**Documento di contributo dell’Unità di Missione per l’Attuazione dell’Agenda Digitale su**

**“Sistema pubblico per la gestione dell’Identità digitale**”

Prosposta di DPCM attuativo dell’art. 17-ter, L. 98/2013

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

* Visto l’art. 17-ter della Legge 9 agosto 2013 n. 98 che istituisce il sistema pubblico per la gestione dell’identità digitale di cittadini e imprese e demanda ad un decreto del Presidente del Consiglio dei Ministeri di stabilirne le misure attuative;
* Visto il D.Lgs. 82 del 2005 recante “Codice dell’Amministrazione Digitale”;
* Visto …..
* Rilevata la necessità di provvedere all’attuazione del suddetto art. 17-ter mediante un decreto che stabilisca i principi, criteri, metodi e tempi con la quale l’Agenzia per l’Italia Digitale dovrà individuare le regole tecniche di funzionamento del sistema e consentire ai soggetti interessati a fornire i servizi di identità di accreditarsi in maniera da erogare a cittadini e imprese i servizi di identificazione ed effettuare i necessari coordinamenti con i provider dei servizi online pubblici e privati.
* Considerato che l’obiettivo del Sistema pubblico per la gestione dell’Identità digitale (SPID) è di instaurare la fiducia nei servizi in rete quale elemento chiave per lo sviluppo economico.
* Considerato che lo SPID consentirà a cittadini e imprese dell’Unione Europea di accedere ai servizi in rete prestati in territorio italiano con un maggiore livello di sicurezza, affidabilità e semplicità, favorendo non solo lo sviluppo dei servizi di eGovernment, ma aprendo la strada a nuovi servizi di tipo pubblico-privato.
* Vista la proposta del Ministro delegato per l’innovazione tecnologica e del Ministro per la pubblica amministrazione e la semplificazione, di concerto con il Ministro dell’economia e delle finanze
* Sentito il Garante per la protezione dei dati personali
* Visti i risultati della consultazione pubblica indetta sulla proposta di Decreto.

Decreta

**Articolo 1: Definizioni**

1. Nell’ambito del presente decreto s’intende per:

* Sistema SPID: il Sistema Pubblico dell’Identità Digitale come definito dall’art. 17-ter della Legge n. 98 del 9 agosto 2013.
* CAD: il Codice dell’Amministrazione Digitale approvato con D.Lgs. 7 marzo 2005, n 82 e s.m.i.
* **Identità Digitale SPID**: l’insieme degli attributi, ovvero delle informazioni, relative ad una persona fisica o giuridica, e i suoi dati di identità, come riconosciuti e registrati presso un Gestore dell’identità Digitale accreditato secondo il presente regolamento, utilizzabile secondo quanto prevede il CAD per l’accesso ai servizi online delle pubbliche amministrazioni e verso i soggetti privati che rendono conformi i propri servizi online ai requisiti del Sistema SPID;
* **Attributo:** certificazione digitale, idonea ad essere incorporata nell’Identità Digitale SPID di una persona fisica o giuridica, relativa alle informazioni di cui all’art. 28 comma 3 del CAD prestata secondo quanto previsto dal DPCM 6 settembre 2012, come reso applicabile all’Identità Digitale SPID e al Sistema SPID dall’Agenzia per l’Italia Digitale con apposita decisione da adottarsi ai sensi del presente Decreto, o appartenente alle categorie individuate dall’Agenzia per l’Italia Digitale ai sensi del presente Decreto;
* **Identificativo:** è un particolare attributo utile per identificare univocamente il titolare dell’identità digitale SPID, costituito dal codice fiscale ovvero dal numero di partiva iva;
* **Credenziale:** è un particolare attributo che il titolare dell’identità digitale SPID utilizza ai fini dell’autenticazione;
* **Utente:** persona fisica o giuridica che utilizza i servizi erogati da un Fornitore di servizi**;**
* **Fornitore di servizi**: il fornitore di servizi della società dell’informazione come definiti dall'articolo 2. comma 1, lettera a), del decreto legislativo 9 aprile 2003, n. 70, o dei servizi di un’amministrazione o ente pubblico che siano accessibili in rete;
* **Gestore dell’Identità digitale accreditato**: la persona giuridica, di cui all’art. 7 Comma 1, che crea, rende disponibili e gestisce gli attributi utilizzati dall’utente al fine di dimostrare la propria Identità digitale;
* **Servizi verificati**: i servizi erogati da un fornitore di servizi previa verifica dell’identità digitale SPID dell’utente, attraverso il gestore dell’identità digitale accreditato presso cui l’identità digitale SPID è registrata;
* **Registrazione**: l’insieme delle procedure informatiche, organizzative e logistiche mediante le quali sono raccolte, verificate e certificate ai sensi del presente Decreto le informazioni componenti l’Identità digitale SPID;
* **Autenticazione**: verifica telematica da parte di un Gestore dell’Identità digitale accreditato della validità delle credenziali presentate per l’identificazione elettronica da un utente all’atto di accedere a un Servizio verificato;
* **Processo di Registrazione**: l’insieme delle procedure informatiche, organizzative e logistiche mediante le quali, con i criteri di gestione e protezione previsti dal presente Decreto e dai suoi atti attuativi, è creata un’Identità digitale SPID, garantendo l’approvvigionamento delle credenziali prescelte e la loro consegna all’Utente mediante metodi che assicurino che il solo soggetto titolare sia in possesso della parte segreta delle credenziali;
* **Delega:** particolare tipo di attributo che consente di accedere, utilizzando la propria Identità digitale SPID, ad un servizio qualificato per conto di una persona fisica o giuridica terza;
* **Asserzione:** comunicazione certificata di dati, tra le componenti ed i soggetti del Sistema pubblico per la gestione dell’Identità digitale, attuata tramite l’adozione delle misure di sicurezza previste ai sensi del presente Decreto e dei relativi atti attuativi per garantirne l’integrità e l’autenticità;
* **Gestori di attributi certificati:** il soggetto titolato, ai sensi dell’art. 3 del DPCM 6 settembre 2012 ad attestare il possesso e la validità di attributi qualificati, abilitazioni professionali o poteri di rappresentanza o altri attributi.

**Articolo 3: Sistema pubblico per la gestione dell’Identità digitale**

1. Lo SPID è attuato come sistema aperto di soggetti pubblici e privati, basato su specifiche e standard aperti, i quali, previo accreditamento quali gestori dell’identità digitale ai sensi del presente decreto e dei relativi atti attuativi, gestiscono secondo quanto ivi previsto i processi di registrazione, di interoperabilità delle credenziali e di messa a disposizione delle credenziali dell’Identità digitale SPID e di accesso ai servizi online utilizzando l’identità digitale SPID.
2. Le pubbliche amministrazioni che erogano servizi online sono tenute a garantire ai cittadini ed utenti la possibilità di autenticarsi ed accedere ai servizi online da esse prestate entro otto mesi dall’entrata in vigore del presente Decreto attraverso il Sistema SPID ai sensi del 64 comma 2-quater del CAD. A tal fine l’Agenzia per l’Italia Digitale predispone con proprio provvedimento, entro 2 mesi dall’entrata in vigore del presente Decreto, le procedure necessarie ad assicurare il corretto processo di autenticazione dei cittadini, utenti dei servizi online delle pubbliche amministrazioni e l’assegnazione agli utenti esistenti delle identità SPID, ove il processo di identificazione sia conforme ai requisiti del Sistema SPID.
3. Le risorse finanziarie necessarie per l’istituzione del Sistema SPID sono prelevate dagli stanziamenti già in essere per l’istituzione e il funzionamento dell’Agenzia per l’Italia Digitale o, comunque, da ciascuna Amministrazione senza nuovi e maggiori carichi per la finanza pubblica.
4. L’Agenzia per l’Italia Digitale, al fine di realizzare le finalità del presente articolo, stabilisce con proprie delibere: (i) entro 3 mesi dall’entrata in vigore del presente Decreto, il Regolamento attuativo contenente le procedure che le pubbliche amministrazioni devono seguire per adeguare i propri servizi online ed aderire al sistema SPID e contenente le specifiche e gli standard delle Identità Digitali SPID secondo quanto previsto dall’art. 17-ter della L. n. 98/2013 e dal presente Decreto; (ii) entro 6 mesi, il regolamento contenente le procedure di accreditamento dei Gestori dell’Identità digitale di cui all’art. 7 del presente Decreto; e (iii) il regolamento contenente le procedure di adesione al Sistema SPID dei Fornitori di servizi privati; (v) sempre entro 6 mesi dall’entrata in vigore del presente Decreto, le regole e procedure necessarie affinché i soggetti di cui all’art. 3 del DPCM 6 settembre 2012 possano emettere e gestire attributi conformi al sistema SPID.
5. L’Agenzia per l’Italia Digitale, emessi i regolamenti di cui al comma 4, procede alla notifica del Sistema SPID ai competenti organi della Commissione Europea, quale sistema di identità digitale che consente l’accesso a cittadini ed imprese ai siti della Pubblica Amministrazione italiana.
6. Nell’ambito del Regolamento di cui al comma 4 numero (v) del presente articolo, l’Agenzia per l’Italia Digitale prevede almeno due tipologie di Identità Digitali SPID, entrambe imputabili come previsto al comma 7.
7. L’Agenzia per l’Italia Digitale prevede nel Regolamento di cui al comma 6 almeno le seguenti tipologie di Identità Digitali: (i) identità digitale SPID “verificata”, l’identità digitale dotata del terzo livello di sicurezza, di cui all’art. 9 comma 5, idonea a consentire al fornitore di servizi avente qualifica di pubblica amministrazione o privato di erogare i propri servizi online avendo certezza dell’identità del richiedente sino a quando l’identità venga revocata secondo le procedure di cui all’art. 9 comma 9; (ii) Identità digitale SPID “forte”, dotata di livello di sicurezza di cui all’art. 9, comma 4 idonea, a consentire al fornitore di servizi privato e/o che abbia la qualità di pubblica amministrazione, ente pubblico o gestore di servizio pubblico di far accedere il titolare dell’Identità SPID ai servizi online, equivalenti a quelli normalmente disponibili senza necessità dell’identicazione “de visu”, a favore di una persona fisica e/o giuridica, alla stipula di contratti commerciali e all’accesso a documenti per i quali siano sufficienti i dati anagrafici del Titolare verificati attraverso identificazione remota, valida sino a che l’Identità venga revocata con le procedure di cui all’art. 9 comma 9; (iii) Identità Digitale SPID “ordinaria”, dotata del livello di sicurezza di cui all’art. 9 comma 3, idonea a rappresentare l’identità dell’utente nei rapporti con persone fisiche e giuridiche sino al disconoscimento secondo l’art. 9 comma 8. .

**Articolo 4: Rilascio dell’Identità digitale**

1. Gli attributi identificativi dell’utente, titolare di una Identità digitale SPID, sono inseriti e certificati dal Gestore dell’Identità Digitale Accreditato di cui all’art. 7, che effettua il processo di registrazione.
2. Il Gestore dell’Identità Digitale Accreditato non può rilasciare ad un utente l’identità Digitale SPID prima di essersi accertato, con processi che assicurino che sia stato compiuto il riconoscimento a vista della persona, che l’identità digitale SPID che viene rilasciata corrisponda all’identità reale del richiedente.
3. La ingiustificata violazione della norma di cui all’art. 2 costituisce motivo di revoca dell’accreditamento presso l’Agenzia per l’Italia Digitale ed espone il Gestore dell’identità Digitale che abbia dolosamente o con colpa grave favorito atti in violazione di legge tramite il rilascio di identità digitali SPID non veritiere alle sanzioni previste dalle norme di cui alla L. 231/2007.
4. Le identità digitali SPID rilasciate all’Utente devono necessariamente contenere l’Identificativo, di cui all’art 2 comma 1 lettera C, e altri attributi qualificati funzionali all’autenticazione e fruizione del servizio. Il Regolamento Attuativo indica i seguenti attributi obbligatori: (a) l’indirizzo di posta elettronica utilizzato dal Gestore dell’Identità digitale SPID nelle comunicazioni con il titolare dell’Identità digitale; (b) ….
5. L’Identità digitale SPID può contenere attributi ulteriori rispetto a quelli di cui al comma 4, registrati su richiesta del titolare stesso, il cui scopo è di favorire l’uso dei servizi digitali. Tali attributi sono conformi alle categorie stabilite dall’art. 28 comma 3 del CAD, ovvero stabiliti dall’Agenzia per l’Italia Digitale con propria decisione, aggiornata a cadenza annuale.
6. L’Utente può richiedere la revoca di una Identità digitale SPID in qualsiasi momento rivolgendosi al Gestore accreditato che la rilasciata o, in mancanza, con istanza all’Agenzia per l’Italia Digitale che individuerà il Gestore accreditato competente.
7. Il Gestore dell’Identità digitale accreditato richiede conferma all’utente, almeno ogni 6 mesi, circa l’esattezza degli attributi dell’Identità digitale ed è tenuto a revocarla nel caso riscontri l’inattività della stessa per un periodo continuativo superiore a 24 mesi o venga a conoscenza del decesso della persona fisica o della cessazione della persona giuridica.
8. Il Gestore dell’Identità digitale accreditato impone ai Titolari di identità digitali SPID di comunicare ad esso tempestivamente ogni variazione dei dati contenuti nell’identità digitale SPID.

**Articolo 5: Utilizzo dell’Identità Digitale da parte delle pubbliche amministrazioni.**

1. L’Identità digitale SPID è lo strumento del Sistema SPID previsto quale metodo di accesso ai servizi in rete delle Pubbliche Amministrazioni ai sensi dell’art. 64 comma 2 del CAD.
2. Entro 6 mesi dall’emanazione da parte dell’Agenzia per l’Italia Digitale dei Regolamenti di cui all’art. 3 comma 4 numero (ii) e (iii) del presente Decreto, le Pubbliche Amministrazioni adottano l’Identità Digitale SPID come metodo di accesso principale per i propri servizi in rete, nei modi, nelle forme, nei limiti e nei tempi previsti dal Regolamento di cui all’art. 3 comma 4 numero (ii) del presente Decreto, delegando ai Gestori dell’Identità digitale accreditati le funzioni informatiche, organizzative e logistiche necessarie alla registrazione del soggetto titolare dell’Identità digitale, al rilascio delle credenziali e all’autenticazione degli Utenti che accedono ai propri servizi qualificati in rete.

**Articolo 6: Adesione allo SPID da parte di Fornitori di servizi privati e validità dell’identità digitale SPID**

1. I Fornitori di servizi privati che aderendo al Sistema SPID, adottano quale metodo di accesso ai propri servizi l’Identità Digitale SPID nei modi, nelle forme, con i limiti e nei tempi previsti dal Regolamento attuativo di cui all’art. 3 comma 4 numero (iii) del presente Decreto, saranno considerati, per quanto riguarda gli utenti identificati attraverso il Sistema SPID, aver ricevuto una identificazione dell’Utente, valida, fino a disconoscimento da effettuarsi mediante le procedure all’uopo predisposte al Gestore dell’Identità Digitale accreditato.

**Articolo 7: Gestore dell’Identità digitale accreditato**

1. L’Agenzia per l’Italia Digitale con il Regolamento di cui all’art. 3 comma 4 n. (ii) definisce i Gestori dell’Identità digitale accreditati come persone giuridiche che garantiscono la registrazione del soggetto titolare dell’Identità digitale, il rilascio e l’interoperabilità delle credenziali, la riservatezza delle informazioni gestite, l’autenticazione dell’Utente e procede a definire i requisiti e le procedure per l’accreditamento dei medesimi..
2. I Gestori dell’Identità digitale accreditati di cui al comma 1 devono consentire la registrazione in rete di una Identità Digitale SPID, identificando il soggetto titolare tramite l’utilizzo di CIE, CNS o carte ad esse conformi, e devono garantire l’autenticazione dell’Identità digitale SPID attraverso l’utilizzo del certificato digitale in esse contenuto, senza alcun onere per il cittadino che la richiede.
3. I Gestori dell’Identità digitale accreditati di cui al comma 1 adottano i modelli architetturali e le regole tecniche del Sistema SPID, come definiti dall’Agenzia per l’Italia Digitale nel Regolamento di cui all’art. 3 comma 4 n. (i) e rilasciano credenziali funzionali all’autenticazione certa dell’Utente, che possono essere accettate, per l’accertamento dell’identità personale del soggetto titolare dell’Identità digitale, da tutti i Fornitori di servizi che hanno aderito allo SPID;
4. I Gestori dell’Identità digitale accreditati che rilasciano e gestiscono l’Identità digitale devono:
5. dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di gestione dell’Identità digitale;
6. utilizzare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della dimestichezza con procedure di sicurezza appropriate e che sia in grado di rispettare le regole tecniche.
7. fornire, oltre alle certificazioni previste, il profilo professionale del personale responsabile della gestione delle Identità digitali trattate
8. applicare procedure e metodi amministrativi e di gestione, adeguati e conformi a tecniche consolidate
9. utilizzare sistemi affidabili e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo e internazionale;
10. adottare adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle credenziali;
11. I Gestori dell’Identità digitale accreditati garantiscono la gestione sicura delle componenti riservate delle Identità digitali degli Utenti, assicurando che le stesse non siano rese disponibili a terzi, ivi compresi i Fornitori di servizi stessi, neppure in forma cifrata.
12. I Gestori dell’Identità digitale accreditati gestiscono, per i Fornitori di servizi aderenti, le funzioni di autenticazione e di asserzione certificata degli attributi. I gestori di attributi gestiscono, per i Fornitori di Servizi aderenti, le funzioni di asserzione Certificata degli attributi.
13. I Gestori dell’Identità digitale accreditati o i loro legali rappresentanti e i soggetti preposti all'amministrazione, devono possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385 e successive modificazioni.
    1. avere forma giuridica di società di capitali e un capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione alla attività bancaria ai sensi dell'articolo 14 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385 ;
    2. garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e dei componenti degli organi preposti al controllo, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche ai sensi dell'articolo 26 del decreto legislativo 1° settembre 1993, n. 385 .
14. Le modalità di richiesta di accreditamento sono definite nel Regolamento Attuativo rilasciato dall’Agenzia per l’Italia Digitale.
15. A seguito dell'accoglimento della domanda, l’Agenzia per l’Italia digitale dispone l'iscrizione del richiedente in un apposito elenco pubblico, tenuto dall’Agenzia per l’Italia digitale stessa e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione. Tale elenco pubblico informatico conterrà anche i dati telematici per la verifica di Gestori dell’Identità digitale accreditati.
16. Il Gestore dell’Identità digitale accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni.
17. L’Agenzia per l’Italia digitale procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la sussistenza dei presupposti e dei requisiti previsti dalla presente legge e dispone, se del caso, con provvedimento motivato da notificare all'interessato, il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti, salvo che, ove ciò sia possibile, l'interessato provveda a conformare alla normativa vigente detta attività ed i suoi effetti entro il termine prefissatogli dall'Agenzia stessa.

***Articolo 8: Modello Architetturale***

1. Il Sistema pubblico per la gestione dell’Identità digitale è costituito da:
   1. l’insieme dei Gestori dell’Identità digitale accreditati che assicurano la registrazione, la verifica e la gestione del ciclo di vita dell’Identità Digitale, nonché l’autenticazione delle richieste di accesso provenienti dai Fornitori di servizi;
   2. l’insieme degli Gestori di Attributi Certificati di cui all’art. 10, responsabili di certificare e rendere disponibili attributi relativi a Identità digitali su richiesta dei Fornitori di servizi;
   3. l’insieme dei Fornitori di servizi, che inoltrano le richieste di autenticazione verso il sottosistema centrale e ne ricevono l’esito;
   4. il registro contenente l’elenco di tutti e soli i soggetti abilitati a operare in qualità di Gestori di Identità digitale accreditati, Enti certificatori di attributo e Fornitori di servizi e reso accessibile a tutti i componenti del Sistema pubblico per la gestione dell’Identità digitale;
   5. l’insieme dei componenti di supporto che assicurano l’interscambio delle asserzioni di identità e di attributo tra i Gestori dell’Identità digitale, gli Enti certificatori di attributo ed i Fornitori di servizi, garantendo il corretto instradamento dei dati, assicurando le necessarie funzioni tecnologiche di supporto e tutelando la separazione, sia logica che fisica, delle componenti del sistema.

**Articolo 9: Fruibilità delle Identità digitali e delle credenziali**

1. Tutte le Identità digitali gestite dallo SPID sono imputabili, in quanto registrate tramite l’identificazione certificata del soggetto titolare, ottenuta “de visu” o tramite l’utilizzo di CIE, CNS o carte similari già possedute dal soggetto;
2. Il Sistema pubblico per la gestione dell’Identità digitale prevede credenziali utilizzabili con diversi sistemi di autenticazione. Il Regolamento attuativo prevederà tre livelli di sicurezza dei sistemi di autenticazioni e indicherà quali sistemi e tecnologie sono consentiti per ciascun livello. L’Agenzia per l’Italia Digitale è incaricata di definire i criteri per la valutazione dei sistemi di autenticazione e la loro assegnazione al relativo livello di sicurezza.
3. Il primo livello di sicurezza prevede l’uso di sistemi di autenticazione ad un fattore (password o parola chiave); tale livello di sicurezza è utilizzabile solo per i servizi erogati dai Fornitori di servizi privati;
4. Il secondo livello di sicurezza prevede l’uso di sistemi di autenticazione a due fattori, senza l’obbligo di utilizzo di certificati digitali “forti” come da Allegato 1 della Direttiva comunitaria 1999/93/EC (one time password, certificati soft, Certificati Qualificati soft come da Allegato 1 della direttiva comunitaria 1999/93/EC, certificati Hard). Questo livello di sicurezza è il minimo consentito per i servizi erogati dai Fornitori di Servizi della Pubblica Amministrazione.
5. Il terzo livello di sicurezza prevede l’uso di sistemi di autenticazione a due fattori con l’obbligo di utilizzo di certificati digitali “forti” come da Allegato 1 della Direttiva Comunitaria 1999/93/EC.
6. Compatibilmente con quanto definito nei commi 3, 4 e 5 del presente articolo, ogni Fornitore di servizi che ha aderito al Sistema pubblico per la gestione dell’Identità digitale comunicherà il livello minimo di sicurezza necessario all’erogazione dei suoi servizi in rete.
7. Al fine di garantire l’accesso ai servizi in rete da qualsiasi stazione di lavoro in qualsiasi luogo, gli strumenti per la presentazione delle credenziali non devono implicare configurazioni non *industry standard* dell’hardware o del software della stazione di lavoro o del dispositivo utilizzato per accedere ai servizi. Sono ammesse soluzioni tecniche che prevedono il caricamento automatico del software eventualmente necessario.
8. Il disconoscimento dell’uso dell’Identità Digitale SPID ordinaria si effettua inviando via PEC o e-mail con allegato documento di riconoscimento, confermata da raccomandata A/R, una dichiarazione di disconoscimento motivata al gestore dell’identità digitale e non richiede che il Titolare indichi il soggetto che ha utilizzato le proprie credenziali qualora questo sia ignoto. Qualora il soggetto rimanga ignoto è necessario indicare il motivo presunto per cui l’identità è stata abusata e, come condizione di ammissibilità, presentare al Gestore dell’Identità digitale accreditato copia di querela contro ignoti per i reati di cui all’art. 494 bis o 615-ter c.p. sporta in relazione all’utilizzo fatto da terzi dell’identità Digitale SPID del titolare.
9. Per richiedere la revoca di Identità Digitale SPID forte e/o verificata che sia stata utilizzata senza autorizzazione da terzi è ammessa esclusivamente la presentazione nei confronti dei terzi medesimi o di ignoti di querela per i reati di cui all’art. 494 bis o 615-ter o querela di falso, da fornire, in copia, al gestore accreditato contestualmente alla richiesta di revoca dell’Identità Digitale SPID abusata. Il Titolare, salvo diversa decisione dell’Autorità giudiziaria competente, rimane responsabile degli atti compiuti utilizzando l’Identità Digitale SPID forte e/o verificata sino alla data della querela.
10. Il gestore accreditato consente, in via cautelare e nelle more della presentazione delle querele di cui ai commi 8 e 9 del presente articolo, la sospensione fino a 30 giorni dell’Identità Digitale SPID per sospetto abuso e/o frode su richiesta del Titolare o di un gestore dei servizi. La sospensione non ha efficacia ed espone chi la ha richiesta a responsabilità per eventuali danni causati qualora non sia confermata dalla presentazione delle querele di cui ai commi 9 e 10.
11. L’Agenzia per l’Italia Digitale prevede procedure per consentire ai Titolari dell’Identità Digitale SPID la rimozione dei dati dell’Identità Digitale medesima dai gestori di servizi online che abbiano fraudolentemente e/o in violazione di legge indotto i titolari ad utilizzarla sui propri siti.

**Articolo 10: Gestori di Attributi Certificati**

1. I gestori di attributi certificati si occupano di registrare, certificare e rendere disponibili attributi a cui la legge affida questo compito.
2. Gli attributi certificati saranno relativi ad una persona fisica o giuridica e legati all’Identità Digitale.
3. I gestori di attributi certificati sono soggetti ad una serie di requisiti definiti dall’Agenzia per l’Italia Digitale, la quale provvederà all’accreditamento dell’ente e al rilascio dell’autorizzazione a poter operare. L’ente di certificazione è tenuto a dichiarare gli attributi che rende disponibili, i quali saranno inseriti in un registro centrale a cura dell’Agenzia per l’Italia Digitale, che li renderà disponibili ai Fornitori di servizi.
4. L’Agenzia per l’Italia Digitale definisce le modalità tecniche per l’accesso agli enti certificanti.

**Articolo 11: Deleghe e Procure**

1. L’Agenzia per l’Italia Digitale emanerà con propria decisione, entro 6 mesi dall’entrata in vigore dei regolamenti di cui all’art. 3 comma 4 del presente Decreto, un Regolamento che specifichi le procedure relativa al caso in cui l’accesso al servizio offerto dal Fornitore di servizi non sia effettuato dall’interessato, ma da un terzo soggetto che, essendo autorizzato dal titolare dell’Identità Digitale SPID, richieda, con la propria diversa Identità digitale SPID di poter ottenere servizi in nome e per conto del suddetto titolare, che ad esso ha attribuito delega o procura.

**Articolo 12: Contratti di Servizio**

1. L’Agenzia per l’Italia Digitale definirà i contratti di servizio con i Gestori dell’Identità digitale accreditati ed i Fornitori di servizi. Tali contratti regoleranno il rapporto tra le parti. I Fornitori di servizi privati interessati all’utilizzo di SPID potranno farlo previa convenzione con l’Agenzia per l’Italia Digitale.