizioni stabilite dalle norme interne e, in particolare, dall'articolo 1 della Legge n. 115/2005.
3. L'espressione "documento elettronico" di cui ai successivi articoli è utilizzata in luogo di quella di "documento informatico" di cui agli articoli 1, comma primo, lettera b) e 2, comma primo della Legge n.115/2005 nonché all'articolo 77, comma primo, lettera d) del Decreto n.156/2005.

CAPO II
MODIFICHE AL DECRETO 8 NOVEMBRE 2005 N.156
-omissis-

CAPO III
DISPOSIZIONI RELATIVE AI SERVIZI ELETTRONICI DI RECAPITO CERTIFICATO

Art. 5 [abrogato][18]

[18] **Testo originario (Decreto Delegato 30 gennaio 2020 n.9)**
Art.5
(Estensione dell'ambito di applicazione dei servizi elettronici di recapito certificato)
1. La trasmissione di documenti elettronici effettuata tramite servizi elettronici di recapito certificato di cui al Decreto Delegato n.46/2016 e successive modifiche produce gli effetti giuridici e probatori di cui all'articolo 8ter del

(Estensione dell'ambito di applicazione dei servizi elettronici di recapito certificato)

1. La trasmissione di documenti elettronici effettuata tramite servizi elettronici di recapito certificato di cui al Decreto Delegato n.46/2016 e successive modifiche produce gli effetti giuridici e probatori di cui all'articolo 8ter del predetto decreto delegato anche qualora intercorra esclusivamente fra soggetti privati, persone fisiche o giuridiche, sammarinesi o residenti.
2. I soggetti privati che intendano utilizzare, anche ai fini di cui al comma 1, i servizi elettronici di recapito certificato di cui al Decreto Delegato n. 46/2016 e successive modifiche eleggono domicilio digitale ai sensi dell'articolo 5 del medesimo decreto delegato e dell'articolo 22 della Legge n. 137/2018 e successive modifiche.

Art. 6 [abrogato][19]

CAPO IV
DISPOSIZIONI TRANSITORIE RELATIVE ALL'UTILIZZO DELLA PEC

Art. 7 [abrogato] [20]

---

predetto decreto delegato anche qualora intercorra esclusivamente fra soggetti privati, persone fisiche o giuridiche, sammarinesi o residenti.
2. I soggetti privati che intendano utilizzare, anche ai fini di cui al comma 1, i servizi elettronici di recapito certificato di cui al Decreto Delegato n. 46/2016 e successive modifiche eleggono domicilio digitale ai sensi dell'articolo 5 del medesimo decreto delegato e dell'articolo 22 della Legge n. 137/2018 e successive modifiche.
Modifiche legislative:
DECRETO DELEGATO 21 marzo 2023 n.51, Art.26 comma 8
8. Sono abrogati:
-omissis-
d) gli articoli 5, 6, 7, 8 e 9 del Decreto Delegato 30 gennaio 2020 n.9;
-omissis-

[19] **Testo originario (Decreto Delegato 30 gennaio 2020 n.9)**
Art. 6
(Disposizioni integrative in merito ai servizi elettronici di recapito certificato)
1. L'accesso a domicilio digitale iscritto nel Registro Pubblico dei domicili digitali può avvenire anche mediante l'utilizzo di accessi secondari autorizzati dal titolare del domicilio.
2. In deroga a quanto previsto dall'articolo 5, comma 3, primo periodo del Decreto Delegato n. 46/2016 come sostituito dall'articolo 3 del Decreto Delegato n. 92/2018, il libero professionista nominato dal Tribunale quale liquidatore o curatore può eleggere, previa richiesta inoltrata al gestore del Registro Pubblico dei domicili digitali, un unico domicilio digitale cui siano associate anche le persone fisiche e giuridiche in relazione alle quali la predetta nomina sia stata effettuata.
Modifiche legislative:
DECRETO DELEGATO 21 marzo 2023 n.51, Art.26 comma 8
8. Sono abrogati:
-omissis-
d) gli articoli 5, 6, 7, 8 e 9 del Decreto Delegato 30 gennaio 2020 n.9;
-omissis-

[20] **Testo originario (Decreto Delegato 30 gennaio 2020 n.9)**
Art. 7
(Utilizzo della posta elettronica certificata)
1. La trasmissione di documenti elettronici effettuata tramite posta elettronica certificata (PEC) di cui al Decreto del Presidente della Repubblica Italiana 11 febbraio 2005, n.68 e successive modifiche produce nell'ordinamento sammarinese gli effetti giuridici e probatori di cui all'articolo 8-*ter* del Decreto Delegato n.46/2016 e successive modifiche esclusivamente nei seguenti casi:

CAPO V
NORME FINALI

Art. 8 [abrogato] [21]

a) la trasmissione sia effettuata esclusivamente fra soggetti privati, ambedue dotati di PEC, di cui uno dei corrispondenti sammarinese o residente nella Repubblica di San Marino e l'altro residente o avente sede nel territorio della Repubblica Italiana;
b) la trasmissione sia effettuata fra uffici e organi dell'Amministrazione sammarinese e uffici e organi delle Amministrazioni ed Enti Pubblici della Repubblica Italiana, ambedue dotati di PEC;

b *bis*) la trasmissione sia effettuata fra uffici e organi dell'Amministrazione sammarinese ed operatore economico avente sede nel territorio della Repubblica Italiana, ambedue dotati di PEC.

2. La disposizione di cui al comma 1 si applica anche con riferimento alle trasmissioni di documenti elettronici in cui il soggetto residente o avente sede nel territorio della Repubblica Italiana utilizzi il servizio PEC ed il soggetto pubblico o privato sammarinese o residente nella Repubblica di San Marino utilizzi un servizio elettronico di recapito certificato di cui al Decreto Delegato n. 46/2016 e successive modifiche quando tale trasmissione avvenga attraverso l'uso di un nodo di scambio che realizzi un'interoperabilità tecnica fra i due diversi servizi. Il livello di adeguatezza dell'interoperabilità tecnica realizzata dal predetto nodo dovrà essere preventivamente valutato e riconosciuto dall'Istituto per l'Innovazione della Repubblica di San Marino S.p.A.

3. Le disposizioni di cui al presente articolo hanno valore transitorio sino al conseguimento della qualificazione, ai sensi dell'articolo 44 del Regolamento eIDAS da parte:
   a) del servizio elettronico di recapito certificato di cui al Decreto Delegato n.46/2016 e successive modifiche, oppure;
   b) del servizio di posta elettronica certificata in uso nella Repubblica Italiana.

Modifiche legislative:
DECRETO DELEGATO 21 marzo 2023 n.51, Art.26 comma 8
8. Sono abrogati:
-omissis-
d) gli articoli 5, 6, 7, 8 e 9 del Decreto Delegato 30 gennaio 2020 n.9;
-omissis-

[21] **Testo originario (Decreto Delegato 30 gennaio 2020 n.9)**
Art. 8
(Comunicazioni fra Amministrazione e propri dipendenti e fra Amministrazione ed iscritti o aspiranti alle graduatorie per l'insegnamento)
1. Gli iscritti ed aspiranti alle graduatorie per l'insegnamento di cui alla Legge 17 luglio 1979 n.41 e successive modifiche ed i pubblici dipendenti hanno l'obbligo di eleggere un proprio domicilio digitale.
2. L'Amministrazione comunica con i soggetti di cui al comma 1 a mezzo di servizio di posta elettronica ordinaria inviata al domicilio digitale, oppure, nei casi in cui sia necessario disporre di una ricevuta di invio e di una ricevuta di consegna, a mezzo di servizio elettronico di recapito certificato di cui al Decreto Delegato n.46/2016 e successive modifiche, nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.
3. L'obbligo di elezione del domicilio digitale di cui al comma 1 è assolto con le modalità di cui all'articolo 5 del Decreto Delegato n.46/2016 e successive modifiche ovvero con modalità semplificate stabilite dalla DGFP, ferma restando, in quest'ultimo caso, la necessità di garantire, in caso di utilizzo di servizi elettronici di recapito certificato, l'identificazione del corrispondente con un elevato livello di sicurezza tramite il suo riconoscimento de visu da parte di pubblico ufficiale oppure da altro pubblico impiegato autorizzato oppure tramite sottoscrizione di apposita istanza con firma elettronica qualificata.
4. L'obbligo di cui al comma 3 decorre dalle scadenze stabilite dalla DGFP la quale ha, altresì, la facoltà di concedere motivate deroghe al medesimo obbligo.
5. I soggetti di cui al comma 1 non sostengono nessun onere economico per l'assolvimento dell'obbligo previsto al predetto comma.

Modifiche legislative:
DECRETO DELEGATO 21 marzo 2023 n.51, Art.26 comma 8
8. Sono abrogati:
-omissis-

Art. 9 [abrogato] [22]

d) gli articoli 5, 6, 7, 8 e 9 del Decreto Delegato 30 gennaio 2020 n.9;
-omissis-

[22] **Testo originario (Decreto Delegato 30 gennaio 2020 n.9)**
Art. 9
(Norme di raccordo e abrogazioni)
1. All'articolo 9, comma 1 del Decreto Delegato 8 luglio 2013 n.81 sono soppresse le parole "in particolare MoReq2".
2. L'espressione "messaggio" di cui all'articolo 5 del Decreto Delegato n.46/2016 e successive modifiche, l'espressione "messaggio elettronico" di cui all'articolo 6 e l'espressione "messaggi elettronici" di cui all'articolo 7, comma 1 del medesimo decreto delegato e successive modifiche è sostituita con "documento elettronico".
3. L'alinea dell'articolo 6, comma 1 del Decreto Delegato n.46/2016 è così modificato: "Le trasmissioni di documenti elettronici tramite un servizio elettronico di recapito certificato qualificato godono:".
4. All'articolo 6, comma 1, lettera c) del Decreto Delegato n.46/2016 è soppresso il seguente periodo: "Tale presunzione sussiste indipendentemente dal fatto che il soggetto privato destinatario riceva il messaggio elettronico su casella di posta sulla quale sia attivo o meno un servizio di recapito certificato qualificato."
5. L'articolo 8-*ter*, comma 1 del Decreto Delegato n.46/2016 e successive modifiche è così ulteriormente modificato:
"1. Le trasmissioni di documenti elettronici mediante un servizio elettronico di recapito certificato godono del medesimo valore giuridico e probatorio stabilito dall'articolo 6, commi 2 e 3 in relazione alle trasmissioni effettuate tramite i servizi elettronici di recapito certificato qualificato.
Le predette trasmissioni sono, pertanto, assistite dalla certezza dell'invio e della consegna, secondo i medesimi termini di cui all'articolo 6, comma 1, lettere b) e c). Le trasmissioni effettuate con servizio elettronico di recapito certificato non godono, tuttavia, della presunzione di integrità dei dati in esse contenuti prevista dall'articolo 6, comma 1, lettera a).".
6. I documenti elettronici formati, acquisiti e gestiti da software in uso nell'Amministrazione che non prevedano l'utilizzo della firma elettronica qualificata bensì di firma elettronica semplice o avanzata, hanno il valore giuridico e probatorio di cui all'articolo 3, comma 4 della Legge n.115/2005 e, pertanto, sono liberamente valutabili in giudizio in relazione alle loro caratteristiche di sicurezza, integrità e immodificabilità.
7. La competenza di cui agli articoli 4, comma 1 e 8 *bis*, comma 3 del Decreto Delegato n.46/2016 e successive modifiche relativa all'individuazione dei servizi elettronici di recapito certificato, qualificato e non, utilizzabili ai fini del medesimo Decreto Delegato n.46/2016 e successive modifiche nonché dei superiori commi è trasferita, in linea con quanto previsto dall'articolo 7 del Decreto Delegato 11 dicembre 2018 n.155, all'Istituto per l'Innovazione della Repubblica di San Marino S.p.A.
7 *bis*. La disposizione di cui all'articolo 11, comma 2 della Legge 5 ottobre 2011 n.159 relativa all'obbligo di spedizione delle istanze e delle dichiarazioni unitamente alla copia fotostatica non autenticata di un documento di identità dell'interessato da questi sottoscritta e dichiarata come conforme all'originale, contenente la dichiarazione di cui al comma 2 dell'articolo 9 della medesima legge, non si applica alla trasmissione all'Amministrazione di documenti elettronici per via telematica tramite servizio elettronico di recapito certificato. Il valore giuridico e probatorio delle istanze e dichiarazioni prodotte nella forma del documento elettronico resta disciplinato, a seconda del tipo di firma elettronica apposta, dall'articolo 3 della Legge n.115/2005 come precisato dal superiore comma 6.
8 L'articolo 22, comma 8, della Legge 31 ottobre 2018 n.137 e gli articoli 2, comma 1, lettera d) e 7, comma 2 del Decreto Delegato n.46/2016 sono abrogati. L'espressione "nonché dei documenti informatici nel loro formato originale" di cui all'articolo 7, comma 1 del Decreto Delegato n.46/2016 è soppressa.
Modifiche legislative:
DECRETO DELEGATO 21 marzo 2023 n.51, Art.26 comma 8
8. Sono abrogati:
-omissis-
d) gli articoli 5, 6, 7, 8 e 9 del Decreto Delegato 30 gennaio 2020 n.9;
-omissis-

Allegato al Decreto Delegato 30 gennaio 2020 n.9

ALLEGATO 1

Sommario

1 Introduzione

Il presente documento fornisce indicazioni iniziali sui formati dei documenti elettronici che per le loro caratteristiche sono, al momento attuale, da ritenersi coerenti con le regole tecniche del documento informatico, del sistema di

conservazione e del protocollo informatico. I formati descritti sono stati scelti tra quelli che possono maggiormente garantire i principi dell'interoperabilità tra i sistemi di conservazione e in base alla normativa vigente riguardante specifiche tipologie documentali.

2 I formati

La leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato.

Il formato di un file è la convenzione usata per interpretare, leggere e modificare il file.

2.1 Identificazione

L'associazione del documento informatico al suo formato può avvenire, attraverso varie modalità, tra cui le più impiegate sono:

1. l'estensione: una serie di lettere, unita al nome del file attraverso un punto, ad esempio [nome del file].docx identifica un formato testo di proprietà della Microsoft;
2. I metadati espliciti: l'indicazione "application/msword" inserita nei tipi MIME che indica un file testo realizzato con l'applicazione Word della Microsoft;
3. il *magic number:* i primi byte presenti nella sequenza binaria del file, ad esempio 0xffd8 dentifica i file immagine di tipo .jpeg.

2.2 Le tipologie di formato

L'evolversi delle tecnologie e la crescente disponibilità e complessità dell'informazione digitale ha indotto la necessità di gestire sempre maggiori forme di informazione digitale (testo, immagini, filmati, ecc.) e di disporre di funzionalità più specializzate per renderne più facile la creazione, la modifica e la manipolazione.

Questo fenomeno porta all'aumento del numero dei formati disponibili e dei corrispondenti programmi necessari a gestirli nonché delle piattaforme su cui questi operano.

In particolare, volendo fare una prima sommaria, e non esaustiva, catalogazione dei più diffusi formati, secondo il loro specifico utilizzo possiamo elencare:

- Testi/documenti (DOC, HTML, PDF,...)
- Calcolo (XLS, ...)
- Immagini (GIF, JPG, BMP, TIF, EPS, SVG, ...)
- Suoni (MP3, WAV, ...)
- Video (MPG, MPEG, AVI, WMV,...)
- Eseguibili (EXE, ...)
- Archiviazione e Compressione (ZIP, RAR, ...)
- Formati email (SMTP/MIME, ...)

2.3 Formati Immagini

Per la rappresentazione delle immagini sono disponibili diversi formati, che possono essere distinti secondo la grafica utilizzata: raster o vettoriale.

2.3.1 Raster

Nel caso della grafica raster, l'immagine digitale è formata da un insieme di piccole aree uguali (pixel), ordinate secondo linee e colonne. I formati più diffusi sono il .tif (usato dai fax), il .jpg, il .bmp.

2.3.2 Vettoriale

La grafica vettoriale è una tecnica utilizzata per descrivere un'immagine mediante un insieme di primitive geometriche che definiscono punti, linee, curve e poligoni ai quali possono essere attribuiti colori e anche sfumature.

I documenti realizzati attraverso la grafica vettoriale sono quelli utilizzati nella stesura degli elaborati tecnici, ad esempio progetti di edifici.

Attualmente i formati maggiormente in uso sono:

- DWG, un formato proprietario per i file di tipo CAD, di cui non sono state rilasciate le specifiche;
- DXF, un formato simile al DWG, di cui sono state rilasciate le specifiche tecniche;
- Shapefile un formato vettoriale proprietario per sistemi informativi geografici (GIS) con la caratteristica di essere interoperabile con i prodotti che usano i precedenti formati;
- SVG, un formato aperto, basato su XML, in grado di visualizzare oggetti di grafica vettoriale, non legato ad uno specifico prodotto.

2.4 Altri Formati

Per determinate tipologie di documenti elettronici sono utilizzati specifici formati. In particolare in campo sanitario i formati più usati sono:

- DICOM (immagini che arrivano da strumenti diagnostici) anche se il DICOM non è solo un formato, ma definisce anche protocolli e altro;
- HL7 ed in particolare il CDA2 (Clinical Document Architecture) che contiene la sua stessa descrizione o rappresentazione.

2.5 Le caratteristiche generali dei formati

L'informazione digitale è facilmente memorizzata, e può essere altrettanto facilmente acceduta, riutilizzata, modificata e elaborata per ottenere nuova informazione.

I formati dei documenti elettronici ed i programmi che li gestiscono vanno valutati in funzione di alcune caratteristiche quali:

- La diffusione, ossia il numero di persone ed organizzazioni che li adotta;
- La portabilità, ancor meglio se essa è indotta dall'impiego fedele di standard documentati e accessibili;
- Le funzionalità che l'utente ha a disposizione per elaborare l'informazione e collegarla ad altre (ad esempio gestione di link);
- La capacità di gestire contemporaneamente un numero congruo (in funzione delle esigenze dell'utente) di formati;
- La diffusione di visualizzatori che consentono una fruibilità delle informazioni in essi contenute indipendentemente dalla possibilità di rielaborarle.

Altre caratteristiche importanti sono la capacità di occupare il minor spazio possibile in fase di memorizzazione (a questo proposito vanno valutati, in funzione delle esigenze dell'utente, gli eventuali livelli di compressione utilizzabili) e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a chi ha eseguito modifiche o aggiunte.

È facilmente comprensibile come, nella fase di gestione degli strumenti digitali, l'utente debba avere a disposizione la massima flessibilità possibile in termini di formati e funzionalità disponibili.

Gli unici limiti sono quelli che un'organizzazione impone a se stessa quando per esigenze di interscambio ed interoperabilità, può determinare i formati, e i relativi programmi di gestione, che maggiormente soddisfano le contingenti esigenze operative.

3 Criteri di scelta dei formati

Ai fini della formazione, gestione e conservazione, è necessario scegliere formati che possano garantire la leggibilità e la reperibilità del documento informatico nel suo ciclo di vita.

La scelta tra i formati dipende dalle caratteristiche proprie del formato e dei programmi che lo gestiscono.

3.1 Caratteristiche

Le caratteristiche di cui bisogna tener conto nella scelta sono:

1. apertura
2. sicurezza
3. portabilità
4. funzionalità
5. supporto allo sviluppo
6. diffusione

3.1.1 Apertura

Un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente.

Questa condizione si verifica sia quando il formato è documentato e pubblicato da un produttore o da un consorzio al fine di promuoverne l'adozione, sia quando il documento è conforme a formati definiti da organismi di standardizzazione riconosciuti. In quest'ultimo caso tuttavia si confida che quest'ultimi garantiscono l'adeguatezza e la completezza delle specifiche stesse.

Nelle indicazioni di questo documento si è inteso privilegiare i formati già approvati dagli Organismi di standardizzazione internazionali quali International Organization for Standardization (ISO) ed European Telecommunications Standards Institute (ETSI).

3.1.2 Sicurezza

La sicurezza di un formato dipende da due elementi: il grado di modificabilità del contenuto del file e la capacità di essere immune dall'inserimento di codice maligno.

3.1.3 Portabilità

Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto è indotta dall'impiego fedele di standard documentati e accessibili.

3.1.4 Funzionalità

Per funzionalità si intende la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione dell'utente per la formazione e gestione del documento informatico.

3.1.5 Supporto allo sviluppo

È la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).

3.1.6 Diffusione

La diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti elettronici.

Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.

Inoltre nella scelta dei prodotti altre caratteristiche importanti sono la capacità di occupare il minor spazio possibile in fase di memorizzazione (a questo proposito vanno valutati, in funzione delle esigenze dell'utente, gli eventuali livelli di compressione utilizzabili) e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a chi ha eseguito modifiche o aggiunte.

4 Scelta

4.1 Formati e prodotti per la formazione e gestione

Per la scelta dei formati idonei alla formazione e gestione dei documenti elettronici sono da tenere in considerazione le caratteristiche indicate nei paragrafi precedenti.

Ulteriori elementi da valutare sono l'efficienza in termini di occupazione di spazio fisico e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a modifiche o aggiunte intervenute sul documento.

Le pubbliche amministrazioni indicano nel manuale di gestione i formati adottati per le diverse tipologie di documenti elettronici motivandone le scelte effettuate; specificano altresì i casi eccezionali in cui non è possibile adottare i formati in elenco motivandone le ragioni.

4.2 Formati per la conservazione

La scelta dei formati idonei alla conservazione oltre al soddisfacimento delle caratteristiche suddette deve essere strumentale a che il documento assuma le caratteristiche di immodificabilità e di staticità previste dalle regole tecniche.

Per quanto fin qui considerato, è opportuno privilegiare i formati che siano standard internazionali (de jure e de facto) o, quando necessario, formati proprietari le cui specifiche tecniche siano pubbliche, dandone opportuna evidenza nel manuale di conservazione dei documenti elettronici.

Ulteriore elemento di valutazione nella scelta del formato è il tempo di conservazione previsto dalla normativa per le singole tipologie di documenti elettronici.

I formati per la conservazione adottati per le diverse tipologie di documenti elettronici devono essere indicati nel manuale di conservazione motivandone le scelte effettuate; sono altresì specificati i casi eccezionali in cui non è possibile adottare i formati in elenco motivandone le ragioni.

5 I formati indicati per la conservazione

I formati di seguito indicati sono un primo elenco di formati che possono essere usati per la conservazione.

Come già indicato nelle premesse questo elenco sarà periodicamente aggiornato.

5.1 PDF - PDF/A

Il PDF (Portable Document Format) è un formato creato da Adobe nel 1993 che attualmente si basa sullo standard ISO 32000. È stato concepito per rappresentare documenti complessi in modo indipendente dalle caratteristiche dell'ambiente di elaborazione del documento. Nell'attuale versione gestisce varie tipologie di informazioni quali: testo formattato, immagini, grafica vettoriale 2D e 3D, filmati.

Un documento PDF può essere firmato digitalmente in modalità nativa attraverso il formato ETSI PAdES.

Il formato è stato ampliato in una serie di sotto-formati tra cui il PDF/A.

Sviluppato da	Adobe Systems http://www.adobe.com/
Estensione	.pdf
Tipo MIME	application/pdf
Formato aperto	Sì
Specifiche tecniche	Pubbliche
Standard	ISO 32000-1 (PDF) ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)
Ultima versione	1.7
Collegamento utile	http://www.pdfa.org/doku.php

Il PDF/A è stato sviluppato con l'obiettivo specifico di rendere possibile la conservazione documentale a lungo termine su supporti digitali.

Tra le caratteristiche di questa tipologia di file abbiamo:

- assenza di collegamenti esterni,
- assenza di codici eseguibili quali javascript ecc.,
- assenza di contenuti crittografati.

Queste caratteristiche rendono il file indipendente da codici e collegamenti esterni che ne possono alterare l'integrità e l'uniformità nel lungo periodo.

Le più diffuse suite d'ufficio permettono di salvare direttamente i file nel formato PDF/A.

Sono disponibili prodotti per la verifica della conformità di un documento PDF al formato PDF/A.

5.2 TIFF

Sviluppato da	Aldus Corporation in seguito acquistata da Adobe
Estensioni	.tif
Tipo MIME	image/tiff
Formato aperto	No
Specifiche tecniche	Pubbliche
Ultime versioni	TIFF 6.0 del 1992 TIFF Supplement 2 del 2002
Collegamenti utili	http://partners.adobe.com/public/developer/tiff/index.html

Di questo formato immagine raster, in versione non compressa o compressa senza perdita di informazione. Di questo formato vi sono parecchie versioni, alcune delle quali proprietarie (che ai fini della conservazione nel lungo periodo sarebbe bene evitare). In genere le specifiche sono pubbliche e non soggette ad alcuna forma di limitazione.

Questo è un formato utilizzato per la conversione in digitale di documenti cartacei. Il suo impiego va valutato

attentamente in funzione del tipo di documento da conservare in considerazione dei livelli di compressione e relativa perdita dei dati.

Esistono, infine, alcuni formati ISO basati sulla specifica TIFF 6.0 di Adobe (che è quella "ufficiale" del TIFF). Si tratta del formato ISO 12639, altrimenti noto come TIFF/IT, rivolto particolarmente al mondo del publishing e della stampa e dell'ISO 12234, altrimenti detto TIFF/EP, più orientato alla fotografia digitale.

5.3 JPG

Sviluppato da	Joint Photographic Experts Group
Estensioni	.jpg, .jpeg
Tipo MIME	image/jpeg
Formato aperto	Sì
Specifiche tecniche	Pubbliche
Standard	ISO/IEC 10918:1
Ultima versione	2009
Collegamenti utili	http://www.jpeg.org/ www.iso.org

Il formato JPEG può comportare una perdita di qualità dell'immagine originale. Anche in questo caso, come nel caso dei TIFF, avendo una grossa diffusione, può essere preso in considerazione, ma il suo impiego, correlato ad un opportuno livello di compressione va valutato attentamente in funzione del tipo di documento da conservare.

JPG è il formato più utilizzato per la memorizzazione di fotografie ed è quello più comune su World Wide Web.
Lo stesso gruppo che ha ideato il JPG ha prodotto il JPEG 2000 con estensione .jp2 (ISO/IEC 15444-1) che può utilizzare la compressione senza perdita di informazione. Il formato JPEG 2000 consente, inoltre, di associare metadati ad un'immagine. Nonostante queste caratteristiche la sua diffusione è tutt'oggi relativa.

5.4 Office Open XML (OOXML)

Sviluppato da	Microsoft http://www.microsoft.com http://www.microsoft.it
Estensioni principali	.docx, .xlsx, .pptx
Tipo MIME	
Formato aperto	Sì
Derivato da	XML
Specifiche tecniche	pubblicate da Microsoft dal 2007
Standard	ISO/IEC DIS 29500:2008
Ultima versione	1.1
Possibile presenza codice maligno	Sì
Collegamenti utili	http://msdn.microsoft.com/en-us/library/aa338205.aspx http://standards.iso.org/ittf/PubliclyAvailableStandards www.iso.org

Comunemente abbreviato in OOXML, è un formato di file, sviluppato da Microsoft, basato sul linguaggio XML per la creazione di documenti di testo, fogli di calcolo, presentazioni, grafici e database.

Open XML è adottato dalla versione 2007 della suite Office di Microsoft.

Lo standard prevede, oltre alle indicazioni fondamentali (strict), alcune norme transitorie (transitional) introdotte per ammettere, anche se solo temporaneamente, alcune funzionalità presenti nelle vecchie versioni del formato e la cui rimozione avrebbe potuto danneggiare gli utenti, facendogli perdere funzionalità.

Per quanto riguarda il supporto di Microsoft Office allo standard ISO/IEC 29500:2008:

- MS Office 2007 legge e scrive file conformi a ECMA-376 Edition 1.
- MS Office 2010 legge e scrive file conformi a ISO/IEC 29500:2008 transitional e legge file conformi a ISO/IEC 29500:2008 strict

Documenti conformi ad ISO/IEC 29500:2008 strict sono supportati da diversi prodotti informatici disponibili sul mercato.

Il formato Office Open XML dispone di alcune caratteristiche che lo rendono adatto alla conservazione nel lungo periodo, tra queste l'embedding dei font, la presenza di indicazioni di presentazione del documento, la possibilità di applicare al documento la firma digitale XML.

I metadati associabili ad un documento che adotta tale formato sono previsti dallo standard ISO 29500:2008.

5.5 Open Document Format

Sviluppato da	OASIS http://www.oasis-open.org/ Oracle America (già Sun Microsystems) http://www.oracle.com/it/index.html
Estensioni	.ods, .odp, .odg, .odb
Tipo MIME	application/vnd.oasis.opendocument.text
Formato aperto	Sì
Derivato da	XML
Specifiche tecniche	pubblicate da OASIS dal 2005
Standard	ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300
Ultima versione	1.0
Collegamenti utili	http://books.evc-cit.info/ http://www.oasis-open.org www.iso.org

ODF (Open Document Format, spesso referenziato con il termine OpenDocument) è uno standard aperto, basato sul linguaggio XML, sviluppato dal consorzio OASIS per la memorizzazione di documenti corrispondenti a testo, fogli elettronici, grafici e presentazioni. Secondo questo formato, un documento è descritto da più strutture XML, relative a contenuto, stili, metadati ed informazioni per l'applicazione.

Lo standard ISO/IEC IS 26300:2006 è ampiamente usato come standard documentale nativo, oltre che da OpenOffice.org, da una ampia serie di altri prodotti disponibili sulle principali piattaforme: Windows, Linux. Mac.

È stato adottato come standard di riferimento da moltissime organizzazioni governative e da diversi governi ed ha una diffusione che cresce giorno per giorno.

5.6 XML

Sviluppato da	W3C
Estensioni	.xml
Tipo MIME	application/xml text/xml
Formato aperto	Sì
Specifiche tecniche	pubblicate da W3C http://www.w3.org/XML/
Collegamenti utili	http://www.w3.org/

Extensible Markup Language (XML) è un formato di testo flessibile derivato da SGML (ISO 8879).

Su XML si basano numerosi linguaggi standard utilizzati nei più diversi ambiti applicativi. Ad esempio:

- SVG usato nella descrizione di immagini vettoriali
- XBRL usato nella comunicazione di dati finanziari
- ebXML usato nel commercio elettronico
- SOAP utilizzato nello scambio dei messaggi tra Web Service

5.7 TXT

Oltre a XML, per quanto concerne i formati non binari "in chiaro", è universalmente utilizzato il formato TXT.

Ai fini della conservazione nell'uso di tale formato, è importante specificare la codifica del carattere (Character Encoding) adottata.

5.8 Formati Messaggi di posta elettronica

Ai fini della conservazione, per preservare l'autenticità dei messaggi di posta elettronica, lo standard a cui fare riferimento è RFC 2822/MIME.

Per quanto concerne il formato degli allegati al messaggio, valgono le indicazioni di cui ai precedenti paragrafi.

ALLEGATO "2"

Metadati minimi del documento elettronico

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

<xs:element name="documento">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="datachiusura" type="xs:date"/>
      <xs:element  name="oggettodocumento"  type="xs:string
      /> <xs:element name="soggettoproduttore" />
        <xs:complexType>
          <xs:sequence>
            <xs:element name="nome" type="xs:string"/>
            <xs:element name="cognome" type="xs:string"/>
            <xs:element                    name="codicefiscale"
          type="xs:string"/> </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="destinatario">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="nome" type="xs:string"/>
            <xs:element name="cognome" type="xs:string"/>
            <xs:element                    name="codicefiscale"
          type="xs:string"/> </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
   <xs:attribute    name="IDDocumento"    type="xs:string"    use="required"/>
  </xs:complexType>
</xs:element>
</xs:schema>
```

Informazione	Valori Ammessi	Tipo dato	xsd
Identificativo	Come da sistema di identificazione formalmente definito.	Alfanumerico 20 caratteri	<xs:attribute name="IDDocumento" type="xs:string" use="required"/>
Definizione			
Identificativo univoco e persistente è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione. Dublin Core raccomanda di identificare il documento per mezzo di una sequenza di caratteri alfabetici a numerici secondo un sistema di identificazione formalmente definito. Esempi di tali sistemi di identificazione includono l'Uniform Resource Identifier (URI), il Digital Object Identifier (DO!) e l'International Standard Book Number (ISBN)			

Informazione	Valori Ammessi	Tipo dato	xsd
Data di chiusura	Data	Data formato gg/mm/aaaa	<xs:element name="datachiusura" type="xs:date"/>
Definizione			
Data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.			

Informazione	Valori Ammessi	Tipo dato	xsd
Oggetto	Testo libero	Alfanumerico 100 caratteri	<xs:element name="oggettodocumento" type="xs:string />
Definizione			
Oggetto, metadato funzionale a riassumere brevemente il contenuto del documento o comunque a chiarirne la natura. Dublic Core prevede l'analoga proprietà "Description" che può includere ma non è limitata solo a: un riassunto analitico, un indice, un riferimento al contenuto di una rappresentazione grafica o un testo libero del contenuto.			

Informazione	Valori Ammessi	Tipo dato	xsd
Soggetto produttore	nome: Testo libero	Alfanumerico 40 caratteri	<xs:element name="soggettoproduttore"> <xs:complexType> <xs:sequence> <xs:element name="nome" type="xs:string"/> <xs:element name="cognome" type="xs:string"/> <xs:element name="codicefiscale“ type="xs:string"/> </xs:sequence> </xs:complexType> </xs:element>
	cognome: testo libero	Alfanumerico 40 caratteri	
	Codice fiscale: Codice Fiscale	Alfanumerico 16 caratteri	
Definizione			
Il soggetto che ha l'autorità e la competenza a produrre il documento informatico.			

Informazione	Valori Ammessi	Tipo dato	xsd
Destinatario	nome: Testo libero	Alfanumerico 40 caratteri	<xs:element name="destinatario"> <xs:complexType> <xs:sequence> <xs:element name-'nome" type="xs:string’7> <xs:element name="cognome” type="xs:string"/> <xs:element name="codicefiscale" type="xs:string"/> </xs:sequence> </xs:complexType> </xs:element>
	cognome: testo libero	Alfanumerico 40 caratteri	
	Codice fiscale: Codice Fiscale **(Obbligatorio, se disponibile)**	Alfanumerico 16 caratteri	
Definizione			
Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico.			

LEGGE 31 OTTOBRE 2018 n.137

II VARIAZIONE AL BILANCIO DI PREVISIONE DELLO STATO, VARIAZIONE AL BILANCIO DI PREVISIONE DEGLI ENTI DEL SETTORE PUBBLICO ALLARGATO PER L'ESERCIZIO FINANZIARIO 2018, MODIFICHE ALLA LEGGE 21 DICEMBRE 2017 N.147 E SUCCESSIVE MODIFICHE

Art.22

(Disposizioni relative al Registro pubblico dei domicili digitali)

1. Gli operatori economici, ai sensi dell'articolo 3, comma 1, lettera c), del Decreto Delegato 11 aprile 2016 n.46, hanno l'obbligo di effettuare la registrazione del proprio domicilio digitale entro il termine massimo del 30 aprile 2019, secondo le modalità stabilite in apposito regolamento.
2. Agli operatori economici che non abbiano provveduto a registrare un domicilio digitale valido, si applica una sanzione pecuniaria amministrativa per ogni infrazione:

a) a decorrere dal 1 maggio 2019 pari alla somma di euro 50,00, per ogni iniziativa d'uso del domicilio digitale dell'operatore economico, fino all'occorrenza di un importo massimo di euro 600,00, per ogni anno solare;
b) a decorrere dall'1 gennaio 2020 pari alla somma di euro 200,00, per ogni iniziativa d'uso del domicilio digitale dell'operatore economico, fino all'occorrenza di un importo massimo di euro 2.400,00, per ogni anno solare.

3. Tutti i soggetti, quando abbiano eletto - volontariamente od obbligatoriamente - il proprio domicilio digitale, hanno l'obbligo di dichiarare, entro trenta giorni dall'evento, ogni variazione delle informazioni relative al proprio domicilio digitale, con le modalità stabilite in apposito regolamento.

Ai soggetti che, non avendo provveduto ad effettuare la variazione delle superiori informazioni, risultino sprovvisti, all'atto di un controllo dell'Amministrazione, di un domicilio digitale valido e funzionale, è applicata la sanzione pecuniaria amministrativa prevista al comma 2, con una riduzione pari al 50% se persone fisiche. Tale riduzione potrà essere modificata tramite decreto delegato.

4. Gli organi competenti all'accertamento dei superiori obblighi, anche attraverso l'uso di sistemi automatizzati e di tecnologie informatiche, sono:

a) l'UO Ufficio Attività di Controllo, di cui all'articolo 23 dell'Allegato A della Legge 5 dicembre 2011 n.188, così come novellato dall'articolo 6 del Decreto Delegato 1 marzo 2018 n.22, con riferimento all'obbligo di cui al comma 1;
b) l'UO Informatica Tecnologia Dati e Statistica, di cui all'articolo 52 dell'Allegato A della Legge n.188/2011, con riferimento all'obbligo di cui al comma 3.
a) I superiori organi applicano la sanzione pecuniaria amministrativa, di cui ai commi 2 e 3, in caso di inosservanza dell'obbligo.

5. Per lo svolgimento delle attività di cui al comma 6, l'UO Informatica Tecnologia Dati e Statistica può avvalersi di altri soggetti dell'Amministrazione, come definita all'articolo 1, comma 2, lettera a) della Legge 5 ottobre 2011 n.160, nel rispetto di protocolli operativi stipulati con i soggetti medesimi.
6. Colui che elegge domicilio digitale con l'iscrizione nel relativo registro, istituito ai sensi dell'articolo 5, comma 1, del Decreto Delegato n.46/2016 così come modificato dall'articolo 3 del Decreto Delegato 26 luglio 2018 n.92, non può opporre eccezioni relative all'uso o disponibilità dell'indirizzo di posta elettronica indicato quale domicilio digitale.
7. Le comunicazioni, gli atti e i documenti trasmessi a mezzo del servizio elettronico di recapito certificato, ai sensi degli articoli 8-*bis* e 8-*ter* del Decreto Delegato n.46/2016, così come modificato all'articolo 4 del Decreto Delegato n.92/2018, non ritirati dal destinatario, producono gli stessi effetti giuridici della compiuta giacenza di una raccomandata postale, quando il servizio elettronico di recapito certificato ha reso disponibile il ritiro in giacenza per un tempo di trenta giorni solari dalla data di trasmissione.

8. [abrogato].[23]

9. Le dichiarazioni sostitutive di atto di notorietà per l'elezione, la variazione e la cancellazione del domicilio digitale di cui all'articolo 2, comma 1, lettera e *bis*) del Decreto Delegato n.46/2016, così come modificato dall'articolo 2, comma 2, del Decreto Delegato n.92/2018, sono esenti da imposta di bollo.

[23] **Testo originario (Legge 31 ottobre 2018 n.137 comma 8)**

8. Sulle copie analogiche dei documenti informatici generati dal Registro pubblico dei domicili digitali e dal servizio elettronico di recapito certificato, può essere apposto a stampa un contrassegno, sulla base dei criteri definiti da standard internazionali, tramite il quale è possibile accedere al documento informatico originale, ovvero verificare la corrispondenza allo stesso della copia analogica

Modifiche Legislative

DECRETO DELEGATO 30 gennaio 2020 n.9, Art. 9 comma 8

8. L'articolo 22, comma 8, della Legge 31 ottobre 2018 n.137 e gli articoli 2, comma 1, lettera d) e 7, comma 2 del Decreto Delegato n.46/2016 sono abrogati. L'espressione "nonché dei documenti informatici nel loro formato originale" di cui all'articolo 7, comma 1 del Decreto Delegato n.46/2016 è soppressa

REGOLAMENTO 22 novembre 2018 n.7 – ABROGATO [24]

REGOLAMENTO PER L'UTILIZZO DEL REGISTRO PUBBLICO DEI DOMICILI DIGITALI

Art. 1
(Finalità)

1. Il presente regolamento disciplina l'utilizzo del Registro pubblico dei domicili digitali istituito ai sensi dell'articolo 5, comma 1, del Decreto Delegato 11 aprile 2016 n. 46 così come modificato all'articolo 3 del Decreto Delegato 26 luglio 2018 n. 92.

Art. 2
(Definizioni)

1. Ai fini del presente Regolamento si intende per:
a) Domicilio digitale: un indirizzo di posta elettronica il cui formato è conforme allo standard RFC2822, al paragrafo "*3.4.1. Addr-spec specification*", definito dall'Internet Engineering Task Force (http://ietf.org);
b) Registro dei domicili digitali (di seguito Registro): insieme di dati in formato elettronico che mette in corrispondenza univoca i dati di identificazione personale di una persona fisica o giuridica con il relativo domicilio digitale;
c) Firma elettronica qualificata: quella definita all'articolo 1, comma 1, lettera e) della Legge 20 luglio 2005 n.115 e all'articolo 3, comma 12, del Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno;
d) Servizio Elettronico di Recapito Certificato (SERC): servizio di trasmissione dati definito dall'articolo *8-bis e 8-ter*, comma 1, del Decreto Delegato n. 46/2016 così come modificato dall'articolo 4 del Decreto Delegato n. 92/2018;
e) Amministrazione: l'intero complesso degli organi, uffici, servizi, enti pubblici e aziende dello Stato e le pertinenti attività del Settore Pubblico Allargato, come definita all'articolo 1, comma 2, lettera a) della Legge 5 ottobre 2011 n.160;
f) Soggetti privati: soggetti non rientranti nella definizione di Amministrazione.

Art. 3
(Tenuta e gestione operativa del Registro)

1. La tenuta del Registro è affidata all'UO Informatica, Tecnologia, Dati e Statistica, che:
a) sovraintende alla realizzazione, allo sviluppo ed alla manutenzione della procedura informatica attraverso cui è gestito il Registro;
b) sovraintende alla realizzazione, allo sviluppo ed alla manutenzione delle interfacce e delle procedure di integrazione, di sincronizzazione e di consolidamento dei dati relativi ai domicili digitali contenuti in altri archivi o registri in uso presso l'Amministrazione;
c) sovraintende alla predisposizione di canali di comunicazione sicuri atti alla trasmissione dei dati relativi ai domicili digitali;

---

[24] **Modifiche legislative:**
DECRETO DELEGATO 21 marzo 2023 n.51, Art.26 comma 8
8. Sono abrogati:
a) il Decreto Delegato 11 aprile 2016 n.46;
b) il Decreto Delegato 26 luglio 2018 n.92;
c) il Regolamento 22 novembre 2018 n.7;
d) gli articoli 5, 6, 7, 8 e 9 del Decreto Delegato 30 gennaio 2020 n.9;
e) l'articolo 85 ter, comma 4 del Decreto n.156/2005, come introdotto dall'articolo 4 del Decreto Delegato n.9/2020;
f) l'articolo 3, comma 1, lettera f), l'articolo 9, comma 1, lettera l), l'articolo 9, comma 2, lettere d) ed e), l'articolo 11 e l'articolo 12 del Decreto Delegato 29 marzo 2021 n.61;
g) il Regolamento 17 dicembre 2021 n.18;
h) gli articoli 12, 13bis e 16, comma 2 *bis* del Decreto Delegato 29 ottobre 2021 n.184;
i) gli articoli 2 e 4 del Decreto Delegato 17 dicembre 2021 n.204.

d) predispone l'accesso di terzi ai dati contenuti nel Registro su autorizzazione del Direttore Pianificazione e Controllo ai sensi dell'articolo 31, comma 2, lettera a), della Legge 5 dicembre 2011 n. 188.

2. La gestione operativa del Registro è affidata ad ATI Poste SM tNotice, affidataria della fornitura del servizio elettronico di recapito certificato di cui al Decreto Delegato n. 46/2016 così come modificato dal Decreto Delegato n. 92/2018.

3. Ai sensi dell'articolo 22, comma 8, della Legge 31 ottobre 2018 n. 137, è adottata come standard internazionale per il contrassegno da utilizzare per i documenti informatici generati dal Registro e dal servizio elettronico di recapito certificato la specifica tecnica EN ISO/IEC 18004:26006.

Art. 4

(Soggetti abilitati alla registrazione e variazione dei dati relativi ai domicili digitali)

1. Il servizio di registrazione e di variazione dei dati relativi ai domicili digitali, per l'Amministrazione e le persone fisiche, autorizzate all'utilizzo del servizio elettronico di recapito certificato in nome e per conto dell'Amministrazione, è svolto dall'UO Informatica, Tecnologia, Dati e Statistica, utilizzando i dati in proprio possesso.

2. Il servizio di registrazione e di variazione delle informazioni relative ai domicili digitali di soggetti diversi da quelli indicati al comma 1 è affidato a ATI Poste SM tNotice.

Art. 5

(Modalità di registrazione e variazione dei dati relativi ai domicili digitali dei soggetti privati)

1. La registrazione e la variazione delle informazioni relative ai domicili digitali dei soggetti privati, persona fisica o giuridica, avvengono tramite acquisizione di dichiarazione sostitutiva di atto di notorietà di cui all'articolo 13 della Legge 5 ottobre 2011 n. 159, sottoscritta dalla persona fisica o da un rappresentante autorizzato della persona giuridica, nella quale il soggetto:

a) dichiara di eleggere domicilio digitale presso un indirizzo di posta elettronica e che lo stesso è nella propria disponibilità d'uso;
b) indica il proprio domicilio digitale nella forma stabilita dall'articolo 2, comma 1, lettera a;
c) esprime il proprio consenso a ricevere dall'Amministrazione documenti o atti amministrativi di proprio interesse mediante un servizio elettronico di recapito certificato;
d) dichiara di avvalersi della modalità di trasmissione per via telematica di documenti informatici o di istanze all'Amministrazione, a mente dell'articolo 10, comma 3, della Legge n. 159/2011 e dell'articolo 10, comma 5, della Legge n. 160/2011.

2. La presentazione della dichiarazione sostitutiva di atto di notorietà di cui al comma 1, può avvenire esclusivamente:

a) presso gli sportelli di Poste San Marino S.p.A., tramite sottoscrizione autografa in calce alla dichiarazione stessa e previa identificazione *de visu* del dichiarante da parte dell'operatore di sportello e acquisizione di copia fotostatica del documento di identità in corso di validità, nel rispetto dell'articolo 11, comma 1, della Legge n. 159/2011;
b) tramite lo "sportello virtuale", messo a disposizione dall'UO Informatica, Tecnologia, Dati e Statistica, previa apposizione di firma elettronica qualificata in corso di validità del dichiarante.

3. La persona giuridica residente all'estero che elegge in via volontaria il proprio domicilio digitale nella Repubblica di San Marino nei termini e secondo le modalità di cui ai commi 1 e 2, è tenuta ad allegare i documenti comprovanti i poteri di rappresentanza mediante certificazione pubblica dell'autorità emittente, redatta in lingua italiana e munita di firma elettronica qualificata, oppure munita di un contrassegno tramite il quale sia possibile accedere al documento informatico originale. Qualora la predetta documentazione sia già stata prodotta all'Amministrazione nell'ambito di altri procedimenti e sia ancora in corso di validità al momento della richiesta di elezione, ai sensi dell'articolo 4 della Legge n. 159/2011, è sufficiente l'allegazione della dichiarazione sostitutiva di certificazione nella quale sia indicato anche l'ufficio dell'Amministrazione presso cui la stessa è stata prodotta.

4. ATI Poste SM tNotice comunica l'avvenuta registrazione delle informazioni relative al domicilio digitale e delle loro successive variazioni tramite trasmissione di servizio elettronico di recapito certificato inviato al medesimo domicilio digitale.

5. L'elezione del domicilio digitale, così come la sua variazione, ha effetto dalla data e ora di completamento di tutte le attività di verifica tecnica dell'indirizzo di posta elettronica indicato e di perfezionamento della trasmissione di cui al comma 4. Fino a tale data e ora restano validi e con pieno effetto

giuridico i precedenti dati iscritti nel Registro, se presenti.

Art. 6
(Cancellazione dal Registro)

1. I soggetti privati non operatori economici i quali abbiano eletto il proprio domicilio digitale per l'utilizzo su base volontaria del servizio elettronico di recapito certificato, secondo quanto previsto dall'articolo 3, comma 1, lettera c), punto 2), del Decreto Delegato n. 46/2016, nonché i soggetti di cui all'articolo 5, comma 3, possono richiedere la cancellazione del proprio domicilio digitale dal Registro tramite apposita richiesta:

a) da presentare nei termini e con le medesime modalità previste dall'articolo 5, commi 1 e 2;
b) inviata a mezzo del servizio elettronico di recapito certificato, previa apposizione della firma elettronica qualificata del richiedente, in corso di validità.

2. Con la richiesta di cancellazione di cui al comma 1 il soggetto rinuncia espressamente alla facoltà di ricevere dall'Amministrazione documenti o atti amministrativi di proprio interesse mediante un servizio elettronico di recapito certificato, nonché alla facoltà di avvalersi della modalità di trasmissione per via telematica di documenti informatici all'Amministrazione a mente dell'articolo 10 della Legge n. 159/2011 e dell'articolo 10 della Legge n. 160/2011.

3. L'UO Informatica, Tecnologia, Dati e Statistica esegue la cancellazione entro il termine di cinque giorni lavorativi dal ricevimento della richiesta.

4. L'UO Informatica, Tecnologia, Dati e Statistica esegue la cancellazione d'ufficio delle informazioni relative ai domicili digitali dal Registro in tutti i casi previsti dalla normativa vigente.

DECRETO DELEGATO 21 marzo 2023 n.51 - TESTO UNICO INNOVATIVO DELLE DISPOSIZIONI IN MATERIA DI COMUNICAZIONE TELEMATICA CON L'AMMINISTRAZIONE E DI ACCESSO AI SERVIZI IN LINEA DELL'AMMINISTRAZIONE

CAPO I
FINALITA' E DEFINIZIONI

Art.1
(Finalità)

1. Il presente decreto delegato coordina ed innova le vigenti disposizioni in materia di servizio elettronico di recapito certificato nonché di comunicazione telematica fra utenti ed Amministrazione.
2. Il presente decreto delegato è adottato nell'esercizio delle deleghe di cui all'articolo 2, comma 4 della Legge 20 luglio 2005 n.115, di cui all'articolo 79 della Legge 22 dicembre 2010 n.194, di cui all'articolo 18, commi 2 e 3 della Legge 30 maggio 2019 n.88 e di cui all'articolo 25, comma 1 della Legge 7 luglio 2020 n.113.
3. Le disposizioni di cui ai Capi III e IV del presente decreto delegato sono dettate in conformità a quanto previsto dall'articolo 2, comma 3 della Legge n.115/2005 e dall'articolo 3bis del Decreto 8 novembre 2005 n.156 e successive modifiche.

Art. 2
(Definizioni)

1. Ai fini del presente decreto delegato i seguenti termini ed espressioni assumono i sotto indicati significati, coerentemente con quanto previsto anche dall'articolo 8 del Decreto Delegato 20 novembre 2020 n.204:

a) "Amministrazione", "Settore Pubblico Allargato", "Pubblica Amministrazione" ed "Enti": quanto rispettivamente definito dalle lettere a), b), c) e d) dell'articolo 3, comma 1, della Legge 5 dicembre 2011 n. 188;
b) "Regolamento eIDAS": Regolamento (UE) n.910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
c) "documento" o "documento analogico": la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti;
d) "documento elettronico": il documento che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, formato secondo quanto previsto dall'articolo 3-bis del Decreto n.156/2005 e successive modifiche;
e) "copia per immagine su supporto elettronico di documento analogico (scansione)" e "duplicato elettronico di documento elettronico": i documenti elettronici definiti rispettivamente dall'articolo 85-ter e dall'articolo 85-quinquies del Decreto n.156/2005, così come introdotti dall'articolo 4 del Decreto Delegato n.9/2020;
f) "documento amministrativo": il documento definito dall'articolo 2, comma 2 della Legge 5 ottobre 2011 n.159. Rientrano, pertanto, nella definizione di "documento amministrativo" le istanze nonché gli atti e documenti di cui rispettivamente agli articoli 10 e 15, comma 1, lettera c) della Legge 5 ottobre 2011 n.160;
g) "documento amministrativo elettronico": il documento amministrativo formato secondo quanto previsto dall'articolo 3-bis del Decreto n.156/2005 e successive modifiche. Rientrano, pertanto, nella definizione di "documento amministrativo elettronico" le istanze nonché gli atti e documenti di cui rispettivamente agli articoli 10 e 15, comma 1, lettera c) della Legge n.160/2011, formati secondo le norme di cui al precedente periodo;

h) “domicilio digitale”: un indirizzo di posta elettronica il cui formato è conforme allo standard RFC2822, al paragrafo “3.4.1. Addr-spec specification”, definito dall’Internet Engineering Task Force (http://ietf.org);
i) “Registro Pubblico dei Domicili Digitali” (in seguito brevemente RPDD): insieme di dati in formato elettronico che mette in corrispondenza univoca i dati di identificazione personale di una persona fisica o giuridica con il relativo domicilio digitale;
l) “PEC”: servizio di posta elettronica certificata di cui al Decreto del Presidente della Repubblica Italiana 11 febbraio 2005, n.68 e successive modifiche;
m) “firma elettronica qualificata”: il tipo di firma elettronica definita dall’articolo 1, comma 1, lettera e) della Legge n.115/2005 e dall’articolo 3, comma 12, del Regolamento eIDAS;
n) “utenza radiomobile”: servizio di telefonia pubblica via radio, associata ad un numero telefonico;
o) “Portale della Pubblica Amministrazione”: portale web attraverso cui l’Amministrazione eroga i propri servizi in linea;
p) “OTP”: One Time Password, codice di accesso usa e getta per autenticazione d’utente per l’accesso ad un servizio in linea;
q) “SMS”: servizio di trasmissione di brevi messaggi testuali a mezzo di rete telefonica pubblica via radio (Short Message Service);
r) “Autorità ICT”: l’Autorità per la Vigilanza e le garanzie nei servizi pubblici ICT (Information and Communications Technology) di cui al Decreto Delegato 20 novembre 2018 n.146, come modificato dal Decreto Delegato 20 novembre 2020 n.204;
s) “autenticazione rafforzata”: l’autenticazione eseguita mediante l’utilizzo di un secondo fattore di autenticazione costituito da un codice OTP ricevuto attraverso il servizio SMS su utenza radiomobile associata in maniera certa al richiedente l’accesso;
t) “programma applicativo”: detto anche applicazione o app, insieme di istruzioni atte a risolvere completamente un dato problema attraverso un calcolatore elettronico;
u) “procedura software”: insieme di istruzioni atto a risolvere parte di uno specifico problema oppure un problema generico;
v) “certificazione”: il documento amministrativo il cui rilascio avviene sulla base della sola operazione di estrazione di dati ed informazioni presenti nelle banche dati dello Stato e degli Enti Pubblici, senza ulteriori attività di ricerca, acquisizione ed elaborazione da parte dell’ufficio, ente ed organo pubblico. Rientrano nella suddetta definizione anche le certificazioni penali, dei carichi pendenti e del casellario giudiziario;
z) “contrassegno elettronico”: una sequenza di bit, codificata mediante una tecnica grafica e idonea a rappresentare un documento elettronico o un suo estratto o una sua copia o un suo duplicato elettronico o i suoi dati identificativi. Esso costituisce uno strumento mediante il quale è possibile effettuare una verifica della corrispondenza della predetta rappresentazione al documento elettronico originale.

Art. 3
(Recepimento di norme)

1. Sono recepite integralmente nell’ordinamento sammarinese le definizioni contenute all’articolo 3 del Regolamento eIDAS.
2. Le definizioni di cui al comma 1 prevalgono, in caso di contrasto, sulle definizioni stabilite dalle norme interne.

CAPO II
SERVIZI ELETTRONICI DI RECAPITO CERTIFICATO E DOMICILIO DIGITALE

SEZIONE I
SERVIZI ELETTRONICI DI RECAPITO CERTIFICATO E DISPOSIZIONI RELATIVE ALLA POSTA ELETTRONICA CERTIFICATA

Art. 4
(Requisiti relativi ai servizi elettronici di recapito certificato – SERC)

1. Un servizio elettronico di recapito certificato, in seguito brevemente SERC, consente la trasmissione di documenti elettronici fra soggetti, pubblici o privati, per via telematica e fornisce prove relative al loro trattamento proteggendoli dal rischio di perdita, furto, danni o modifiche non autorizzate.
2. Il SERC soddisfa i seguenti requisiti:
a) garantisce, con un elevato livello di sicurezza, l'identificazione del mittente;
b) garantisce l'identificazione del destinatario prima della consegna dei dati;
c) l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato per la firma elettronica, in modo da escludere la possibilità di modifiche non rilevabili dei dati;
d) qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente e al destinatario dei dati stessi;
e) la data e l'ora di invio e di ricezione e qualsiasi modifica dei dati sono indicate da una validazione temporale elettronica qualificata.
3. I SERC utilizzabili ai fini del presente decreto delegato sono autorizzati dall'Autorità ICT, fatto salvo il SERC già autorizzato alla data di entrata in vigore del presente decreto delegato.

Art. 5
(Effetti giuridici relativi alla trasmissione di documenti elettronici mediante SERC)

1. I documenti elettronici trasmessi mediante SERC fra soggetti, pubblici o privati, dotati di domicilio digitale godono:
a) della certezza dell'invio da parte del mittente dotato di domicilio digitale;
b) della certezza della loro consegna al destinatario dotato di domicilio digitale;
c) della presunzione di integrità dei dati e documenti in essi contenuti.
2. La trasmissione di documenti elettronici tramite SERC fra soggetti, pubblici o privati, dotati di domicilio digitale equivale alla spedizione per mezzo di posta raccomandata con avviso di ricevimento. In particolare, la notificazione degli atti amministrativi di qualsiasi natura, ivi compresi quelli in materia tributaria nonché quelli che irrogano sanzioni amministrative può essere eseguita mediante trasmissione a mezzo SERC ai sensi dell'articolo 6, con i medesimi effetti giuridici della notificazione a mezzo di raccomandata con ricevuta di ricevimento di cui all'articolo 17 della Legge 29 luglio 2013 n.100.
3. Le ricevute di invio e consegna convalidate dal prestatore di servizi fiduciari sono valide e rilevanti a tutti gli effetti di legge e possono essere opposte a terzi in giudizio.
4. I documenti elettronici inviati mediante SERC si intendono spediti dal mittente se inviati al prestatore del SERC e si intendono consegnati se resi disponibili al domicilio digitale del destinatario, salva la prova che la mancata consegna sia dovuta a fatto non imputabile al destinatario medesimo.
5. I documenti elettronici trasmessi a mezzo SERC non ritirati dal destinatario, producono gli stessi effetti giuridici della compiuta giacenza di una raccomandata postale, quando il SERC ha reso disponibile il ritiro in giacenza per un tempo di trenta giorni solari dalla data di trasmissione oppure per il minore periodo di tempo stabilito dalle norme speciali relative allo specifico procedimento od attività amministrativa.
6. Qualora il SERC generi un certificato postale forense di mancata consegna o di altra anomalia per cause non dipendenti dal mittente, il deposito del documento amministrativo

elettronico tramite SERC deve essere ripetuto tempestivamente con il medesimo contenuto, allegando la ricevuta ed il certificato postale forense relativi alla precedente trasmissione; ciò anche allo scopo di provare la non imputabilità al mittente dell'eventuale mancato rispetto delle scadenze previste, con conseguente rimessione in termini del mittente stesso.

Art. 6

(Utilizzo di SERC nei rapporti fra soggetti pubblici e soggetti privati)

1. L'utilizzo di SERC per la trasmissione di dati e documenti elettronici in relazione alla quale il mittente, soggetto pubblico o privato dotato di domicilio digitale, debba acquisire la certezza dell'invio e della consegna al destinatario, soggetto pubblico o privato dotato anch'esso di domicilio digitale, avviene secondo i termini sotto specificati:
   a) fra Pubblica Amministrazione ed Enti del Settore Pubblico Allargato: obbligatoriamente;
   b) fra Amministrazione e persone pubbliche o private che erogano un pubblico servizio: secondo modalità e termini definiti con appositi protocolli operativi;
   c) fra Amministrazione e soggetti privati:
      1) qualora l'Amministrazione sia il mittente della trasmissione a mezzo SERC:
         1.1) obbligatoriamente, in caso di destinatario in possesso di codice operatore economico (in seguito brevemente COE). A tal fine, sono obbligati all'elezione di domicilio digitale, entro il termine massimo di trenta giorni dall'attribuzione del COE, gli operatori economici (in seguito brevemente OE) ad esclusione dei seguenti:
            1.1.1) i soggetti in possesso di COE unicamente ai fini dell'assunzione, in qualità di datore di lavoro, di lavoratore migrante o straniero che svolga attività di assistenza continua rivolta a soggetti non autosufficienti;
            1.1.2) i soggetti in possesso di COE quali operatori agricoli non professionali;
            1.1.3) altre categorie di soggetti in possesso di COE individuate con direttiva del Congresso di Stato.
         1.2) in caso di destinatario non operatore economico, esclusivamente qualora il soggetto abbia volontariamente eletto domicilio digitale. Le Direzioni Generali del Settore Pubblico Allargato hanno, tuttavia, facoltà, sentita la Direzione Generale della Funzione Pubblica (in seguito brevemente DGFP) di stabilire l'obbligatorietà di elezione di domicilio digitale e di utilizzo del SERC ai fini delle comunicazioni telematiche relative a specifici procedimenti, servizi ed attività;
   d) fra persone pubbliche o private che erogano un pubblico servizio e soggetti privati: secondo quanto previsto dai rispettivi regolamenti o norme interne, adottati sentita l'Autorità ICT;
   e) esclusivamente fra soggetti privati, persone fisiche o giuridiche, sammarinesi o residenti: l'utilizzo del SERC avviene su base volontaria.

2. All'OE che non abbia provveduto ad eleggere un domicilio digitale valido si applica una sanzione pecuniaria amministrativa pari a euro 200,00 (duecento/00) per ogni iniziativa d'uso del domicilio digitale dell'operatore economico, fino all'occorrenza di un importo massimo di euro 2.400,00 (duemilaquattrocento/00) per ogni anno solare. L'accertamento delle violazioni di cui al presente comma ed al comma 4, anche attraverso l'uso di sistemi automatizzati e di tecnologie informatiche, e la comminazione delle sanzioni amministrative previste in caso di inosservanza compete all'UO Ufficio Attività di Controllo il quale si attiva, altresì, su segnalazione di soggetti pubblici e privati.

3. Tutti i soggetti, quando abbiano eletto - volontariamente od obbligatoriamente - il proprio domicilio digitale, hanno l'obbligo di dichiarare, entro trenta giorni dall'evento, ogni variazione delle informazioni relative al proprio domicilio digitale mediante dichiarazione sostitutiva di atto di notorietà di cui all'articolo 13 della Legge n.159/2011, esente da imposta di bollo.

4. Ai soggetti che, non avendo provveduto ad effettuare la variazione delle superiori informazioni, risultino sprovvisti, all'atto dei controlli effettuati dall'Amministrazione, di un domicilio digitale valido e funzionale, è applicata la sanzione pecuniaria amministrativa prevista al comma 2, con una riduzione pari al 50% se persone fisiche.

5. Il mittente, soggetto privato, che abbia eletto domicilio digitale ha facoltà di utilizzare il SERC per la presentazione di documenti amministrativi elettronici, salvo che, in relazione a specifici procedimenti, servizi ed attività, le Direzioni Generali del Settore Pubblico Allargato ne stabiliscano l'obbligatorietà, sentita la DGFP.
6. I dipendenti del Settore Pubblico Allargato e gli iscritti ed aspiranti all'iscrizione nelle graduatorie per l'insegnamento di cui alla Legge 17 luglio 1979 n.41 e successive modifiche ed alle graduatorie per l'accesso a posizioni presso l'UO Nido per l'Infanzia hanno l'obbligo di ricevere dati e documenti elettronici relativi al rapporto di lavoro pubblico, costituito o costituendo, mediante trasmissione a mezzo SERC o a mezzo posta elettronica ordinaria inviata a domicilio digitale che hanno, quindi, l'obbligo di eleggere.
7. L'obbligo di elezione del domicilio digitale di cui al comma 6 è assolto con le modalità di cui all'articolo 8 ovvero con modalità semplificate stabilite dalla DGFP, ferma restando, in quest'ultimo caso, la necessità di garantire, in caso di utilizzo di SERC, l'identificazione del corrispondente con un elevato livello di sicurezza tramite il suo riconoscimento *de visu* da parte di pubblico ufficiale oppure da altro pubblico impiegato autorizzato oppure tramite sottoscrizione di apposita istanza con firma elettronica qualificata. I soggetti di cui al comma 6 non sostengono nessun onere economico per l'assolvimento dell'obbligo previsto al predetto comma.
8. I soggetti di cui al comma 6 hanno facoltà di esercitare o meno l'opzione di cui all'articolo 8, comma 7. Nel caso in cui non eserciti alcuna delle predette due opzioni, il domicilio digitale di soggetto di cui al comma 6 potrà essere utilizzato unicamente per le comunicazioni relative al rapporto di lavoro pubblico, costituito o costituendo.

Art. 7
(Effetti giuridici dell'utilizzo della posta elettronica certificata - PEC nell'ordinamento sammarinese)

1. La trasmissione di documenti elettronici effettuata tramite PEC produce nell'ordinamento sammarinese gli effetti giuridici e probatori di cui all'articolo 5 nei seguenti casi:
a) la trasmissione sia effettuata esclusivamente fra soggetti privati, ambedue dotati di PEC, di cui uno dei corrispondenti sia residente, soggiornante o avente sede nella Repubblica di San Marino e l'altro sia residente, soggiornante o avente sede nel territorio della Repubblica Italiana;
b) la trasmissione sia effettuata fra soggetto residente, soggiornante o avente sede nel territorio della Repubblica Italiana tramite PEC e soggetto, pubblico o privato, residente o soggiornante o avente sede nella Repubblica di San Marino tramite SERC laddove tale trasmissione avvenga attraverso l'uso di un nodo di scambio che realizzi un'interoperabilità tecnica fra i due diversi servizi. Il livello di adeguatezza dell'interoperabilità tecnica realizzata dal predetto nodo dovrà essere preventivamente valutato e riconosciuto dall'Autorità ICT, fatta salva l'interoperabilità già riconosciuta in relazione al SERC in uso alla data di entrata in vigore del presente decreto delegato;
c) la trasmissione sia effettuata fra uffici ed organi dell'Amministrazione sammarinese, da una parte, e uffici ed organi delle Amministrazioni ed Enti Pubblici della Repubblica Italiana, dall'altra parte, ambedue dotati di PEC. La presente modalità di comunicazione telematica è subordinata ad autorizzazione della DGFP su richiesta motivata dell'ufficio od organo pubblico richiedente.
2. Le disposizioni di cui al comma 1 hanno valore transitorio sino al conseguimento della qualificazione, ai sensi dell'articolo 44 del Regolamento eIDAS da parte:
a) di SERC autorizzato nella Repubblica di San Marino, oppure;
b) della PEC.

SEZIONE II
DOMICILIO DIGITALE E REGISTRO PUBBLICO DEI DOMICILI DIGITALI

Art. 8
(Elezione di domicilio digitale)

1. Ai fini dell'elezione di domicilio digitale il soggetto privato, persona fisica o giuridica, operatore economico o non operatore, deve essere identificato. Il soggetto privato si intende identificato quando sussistano le seguenti condizioni cumulative:
a) il suo domicilio digitale sia contenuto nel RPDD;
b) il suo domicilio digitale, inserito nel RPDD, sia associato ai dati di identificazione personale tramite una dichiarazione sostitutiva di atto di notorietà di cui all'articolo 13 della Legge n.159/2011, sottoscritta dalla persona fisica o da un rappresentante autorizzato della persona giuridica, con la quale dichiari di eleggere domicilio digitale presso un indirizzo di posta elettronica nella propria disponibilità d'uso.
2. La presentazione della dichiarazione sostitutiva di cui al comma 1, lettera b), della dichiarazione sostitutiva di variazione delle informazioni relative al domicilio digitale originariamente fornite nonché della richiesta di cancellazione dal RPDD è esente da imposta di bollo e può avvenire esclusivamente:
a) presso gli sportelli di Poste San Marino S.p.A. ed eventuali altri soggetti autorizzati dal Congresso di Stato, tramite sottoscrizione autografa in calce alla dichiarazione stessa e previa identificazione *de visu* del dichiarante da parte dell'operatore di sportello e acquisizione di copia fotostatica del documento di identità in corso di validità, nel rispetto dell'articolo 11, comma 1, della Legge n. 159/2011;
b) tramite lo "sportello virtuale", messo a disposizione dall'Unità Organizzativa (in seguito brevemente UO) Informatica, Tecnologia, Dati e Statistica (in seguito brevemente UITDS), previa apposizione di firma elettronica qualificata in corso di validità del dichiarante.
3. La persona giuridica residente all'estero che elegga, in via volontaria, il proprio domicilio digitale nella Repubblica di San Marino nei termini e secondo le modalità di cui ai commi 1 e 2, è tenuta ad allegare i documenti comprovanti i poteri di rappresentanza mediante certificazione pubblica dell'autorità emittente, redatta in lingua italiana e munita di firma elettronica qualificata, oppure munita di un contrassegno tramite il quale sia possibile accedere al documento elettronico originale. Qualora la predetta documentazione sia già stata prodotta all'Amministrazione nell'ambito di altri procedimenti e sia ancora in corso di validità al momento della richiesta di elezione, ai sensi dell'articolo 4 della Legge n.159/2011, è sufficiente l'allegazione della dichiarazione sostitutiva di certificazione nella quale sia indicato anche l'ufficio dell'Amministrazione presso cui la stessa è stata prodotta.
4. La cancellazione del soggetto dal RPDD avviene su richiesta del soggetto interessato tramite la quale:
a) il soggetto manifesti la volontà di cancellare il proprio domicilio digitale dal RPDD;
b) il soggetto dichiari, tramite dichiarazione sostitutiva di atto di notorietà di cui all'articolo 13 della Legge n.159/2011, di non rientrare tra le categorie di soggetti per i quali è stabilito l'obbligo di registrazione di un proprio domicilio digitale.
5. L'avvenuta registrazione delle informazioni relative al domicilio digitale e delle loro successive variazioni nonché cancellazione è comunicata all'interessato dal soggetto gestore del RPDD di cui all'articolo 9, commi 4 e 5, tramite SERC inviato al medesimo domicilio digitale.
6. L'elezione del domicilio digitale, la sua variazione e cancellazione hanno effetto dalla data ed ora di completamento di tutte le attività di verifica tecnica dell'indirizzo di posta elettronica indicato e di perfezionamento della trasmissione di cui al comma 5. Fino a tale data ed ora restano validi e con pieno effetto giuridico i precedenti dati iscritti nel RPDD, se presenti.
7. All'atto dell'elezione del domicilio digitale, il soggetto privato, in possesso o meno di COE, è tenuto ad optare – mediante atto scritto o procedura software - per una delle due seguenti alternative:
a) il suo domicilio digitale sia reso ostensibile solo agli uffici ed organi dell'Amministrazione sammarinese. Con tale opzione, l'interessato esprime il proprio consenso a ricevere dall'Amministrazione documenti o atti amministrativi di proprio interesse mediante SERC e ha

facoltà di avvalersi della modalità di trasmissione per via telematica di documenti amministrativi elettronici all'Amministrazione, a mente dell'articolo 10, comma 3, della Legge n. 159/2011 e dell'articolo 10, comma 5, della Legge n. 160/2011;

b) il suo domicilio digitale sia reso ostensibile a tutti i soggetti iscritti nel RPDD. Tale opzione comporta, oltre a quanto previsto alla precedente lettera a), l'accettazione da parte dell'interessato della possibilità di ricevere, con gli effetti giuridici di cui all'articolo 4, la trasmissione di documenti elettronici da tutti i soggetti, pubblici e privati, iscritti nel RPDD.

8. L'opzione di cui al comma 7 originariamente espressa può essere variata dall'interessato con le medesime forme.

9. Ad un soggetto privato, persona fisica o giuridica, può corrispondere un solo domicilio digitale individuato con le modalità di cui al comma 2, ad esclusione del libero professionista nominato dal Tribunale quale liquidatore o curatore il quale può eleggere, previa richiesta inoltrata al gestore del RPDD, un unico domicilio digitale cui siano associate anche le persone fisiche e giuridiche in relazione alle quali la predetta nomina sia stata effettuata.

10. I domicili digitali utilizzati dall'Amministrazione e dai gestori di pubblici servizi sono individuati mediante pubblicazione nel RPDD. La trasmissione e ricezione di documenti amministrativi elettronici tramite SERC avviene avvalendosi esclusivamente di tali domicili digitali.

11. È obbligo del pubblico dipendente e dell'incaricato di pubblico servizio, all'atto di ogni invio e ricezione di documenti amministrativi elettronici mediante SERC verificare la rispondenza fra il corrispondente della trasmissione ed il domicilio digitale riportato nel RPDD.

12. Colui che elegge domicilio digitale con l'iscrizione nel RPDD non può opporre eccezioni relative all'uso o disponibilità dell'indirizzo di posta elettronica indicato quale domicilio digitale.

13. I domicili digitali presenti nel RPDD possono essere utilizzati anche per la trasmissione di documenti elettronici tramite servizi di posta elettronica ordinaria qualora il mittente, soggetto pubblico o privato, ritenga non necessaria l'acquisizione della certezza dell'invio e della consegna al destinatario con i connessi effetti giuridici di cui all'articolo 5; in tale caso di trasmissione a mezzo posta elettronica ordinaria, resta fermo, in ordine agli effetti giuridici del documento elettronico, quanto previsto dall'articolo 3 della Legge n.115/2005, come modificato dal successivo articolo 26, comma 2 e dal Decreto n.156/2005 e successive modifiche.

Art. 9

(Istituzione, tenuta e gestione operativa del Registro Pubblico dei Domicili Digitali)

1. È istituito il RPDD. Il RPDD può integrarsi con altri elenchi, anagrafi e registri già in uso presso l'Amministrazione.

2. Il RPDD è tenuto dall'UO UITDS. La tenuta del RPDD implica le seguenti attività:

a) sovraintendere alla realizzazione, allo sviluppo ed alla manutenzione della procedura software attraverso cui è gestito il RPDD;

b) sovraintendere alla realizzazione, allo sviluppo ed alla manutenzione delle interfacce e delle procedure di integrazione, di sincronizzazione e di consolidamento dei dati relativi ai domicili digitali contenuti in altri archivi o registri in uso presso l'Amministrazione;

c) sovraintendere alla predisposizione di canali di comunicazione sicuri atti alla trasmissione dei dati relativi ai domicili digitali;

d) predisporre l'accesso di terzi ai dati contenuti nel RPDD su autorizzazione del Direttore della Funzione Pubblica.

3. Il RPDD è reso accessibile secondo termini differenziati all'Amministrazione, alle persone pubbliche o private che erogano un pubblico servizio ed ai soggetti privati sulla base del livello di pubblicità del domicilio digitale autorizzato dal titolare del domicilio medesimo. In particolare, l'accesso a domicilio digitale iscritto nel RPDD può avvenire anche mediante l'utilizzo di accessi secondari autorizzati dal titolare del domicilio.

4. Il servizio di registrazione, variazione e cancellazione dei dati relativi ai domicili digitali dei Dipartimenti, UO, articolazioni organizzative del Settore Pubblico Allargato, organi istituzionali ed

amministrativi dello Stato, Corpi Militari e di Polizia autorizzati all'utilizzo del SERC è svolto dall'UO UITDS, utilizzando i dati in proprio possesso.
5. Il servizio di registrazione, variazione e cancellazione dei dati relativi ai domicili digitali di soggetti non rientranti fa quelli di cui al comma 4 è concesso, su decisione del Congresso di Stato, in tutto o in parte, in gestione ad Enti a partecipazione maggioritaria o totalitaria pubblica, secondo i termini definiti nel provvedimento di concessione.

CAPO III
NORME GENERALI PER LA PRESENTAZIONE DI ISTANZE E DOCUMENTI IN VIA TELEMATICA ALL'AMMINISTRAZIONE

SEZIONE I
NORME COMUNI

Art. 10
(Modalità generali e residuali di comunicazione in via telematica con l'Amministrazione)

1. La presentazione di domande, istanze, dichiarazioni e, in genere, documenti in via telematica all'Amministrazione avviene secondo le norme di cui al presente Capo e di cui al successivo Capo IV.
2. Le modalità di presentazione in via telematica di documenti amministrativi elettronici disciplinate nelle Sezioni II e III del presente Capo hanno valore generale, poiché applicabili per tutti i settori dell'Amministrazione, salvo espresse deroghe autorizzate dalla DGFP, e residuale, perché utilizzabili in assenza di specifiche disposizioni normative settoriali ovvero di specifici programmi applicativi.
3. La disposizione di cui all'articolo 11, comma 2 della Legge n.159/2011 relativa all'obbligo di spedizione delle istanze e delle dichiarazioni unitamente alla copia fotostatica non autenticata di un documento di identità dell'interessato da questi sottoscritta e dichiarata come conforme all'originale, contenente la dichiarazione di cui al comma 2 dell'articolo 9 della medesima legge, non si applica alla trasmissione all'Amministrazione di documenti elettronici ai sensi delle successive Sezioni II e III del presente Capo.
4. Le disposizioni di cui alla Sezione III del presente Capo sono dettate al fine di elevare significativamente il grado di certezza che l'identità rivendicata dal richiedente l'accesso ai servizi in linea del Portale della Pubblica Amministrazione sia la sua vera identità, tramite l'introduzione dell'utilizzo di un secondo fattore di autenticazione.

SEZIONE II
PRESENTAZIONE DI ISTANZE E DOCUMENTI TRAMITE SERC

Art.11
(Presentazione di documenti elettronici all'Amministrazione da parte di non operatori economici)

1. Le domande, istanze, dichiarazioni e, in genere, documenti presentati da cittadino o residente o soggiornante in Repubblica, che non sia in possesso di COE, si ritengono valide e rilevanti a tutti gli effetti di legge nonché validamente trasmesse ad un ufficio dell'Amministrazione o ad un gestore di pubblico servizio se formate quale documento amministrativo elettronico ed inoltrate a mezzo SERC. Qualora il documento amministrativo elettronico abbia la forma della copia per immagine su supporto elettronico di documento analogico sottoscritto con firma autografa non sussiste la necessità di fare pervenire l'originale analogico, salvo che l'ufficio o organo ricevente lo richieda motivando tale determinazione.

Art. 12
(Presentazione di documenti elettronici all'Amministrazione da parte di operatori economici)

1. Le domande, istanze, dichiarazioni e, in genere, documenti presentati da operatori economici sammarinesi ed esteri iscritti nel RPDD possono essere trasmesse dagli stessi all'Amministrazione o ad un gestore di pubblico servizio nella forma del documento amministrativo elettronico sottoscritto con firma elettronica qualificata inoltrato a mezzo SERC al domicilio digitale dell'ufficio, organo o gestore competente. Le domande, istanze e dichiarazioni formate ed inoltrate in conformità al precedente periodo si ritengono valide e rilevanti a tutti gli effetti di legge nonché validamente presentate e trasmesse.
2. I documenti amministrativi elettronici costituenti allegati alla domanda od istanza principale sono validamente presentati e trasmessi senza necessità di fare pervenire l'originale analogico, salvo che l'ufficio o organo ricevente lo richieda motivando tale determinazione.

SEZIONE III
PRESENTAZIONE DI ISTANZE E DOCUMENTI TRAMITE IL PORTALE DELLA PUBBLICA AMMINISTRAZIONE E L'IMPLEMENTAZIONE DEL PROGETTO "SAN MARINO CARD"

Art. 13
(Implementazione del progetto San Marino Card)

1. Il progetto San Marino Card (in seguito brevemente SMaC Card) di cui al Decreto Delegato 15 settembre 2022 n.130 è implementato - oltre che ai fini di incentivazione dei consumi interni, di promozione turistica, di carta di pagamento interna alla Repubblica di San Marino e di certificazione telematica dei ricavi - quale strumento di autenticazione rafforzata per l'utilizzo dei servizi in linea del Portale della Pubblica Amministrazione.
2. L'autenticazione rafforzata di cui al comma 1 è funzionale a consentire alla persona fisica titolare di SMaC Card di utilizzare i moduli ed i formulari elettronici disponibili tramite le funzioni dei servizi in linea contenuti nel Portale della Pubblica Amministrazione, quale mezzo di presentazione in via telematica di istanze, domande, dichiarazioni e, in generale, documenti all'Amministrazione, con la validità ed efficacia probatoria di cui all'articolo 14.
3. L'associazione, in maniera certa, dell'utenza radiomobile alla persona fisica avviene all'atto del rilascio della SMaC Card da parte dei soggetti autorizzati di cui all'articolo 5, comma 8 del Decreto Delegato n.130/2022 i quali curano l'acquisizione, da parte delle persone fisiche richiedenti la SMaC Card, di dichiarazione sostitutiva di atto di notorietà di cui all'articolo 13 della Legge n.159/2011 tramite la quale il numero dell'utenza radiomobile sia associato al richiedente la cui identità è accertata *de visu* e con la presentazione di documento d'identità.
4. Il soggetto autorizzato acquisisce, inoltre, il consenso del richiedente la SMaC Card a che l'Amministrazione utilizzi i dati personali di quest'ultimo per le finalità di cui alla presente Sezione nonché secondo i termini previsti dall'articolo 91 della Legge 21 dicembre 2018 n.171.

Art. 14
(Validità ed efficacia probatoria di documenti elettronici inviati all'Amministrazione tramite il Portale della Pubblica Amministrazione)

1. In attuazione dell'articolo 2, comma 3, della Legge n.115/2005 ed ai sensi dell'articolo 3-bis, comma 1, lettera c) del Decreto Delegato n.156/2015 e successive modifiche, il presente articolo stabilisce le modalità di formazione, di sottoscrizione e di invio dei moduli e dei formulari elettronici aventi piena validità e rilevanza ad ogni effetto di legge nonché validamente presentati e trasmessi ad un ufficio o organo dell'Amministrazione tramite l'utilizzo delle funzioni dei servizi in

linea contenuti nel Portale della Pubblica Amministrazione.

2. I moduli ed i formulari dei servizi in linea di cui al comma 1 producono documenti amministrativi elettronici che soddisfano il requisito della forma scritta ed hanno il medesimo valore probatorio di un documento sottoscritto con firma autografa quando siano tutte soddisfatte le seguenti condizioni:

a) l'autore componga il modulo o formulario elettronico attraverso un servizio in linea dell'Amministrazione;
b) il servizio in linea formi, su richiesta dell'autore, un documento amministrativo elettronico avente gli stessi contenuti del modulo o formulario e lo mostri per intero all'autore;
c) l'autore, tramite azione esplicita e volontaria, confermi:
   1) di avere preso piena conoscenza del contenuto del documento elettronico stesso;
   2) la sua piena volontà di volere convalidare il documento elettronico;
d) l'autore sia univocamente individuato tramite procedura software di autenticazione rafforzata sul servizio in linea. Tale univoca individuazione dell'autore assume valore di sottoscrizione;
e) il servizio in linea dell'Amministrazione generi almeno i seguenti dati:
   1) la data e l'ora del completamento della procedura software di autenticazione rafforzata, attestata dal servizio in linea. La data e l'ora di sistema dell'applicativo fanno fede nei confronti dell'Amministrazione ai fini del rispetto dei termini eventualmente previsti dalla pertinente normativa per la presentazione del documento amministrativo nonché dell'osservanza dei termini stabiliti per l'adozione del provvedimento finale;;
   2) il nome, il cognome ed il codice ISS dell'autore;
   3) il numero progressivo di registrazione del documento amministrativo;
   4) l'identificativo della sessione di autenticazione dell'utente nel servizio in linea;
   5) il nome del servizio in linea che ha generato il documento amministrativo elettronico convalidato;
f) il servizio in linea dell'Amministrazione renda disponibile all'autore un duplicato elettronico del documento amministrativo finale, completo di dati di firma e di sigillo elettronico qualificato, contestualmente al suo invio.

3. Contestualmente all'atto della sottoscrizione effettuata a mente del comma 2, lettera d), al documento amministrativo elettronico sono acclusi i dati di cui al comma 2, lettera e) ed è apposto un sigillo elettronico qualificato intestato all'Amministrazione.

4. La sottoscrizione effettuata a mente del comma 2, lettera d), comporta il contestuale invio all'Amministrazione del documento amministrativo elettronico, completo di dati di firma e di sigillo elettronico qualificato.

5. L'Amministrazione tratta il documento amministrativo elettronico così ricevuto in conformità alle norme contenute nella Legge 11 maggio 2012 n.50 e successive modifiche ed alle successive norme di attuazione.

Art. 14 *bis*

(Rilascio di atti o provvedimenti in esito ad istanze presentate con moduli e formulari dei servizi in linea tramite il Portale della Pubblica Amministrazione)

1. La trasmissione all'autore del modulo o formulario elettronico di cui all'articolo 14, degli eventuali atti endoprocedimentali nonché del provvedimento finale avviene, a cura dell'UO competente, attraverso l'inoltro all'interessato, tramite posta elettronica ordinaria, di una o più comunicazioni contenenti le indicazioni per accedere all'indirizzo web da cui poter scaricare i suddetti atti e provvedimenti.

2. L'invio della comunicazione di cui al comma 1 è effettuato al domicilio digitale dell'autore del modulo o formulario elettronico, qualora lo stesso ne sia dotato, oppure, in assenza del suddetto domicilio digitale, all'indirizzo di posta elettronica ordinaria fornito dall'autore medesimo all'atto della sua registrazione nel Portale della Pubblica Amministrazione.

3. La data e l'ora di sistema dell'applicativo, generata al momento dello scarico dell'atto o provvedimento, così come attestata dal servizio in linea, costituisce la data di ritiro dell'atto o

provvedimento medesimo dalla quale decorrono i termini per l'ottemperanza a quanto eventualmente richiesto dall'UO competente nonché, in caso di provvedimento finale, per l'eventuale impugnazione in sede amministrativa e giurisdizionale.

CAPO IV
NORME PER LA PRESENTAZIONE DI ISTANZE E DOCUMENTI IN VIA TELEMATICA RELATIVAMENTE A SPECIFICI SETTORI DELL'AMMINISTRAZIONE

SEZIONE I
NORME RELATIVE ALLA PRESENTAZIONE DI ISTANZE E DOCUMENTI NEGLI AMBITI EDILIZIO, STRUTTURALE, DELLA PREVENZIONE INCENDI, DELL'EFFICIENTAMENTO ENERGETICO E DELLE ENERGIE RINNOVABILI, AMBIENTALE, CATASTALE, AGRICOLO ED URBANISTICO

Art. 15
(Presentazione delle istanze in via telematica)

1. Le istanze e relativi documenti a corredo nonché le comunicazioni (di seguito, cumulativamente, indicati con il termine "istanze") relative ai sotto elencati ambiti e settori dell'attività amministrativa afferenti al Dipartimento Territorio e Ambiente possono essere facoltativamente presentate alle competenti UO in via telematica mediante il programma applicativo denominato "Gestione Elettronica dei Documenti Informatici" (in seguito brevemente GEDI), accessibili dal Portale della Pubblica Amministrazione, previa richiesta di abilitazione:
a) edilizio;
b) strutturale;
c) della prevenzione incendi;
d) dell'efficientamento energetico e delle energie rinnovabili;
e) ambientale.
2. La decorrenza della possibilità di presentazione delle istanze negli ambiti e settori dell'attività amministrativa di cui al comma 1 tramite il programma applicativo GEDI è stabilita, in ragione della progressiva implementazione del suddetto programma, tramite direttiva della DGFP. Sino all'avvio dell'utilizzo del programma applicativo GEDI non è consentita la presentazione, in via telematica, all' UO Ufficio Pianificazione Territoriale e per l'Edilizia (in seguito brevemente UPTE) di istanze volte all'ottenimento di titoli abilitativi all'esecuzione di interventi edilizi tramite le forme di cui al Capo III.
3. A decorre dall'1 settembre 2023, le istanze e relativi documenti a corredo in ambito catastale sono obbligatoriamente presentate all'UO Ufficio Tecnico del Catasto e Cartografia (in seguito brevemente UTCC) mediante i programmi applicativi denominati "Gestione Richieste Aggiornamento Terreni" (in seguito brevemente GRAT) e "Gestione Richieste Aggiornamento Fabbricati" (in seguito brevemente GRAF) accessibili dal Portale della Pubblica Amministrazione, previa richiesta di abilitazione a "Servizi catastali - aggiornamento catastale".
4. La disciplina delle modalità di presentazione in via telematica di pratiche urbanistiche, di pratiche relative al settore agricolo e di pratiche destinate a commissioni e collegi aventi competenza negli ambiti e settori dell'attività amministrativa di cui al comma 1 è stabilita tramite successiva integrazione al presente decreto delegato.
5. Le istanze si ritengono ad ogni effetto validamente presentate qualora trasmesse alle competenti UO UPTE, UTCC, Servizio Protezione Civile (in seguito brevemente SPC) e Ufficio Prevenzione Ambiente e Vigilanza del Territorio (in seguito brevemente UPAV) con le modalità di cui ai successivi articoli della presente Sezione.
6. I diritti di pratica stabiliti per la presentazione delle istanze sono significativamente

differenziati a seconda che i documenti siano presentati in forma elettronica oppure analogica e, in quest'ultimo caso, a seconda della voluminosità. Qualora la pratica non possa essere presentata in forma elettronica per giustificati motivi legati a malfunzionamenti di sistemi informatici o all'eccessiva dimensione dei file si applicano specifici diritti di pratica.

Art. 16

(Sottoscrizione delle istanze presentate tramite GEDI, GRAT e GRAF)

1. Le istanze negli ambiti e settori dell'attività amministrativa di cui all'articolo 15, comma 1 nonché in ambito catastale presentate in via telematica possono essere sottoscritte da parte del solo tecnico abilitato e sotto l'esclusiva responsabilità di quest'ultimo; ciò anche a modifica di quanto previsto dalla Legge 14 dicembre 2017 n.140 e successive modifiche, dalla Legge 23 gennaio 2015 n.2, dalla Legge 25 gennaio 2011 n.5, dal Decreto Delegato 24 febbraio 2016 n.18 e successive modifiche e relativo *errata corrige*, nonché dalle norme speciali in materia di sanatoria edilizia straordinaria.
2. Nel caso di sottoscrizione da parte del solo tecnico abilitato, è onere di quest'ultimo acquisire dal proprietario o concessionario o titolare del diritto di superficie sull'immobile o loro delegati l'atto di procura speciale di delega per la sottoscrizione digitale e per la presentazione telematica delle istanze. Tale atto è conservato sotto la cura e responsabilità del tecnico incaricato.

Art. 17

(Disposizioni comuni per la presentazione delle istanze tramite GEDI)

1. Il programma applicativo GEDI prevede l'effettuazione, da parte dell'istante abilitato e legittimato alla presentazione, di richiesta preliminare di prenotazione dell'istanza che si intende avanzare. La richiesta di prenotazione dell'istanza effettuata secondo i termini previsti ai commi 2 e 3 diviene presentazione effettiva solo a seguito dell'esecuzione delle operazioni indicate al comma 5.
2. L'istanza è sottoscritta dall'uno o più soggetti abilitati e legittimati alla presentazione sotto l'esclusiva responsabilità di questi ultimi, nella forma del documento amministrativo elettronico sottoscritto con firma elettronica qualificata. Qualora l'istanza sia presentata da tecnico abilitato, la stessa è sottoscritta con firma elettronica qualificata contenente la specifica qualifica professionale del titolare.
3. L'inserimento dell'istanza, ivi compresi i pareri ed autorizzazioni previsti dall'articolo 57, comma 9 della Legge n.140/2017 e quelli di competenza di altre UO od organi, avviene con le seguenti modalità:
   a) inserimento diretto dei dati generali della richiesta;
   b) compilazione dei dati tecnici;
   c) caricamento dei documenti amministrativi elettronici a corredo dell'istanza previsti dalle pertinenti normative. I suddetti documenti a corredo, sottoscritti anch'essi con firma elettronica qualificata del soggetto, pubblico o privato, emittente, sono caricati in formato PDF/A. In relazione alle pratiche di competenza dell'UO SPC non è necessario il caricamento del progetto architettonico in quanto tale documento è già acquisito internamente e, quindi, consultabile dall'UO medesima tramite il programma applicativo GEDI.
4. L'UO UPTE, l'UO SPC e l'UO UPAV, ciascuno in relazione all'ambito e settore amministrativo di competenza, a seguito della prenotazione di cui ai superiori commi, controllano la completezza dei dati e dei documenti inseriti e, in caso di esito positivo, richiedono il pagamento dei diritti di pratica.
5. L'assegnazione del protocollo al documento amministrativo elettronico formato secondo quanto stabilito dai superiori commi e l'invio al soggetto abilitato e legittimato alla presentazione dell'istanza della ricevuta di avvenuto deposito dell'istanza avviene a seguito del pagamento dei diritti di pratica e della trasmissione in formato elettronico, tramite il programma applicativo GEDI, della ricevuta di pagamento.

Art.18

(Sospensione della pratica ed integrazione della documentazione)

1. Qualora la pratica sia sospesa da parte dell'istruttore designato per esigenze di integrazione documentale, il soggetto abilitato e legittimato alla presentazione dell'istanza provvede a trasmettere le integrazioni richieste in formato elettronico tramite il programma applicativo GEDI.
2. La documentazione elettronica integrativa di cui al comma 1 è accompagnata da relazione con cui si riscontrino i profili e motivi di sospensione evidenziati nella comunicazione dell'UO.

Art. 19

(Irricevibilità delle istanze presentate tramite GEDI)

1. Sono irricevibili e archiviate d'ufficio le istanze inoltrate in formato elettronico tramite il programma applicativo GEDI in caso di:
1) documentazione non sottoscritta con firma elettronica qualificata oppure sottoscritta con firma elettronica non valida. Nel caso l'istanza sia presentata da tecnico abilitato, la stessa è irricevibile qualora la documentazione non sia sottoscritta con firma elettronica qualificata contenente la specifica qualifica professionale del titolare;
2) documentazione salvata in formati elettronici non ammessi;
3) mancanza dell'atto di procura speciale di delega, laddove necessario ai sensi dell'articolo 16, comma 2;
4) assenza di documentazione obbligatoria ai sensi dell'articolo 17, comma 3, lettera c);
5) utilizzo di COE cessato, sospeso o, comunque, non attivo;
6) qualora la rilevanza delle omissioni sia tale da non consentire la completa identificazione dell'intervento, dell'immobile o di altri elementi essenziali all'istruttoria della pratica.
2. Nel caso in cui l'istanza, ai sensi del comma 1, sia dichiarata irricevibile la stessa potrà essere presentata nuovamente.

Art. 20

(Rilascio del provvedimento in esito a pratiche presentate tramite GEDI e conservazione nel tempo dei documenti digitali)

1. All'atto del rilascio dei provvedimenti finali di rispettiva competenza, l'UO UPTE, l'UO SPC e l'UO UPAV appongono una marca temporale qualificata volta ad estendere la validità temporale del documento amministrativo elettronico per un periodo di venti anni; qualora il provvedimento finale comprenda elaborati grafici approvati, la marca temporale è apposta anche su questi ultimi.
2. Il rilascio da parte dell'UO UPTE, dell'UO SPC e dell'UO UPAV, in favore dell'uno o più soggetti abilitati e legittimati alla presentazione dell'istanza, dei documenti amministrativi elettronici di cui al comma 1 avviene attraverso l'invio all'interessato, tramite SERC, di una comunicazione contenente le indicazioni per accedere all'indirizzo web da cui poter scaricare i suddetti provvedimenti e gli eventuali elaborati grafici approvati muniti di marca temporale.
3. Per quanto concerne i provvedimenti finali consistenti in titoli abilitativi all'esecuzione di interventi edilizi, la data dell'atto di scarico del provvedimento costituisce la data di ritiro della concessione od autorizzazione edilizia ai sensi dell'articolo 61 della Legge n.140/2017 e, pertanto, deve avvenire entro un anno dal ricevimento della comunicazione di cui al comma 2.
4. L'Amministrazione garantisce nel tempo la conservazione dei propri documenti digitali tramite il predetto programma applicativo GEDI secondo parametri di integrità e autenticità, governo e controllo degli accessi ed audit trail conformi alle raccomandazioni ed alle linee guida internazionali, senza ricorrere a processi di conservazione sostitutiva.

Art. 21

(Disposizioni in merito alla presentazione delle denunce di

variazione catastale tramite GRAT e GRAF)

1. Le denunce di variazione catastale, sia a Catasto Terreni che Catasto Fabbricati, sono presentate esclusivamente attraverso i programmi applicativi GRAT e GRAF.
2. La procedura telematica per le variazioni catastali si articola secondo le seguenti fasi:

a) variazioni a Catasto Fabbricati tramite programma applicativo GRAF:
   1) richiesta telematica della documentazione da parte del tecnico abilitato;
   2) invio da parte dell'UTCC della documentazione elettronica necessaria per la lavorazione della pratica ed attivazione delle maschere di compilazione nell'applicativo;
   3) compilazione, da parte del tecnico abilitato, delle schede in GRAF (elenco vani e unità immobiliari, accessori comuni e scheda fabbricato ove applicabile) e preparazione del disegno planimetrico in formato vettoriale;
   4) convalida delle schede attraverso specifica funzione del programma applicativo che rende immodificabili i documenti compilati dal tecnico abilitato, riproducendone il contenuto in documenti PDF/A con data e codice identificativo univoco;
   5) sottoscrizione, da parte del tecnico abilitato, di tutti i documenti elettronici con firma elettronica qualificata;
   6) pagamento dei diritti dovuti attraverso le modalità definite dall'Amministrazione;
   7) caricamento dei *file* firmati nel programma applicativo ed invio della pratica;
   8) l'UO UTCC, verificata la completezza della pratica presentata, assegna un numero di protocollo e, attraverso il programma applicativo, comunica al tecnico abilitato l'avvio del procedimento amministrativo anche ai fini della decorrenza dei termini previsti dalla normativa di riferimento;

b) variazioni a Catasto Terreni tramite programma applicativo GRAT:
   1) richiesta telematica della documentazione da parte del tecnico abilitato;
   2) invio, da parte dell'UO UTCC, della documentazione elettronica necessaria per la lavorazione della pratica;
   3) compilazione, da parte del tecnico abilitato, delle schede e del materiale inviato (elaborati grafici con oggetto del rilievo e schema rilievo, risultato del frazionamento, libretto delle misure, scheda delle monografie) e preparazione del disegno planimetrico in formato vettoriale;
   4) sottoscrizione, da parte del tecnico abilitato, di tutti i documenti elettronici con firma elettronica qualificata;
   5) pagamento dei diritti dovuti attraverso le modalità definite dall'Amministrazione;
   6) caricamento dei *file* firmati nel programma applicativo ed invio della pratica;
   7) l'UO UTCC, verificata la completezza della pratica presentata, assegna un numero di protocollo e attraverso il programma applicativo, comunica al tecnico abilitato l'avvio del procedimento amministrativo, anche ai fini della decorrenza dei termini previsti dalla normativa di riferimento.

3. Le eventuali sospensioni del procedimento amministrativo sono comunicate al tecnico abilitato attraverso i predetti programmi applicativi.
4. L'esito del procedimento amministrativo è comunicato al tecnico abilitato attraverso il programma applicativo e, limitatamente alle variazioni che incidono sulla rendita catastale, alla proprietà con raccomandata con ricevuta di ritorno ovvero con SERC; la notifica alla proprietà è effettuata ai fini dell'eventuale ricorso alla Commissione Censuaria Permanente.
5. Le modalità tecnico-operative di dettaglio che regolano le procedure telematiche di variazione catastale restano disciplinate, sino alla loro modifica ai sensi di quanto previsto dall'articolo 22, dalle vigenti circolari dell'UO UTCC nonché, per quanto riguarda il Catasto Terreni, anche dal Regolamento 27 novembre 2015 n.15.

Art. 22

(Circolari applicative e norme comuni)

1. L’UO UPTE, l’UO UTCC, l’UO SPC e l’UO UPAV emettono, sentita l’Autorità ICT, direttive e/o circolari al fine di fornire indirizzi e dettagliare ulteriormente le modalità applicative per la presentazione delle pratiche di rispettiva competenza in formato elettronico.
2. Tramite circolare del Direttore del Dipartimento Territorio e Ambiente può essere adottato un modello di procura speciale di delega.
3. La disposizione di cui all’articolo 11, comma 2 della Legge n.159/2011 relativa all’obbligo di spedizione delle istanze e delle dichiarazioni unitamente alla copia fotostatica non autenticata di un documento di identità dell’interessato da questi sottoscritta e dichiarata come conforme all’originale, contenente la dichiarazione di cui al comma 2 dell’articolo 9 della medesima legge, non si applica alla trasmissione all’Amministrazione di documenti elettronici ai sensi della presente Sezione.

SEZIONE II
NORME IN MATERIA DI APPALTI E CONTRATTI PUBBLICI

Art. 23
(Norme per la presentazione di offerte in via telematica negli appalti e contratti pubblici)

1. La presentazione delle offerte in via telematica da parte di operatori economici sammarinesi ed esteri avviene:
a) in relazione a sistemi competitivi di scelta del contraente in materia di appalti pubblici di lavori, servizi e forniture complementari alle opere pubbliche, di cui all’articolo 10 del Decreto 20 gennaio 2000 n.10: secondo quanto previsto dall’articolo 12, le cui disposizioni superano, con riferimento alla suddetta specifica modalità di formazione e trasmissione dell’offerta, quanto previsto dagli articoli 26, 27 e 28 del predetto Decreto n.10/2000;
b) in relazione a sistemi competitivi di scelta del contraente ed a procedure speciali competitive in materia di contratti di fornitura o somministrazione di beni o servizi della Pubblica Amministrazione e degli Enti Pubblici, di cui rispettivamente all’articolo 12 ed al Capo III del Decreto Delegato 2 marzo 2015 n.26 e successive modifiche: secondo quanto previsto dall’articolo 12, le cui disposizioni superano, con riferimento alla suddetta specifica modalità di formazione e trasmissione dell’offerta, quanto previsto dagli articoli 14 e 15 del Regolamento 7 marzo 2019 n.3.

2. Qualora l’impresa partecipante presenti, in via facoltativa od obbligatoria sulla base di quanto previsto dai documenti di gara, la propria offerta in via telematica al domicilio digitale della Stazione Appaltante, le disposizioni relative alle modalità di trasmissione ed ai termini di apertura delle offerte di cui ai successivi commi superano:
a) in materia di appalti pubblici di lavori, servizi e forniture complementari alle opere pubbliche: quelle di cui agli articoli 26 e 28 del Decreto n.10/2000;
b) in materia di contratti di fornitura o somministrazione di beni o servizi della Pubblica Amministrazione e degli Enti Pubblici: quelle di cui all’articolo 16 del Regolamento n.3/2019 mentre non si applicano quelle previste dall’articolo 17, comma 1, lettera c) e comma 2, lettera b) del medesimo Regolamento.

3. Qualora l’offerta sia presentata in via telematica, la cauzione provvisoria è presentata mediante scansione dell’originale analogico ovvero in formato digitale con firma elettronica qualificata dell’ente emittente.
4. In caso di presentazione di offerta in via telematica nell’ambito di gara che preveda quale criterio di aggiudicazione quello dell’offerta economicamente più vantaggiosa, l’impresa partecipante effettua contestualmente due distinte trasmissioni, tramite SERC, in relazione ai seguenti documenti elettronici:
a) una relativa alla documentazione amministrativa indicata nel bando o nella lettera d’invito o nella richiesta di preventivo ed all’offerta tecnica;
b) l’altra relativa al deposito cauzionale provvisorio ed all’offerta economica.

5. In linea con quanto previsto dall'articolo 12, sono sottoscritti con firma elettronica qualificata apposta in modalità Cades o Pades o Xades, a pena di esclusione dalla valutazione dell'offerta, unicamente i seguenti documenti:

a) documento elettronico ove sia espressa la volontà dell'impresa di partecipazione alla gara;
b) dichiarazione con cui l'impresa si impegna a mantenere ferma ed irrevocabile l'offerta presentata fino al termine richiesto dalla Stazione Appaltante e dichiara di non essere né controllata né collegata ad altre imprese concorrenti alla gara;
c) offerta tecnica;
d) offerta economica;
e) eventuali dichiarazioni sostitutive di certificazione e/o di atto di notorietà;
f) eventuali copie di cui all'articolo 21 della Legge 5 ottobre 2011 n.159. In tali casi l'apposizione della firma elettronica qualificata sul documento scansionato produce gli effetti e determina, in capo al sottoscrittore, le responsabilità di cui al medesimo articolo 21 ed all'articolo 24 della Legge n.159/2011.

6. Le Stazioni Appaltanti sono dotate di specifico domicilio digitale dedicato alla gestione in via telematica dei procedimenti di gara e delle trattative.

7. Il deposito presso la Stazione Appaltante di offerta presentata tramite SERC si considera effettuato alla data ed ora individuate nella ricevuta di accettazione generata dal SERC medesimo, senza necessità che la Stazione Appaltante produca alcuna ulteriore attestazione di avvenuto deposito.

8. Qualora il SERC generi un certificato postale forense di mancata consegna o altra anomalia per cause non dipendenti dall'impresa offerente, il deposito tramite SERC deve essere ripetuto tempestivamente con il medesimo contenuto, allegando la ricevuta ed il certificato postale forense relativi alla precedente trasmissione; ciò anche allo scopo di provare la non imputabilità all'impresa offerente dell'eventuale mancato rispetto delle scadenze previste, con conseguente rimessione in termini dell'impresa stessa.

9. I documenti elettronici costituenti l'offerta sono depositati nel formato PDF/A oppure in altri formati di cui all'Allegato 1 al Decreto Delegato 30 gennaio 2020 n.9 stabiliti dalla Stazione Appaltante la quale potrà anche individuarne di ulteriori ai sensi dell'articolo 3 *bis,* comma 13, del Decreto 8 novembre 2005 n.156 e successive modifiche.

10. Allo scopo di assicurare il rispetto dei principi di segretezza ed integrità della documentazione relativa alla partecipazione alla gara, le offerte pervenute in via telematica tramite SERC non sono ritirate dalla Stazione Appaltante sino al termine di scadenza per la presentazione delle stesse previsto dai documenti di gara.

11. Decorso il termine di scadenza per la presentazione delle offerte nell'ambito di gare effettuate con il sistema dell'asta pubblica, dell'appalto concorso e della licitazione privata, le offerte pervenute nei termini sono ritirate in seduta pubblica dalla Stazione Appaltante alla presenza della Commissione, ove prevista. Delle operazioni di ritiro della Raccomandata Elettronica (in seguito brevemente RE) è data piena visibilità ai presenti anche, se richiesto, tramite la proiezione dello schermo del personal computer utilizzato per le operazioni. Qualora la gara preveda quale criterio di aggiudicazione quello dell'offerta economicamente più vantaggiosa, la Stazione Appaltante procede dapprima al ritiro della RE relativa ai documenti di cui al superiore comma 4, lettera a) e, solo a seguito dell'ultimazione della valutazione dell'offerta tecnica, al ritiro della RE relativa ai documenti di cui al superiore comma 4, lettera b).

12. I documenti di gara predisposti dalla Stazione Appaltante indicano, oltre al termine finale di scadenza per la presentazione delle offerte, anche il termine iniziale successivamente al quale le offerte possano essere presentate, specificando le conseguenze del mancato rispetto dello stesso; ciò allo scopo di evitare periodi di giacenza delle RE nella casella di posta elettronica della Stazione Appaltante superiori, ordinariamente, ai trenta giorni.

13. La trasmissione delle comunicazioni della Stazione Appaltante alle imprese partecipanti ed all'impresa appaltatrice iscritte nel RPDD, sia nei casi in cui l'offerta sia stata presentata dall'impresa interessata in via telematica sia nei casi in cui sia stata presentata con le ordinarie modalità, è effettuata a mezzo SERC. Tale modalità di trasmissione è osservata dalle Stazioni

Appaltanti anche per l'invio alle imprese iscritte nel RPDD di tutti i provvedimenti relativi alla gara che sono sottoscritti dal funzionario incaricato con firma elettronica qualificata.

14. Le imprese partecipanti e l'impresa appaltatrice iscritte nel RPDD, sia nei casi in cui l'offerta sia stata presentata dall'impresa interessata in via telematica sia nei casi in cui sia stata presentata con le ordinarie modalità, hanno facoltà di comunicare con la Stazione Appaltante a mezzo SERC.

15. La presentazione delle offerte in via telematica in relazione a procedimenti di tipo non competitivo volti all'aggiudicazione di appalti pubblici di lavori, servizi e forniture complementari alle opere pubbliche ed all'aggiudicazione di fornitura o somministrazione di beni o servizi può avvenire anche tramite inoltro, a mezzo posta elettronica ordinaria o PEC, di documento elettronico consistente in copia per immagine su supporto elettronico di documento analogico, senza necessità di fare pervenire l'originale analogico, salvo che la Stazione Appaltante lo richieda motivando tale determinazione.

16. La disposizione di cui all'articolo 11, comma 2 della Legge n.159/2011 relativa all'obbligo di spedizione delle istanze e delle dichiarazioni unitamente alla copia fotostatica non autenticata di un documento di identità dell'interessato da questi sottoscritta e dichiarata come conforme all'originale, contenente la dichiarazione di cui al comma 2 dell'articolo 9 della medesima legge, non si applica alla trasmissione all'Amministrazione di documenti elettronici ai sensi del presente articolo.

SEZIONE III
NORME IN MATERIA DI SPECIFICI PROGRAMMI APPLICATIVI

Art. 24
(Presentazione di documenti amministrativi tramite specifici programmi applicativi - Rinvio)

1. E' fatto salvo quanto previsto da fonti normative di rango primario e secondario che disciplinino l'utilizzo di programmi applicativi per la presentazione, deposito e gestione dei documenti amministrativi. In questo senso si richiamano le seguenti norme speciali relative a specifici programmi applicativi:

a) Decreto Legge 28 aprile 2011 n.69 ed articolo 87 della Legge 16 dicembre 2013 n.166 relativo al programma applicativo denominato "Tribweb";
b) Regolamento 1 febbraio 2016 n.1, relativo al programma applicativo denominato "Repe";
c) Decreto Delegato 5 dicembre 2017 n.137 e successive modifiche, relativo al programma applicativo denominato "Labor".

2. In relazione a programmi applicativi che non siano disciplinati da fonti di rango primario o secondario speciali e le cui caratteristiche non siano conformi alle norme di cui al Capo III, il valore giuridico e probatorio delle istanze e dichiarazioni prodotte nella forma del documento elettronico resta disciplinato, a seconda del tipo di firma elettronica apposta, dall'articolo 3 della Legge n.115/2005 e successive modifiche, precisando come i documenti elettronici formati, acquisiti e gestiti da programmi applicativi in uso nell'Amministrazione che non prevedano l'utilizzo della firma elettronica qualificata bensì di firma elettronica semplice o avanzata, abbiano il valore giuridico e probatorio di cui all'articolo 3, comma 4 della predetta Legge n.115/2005 e, pertanto, siano liberamente valutabili in giudizio in relazione alle loro caratteristiche di sicurezza, integrità ed immodificabilità.

3. In relazione al valore probatorio della scansione di documento analogico si rinvia all'articolo 85-*ter* del Decreto n.156/2005 e successive modifiche.

CAPO V
CERTIFICAZIONI ELETTRONICHE

Art.25
(Certificazioni formate da sistemi informatici o telematici e copie analogiche di documenti amministrativi elettronici)

1. Nell'ambito dell'Amministrazione l'emanazione di certificazioni attraverso sistemi informatici o telematici, devono essere accompagnate dall'indicazione della fonte e del responsabile dell'emanazione. L'apposizione di firma autografa sulla predetta certificazione è sostituita dall'indicazione a stampa, sul documento prodotto dal sistema automatizzato, del nominativo del soggetto responsabile.
2. La certificazione formata ai sensi del comma 1 è trasmessa al domicilio digitale del soggetto richiedente oppure resa scaricabile direttamente dal Portale della Pubblica Amministrazione, previa autenticazione rafforzata del soggetto richiedente.
3. Sulle copie analogiche dei documenti amministrativi elettronici può, inoltre, essere apposto a stampa un contrassegno, sulla base dei criteri definiti dalla specifica tecnica EN ISO/IEC 18004:2015, tramite il quale sia possibile verificare l'autenticità del documento.
4. L'applicazione delle norme di cui al presente Capo decorre dalla data indicata con delibera del Congresso di Stato, tenendo conto dei tempi necessari all'esecuzione dei necessari adeguamenti informatici.

CAPO VI
NORME FINALI

Art. 26
(Norme di coordinamento e abrogazioni)

1. L'espressione "con le modalità e le forme di cui all'articolo 3 della Legge 20 luglio 2005 n. 115, tenuto conto del Decreto 8 settembre 2005 n. 156 e comunque" di cui agli articoli 10, comma 5 e 24, comma 2 della Legge n.160/2011 nonché di cui all'articolo 10, comma 3 della Legge n.159/2011 è soppressa.
2. Al termine dell'articolo 3, comma 2 della Legge n.115/2005 è aggiunta la seguente espressione "raccomandata con avviso di ricevimento".
3. Laddove il Decreto n.156/2005 e successive modifiche e le vigenti norme che prevedano l'utilizzo del SERC facciano riferimento al Decreto Delegato 11 aprile 2016 n.46 e successive modifiche ed al Decreto Delegato 26 luglio 2018 n. 92 ovvero a specifici articoli degli stessi, il richiamo deve intendersi effettuato al presente decreto delegato.
4. L'alinea dell'articolo 15 del Decreto Delegato 29 ottobre 2021 n.184 è così modificata: "1. Dopo l'articolo 2 del Decreto 8 novembre 2005 n.156 e successive modifiche è aggiunto il seguente articolo:".
5. La numerazione e la rubrica dell'articolo 85bis del Decreto n.156/2005, come modificato dal CAPO IV FIRMA ELETTRONICA REMOTA e dall'articolo 15 Decreto Delegato n.184/2021, è così modificata: "Art.2bis (Firma elettronica remota)".
6. All'articolo 9, comma 1 del Decreto Delegato 8 luglio 2013 n.81 sono soppresse le parole ", in particolare MoReq2".
7. In materia di utilizzo di strumenti informatici nell'ambito dell'attività giudiziaria resta fermo il Decreto - Legge 27 luglio 2020 n.124 e successive modifiche.
8. Sono abrogati:
a) il Decreto Delegato 11 aprile 2016 n.46;
b) il Decreto Delegato 26 luglio 2018 n.92;
c) il Regolamento 22 novembre 2018 n.7;

d) gli articoli 5, 6, 7, 8 e 9 del Decreto Delegato 30 gennaio 2020 n.9;
e) l'articolo 85 ter, comma 4 del Decreto n.156/2005, come introdotto dall'articolo 4 del Decreto Delegato n.9/2020;
f) l'articolo 3, comma 1, lettera f), l'articolo 9, comma 1, lettera l), l'articolo 9, comma 2, lettere d) ed e), l'articolo 11 e l'articolo 12 del Decreto Delegato 29 marzo 2021 n.61;
g) il Regolamento 17 dicembre 2021 n.18;
h) gli articoli 12, 13bis e 16, comma 2 *bis* del Decreto Delegato 29 ottobre 2021 n.184;
i) gli articoli 2 e 4 del Decreto Delegato 17 dicembre 2021 n.204.