LINEE GUIDA PER IL RILASCIO DELL'IDENTITÀ DIGITALE

PER USO PROFESSIONALE

VISTI gli articoli 19 (Istituzione dell'Agenzia per l'Italia Digitale), 21 (Organi e statuto), 22 (Soppressione di DigitPA e dell'Agenzia per la diffusione delle tecnologie per l'innovazione; successione dei rapporti e individuazione delle effettive risorse umane e strumentali) del decreto legge n. 83 del 22 giugno 2012, recante "Misure urgenti per la crescita del Paese", convertito, con modificazioni, nella legge n. 134 del 7 agosto 2012 e s.m.i. e l'articolo 14-bis (Agenzia per l'Italia digitale) del decreto legislativo n.82 del 7 marzo 2005 (Codice dell'amministrazione digitale) e s.m.i.;

VISTO il decreto legislativo 7 marzo 2005, n. 82 e s.m.i., che assegna all'Agenzia la regolamentazione del sistema SPID e, in particolare l'articolo 71;

VISTO il DPCM 24 ottobre 2014 recante "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese." pubblicato sulla G.U. Serie Generale n. 285 del 9 dicembre 2014;

ESPLETATA ai sensi dell'articolo 71, comma 1, del CAD la procedura di consultazione pubblica;

SENTITE ai sensi dell'articolo 71, comma 1, del CAD le amministrazioni competenti;

SENTITO ai sensi dell'articolo 71, comma 1, il Garante per la protezione dei dati personali;

ACQUISITO ai sensi dell'articolo 71, comma 1, il parere della Conferenza unificata;

sono emanate le presenti linee guida.

Articolo 1

Ambito di applicazione

1. Le presenti linee guida normano le modalità di rilascio delle identità digitali per uso professionale cui i gestori di identità digitali del sistema SPID devono attenersi. Tali identità digitali sono quelle utili a provare l'appartenenza di una persona fisica all'organizzazione di una persona giuridica e/o la sua qualità di professionista. Le identità in questione, al contrario, non costituiscono prova dei poteri di rappresentanza di una persona giuridica dei quali una persona fisica è eventualmente in possesso né l'appartenenza di un professionista a un determinato ordine professionale o altro elenco qualificato.
2. Nel caso in cui il gestore dell'identità digitale deleghi all'*organizzazione* l'attività di verifica dell'identità digitale per il rilascio dell'*identità digitale uso professionale per la persona giuridica*, sono applicabili anche gli articoli dal 6 al 13.

Articolo 2

Definizioni generali

1. Ai fini del presente provvedimento si intende per:

a) *identità digitale uso professionale*: identità digitale SPID contenente un attributo che dichiara tale caratteristica;
b) *identità digitale uso professionale della persona fisica*: l'identità digitale che contiene gli attributi della persona fisica cui sono state rilasciate le credenziali di autenticazione;
c) *identità digitale uso professionale per la persona giuridica*: l'identità digitale che contiene gli attributi della persona giuridica e della persona fisica cui sono state rilasciate le credenziali di autenticazione;
d) *DPCM*: il DPCM 24 ottobre 2014 recante "*Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese.*";
e) *RGPD*: Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016;
f) *IdP*: il gestore dell'identità digitale SPID;
g) *organizzazione*: la persona giuridica che stipula un accordo con un IdP al fine del rilascio delle identità digitali di cui alla precedente lettera c) in favore di soggetti che agiscono in qualità di dipendenti o, comunque, a nome o per conto dell'organizzazione stessa.

Si applicano inoltre le definizioni di cui al DPCM 24 ottobre 2014 e s.m.i.

Articolo 3

Modalità di rilascio

1. Al fine di rilasciare l'*identità digitale uso professionale della persona fisica*, il gestore dell'identità deve verificare l'identità personale della persona fisica richiedente. La verifica dell'identità è assolvibile anche attraverso un servizio in rete accessibile con l'uso di identità digitale SPID della medesima persona fisica, a condizione che le credenziali utilizzate per l'autenticazione siano state rilasciate dallo stesso IdP al quale vengono richieste le credenziali per uso professionale e siano di livello pari o superiore a quelle richieste. Tale limitazione non si applica nel caso in cui siano intervenuti specifici accordi di natura privata fra gli IdP.

2. Al fine di rilasciare l'*identità digitale uso professionale per la persona giuridica* il gestore dell'identità deve:
   a) verificare l'identità personale della persona fisica richiedente;
   b) verificare che il richiedente abbia titolo per richiedere l'*identità digitale per la persona giuridica*.
3. La verifica di cui ai precedenti commi 1 e 2 lettera a) è effettuata con le modalità e i controlli previsti dalla normativa vigente in materia di rilascio dell'identità digitale della persona fisica.
4. La verifica di cui al comma 2, lettera b) è effettuata con modalità preventivamente sottoposte dal gestore dell'identità ad AgID per l'approvazione.

Articolo 4

Rapporti fra le parti

1. Fermo restando il rispetto della normativa vigente in materia, le condizioni per la fornitura dell'identità digitale uso professionale sono oggetto di contrattazione fra le parti.
2. Al fine della stipula dell'atto di cui al precedente comma 1, l'*IdP* verifica l'esistenza della persona giuridica, che il firmatario abbia adeguati poteri e la sua identità.

Articolo 5

Attributo uso professionale

1. L'*identità digitale uso professionale* contiene l'attributo-estensione *Purpose* valorizzato con codice **P**.
2. L'attributo oggetto del presente articolo consente ai fornitori di servizi SPID di regolare l'accesso ai servizi dedicati a professionisti e a persone giuridiche.
3. Resta in carico ai fornitori dei servizi SPID la definizione del livello di autorizzazione associato alla persona fisica risultante dall'*identità digitale uso professionale.*
4. Il fornitore di servizi SPID che intende far autenticare un soggetto con l'*identità digitale uso professionale*, inserisce la seguente estensione SAML nell'authRequest:

```
<samlp:Extensions
```

```
      xmlns:spid="https://spid.gov.it/saml-extensions">
    [...]
    <spid:Purpose>P</spid:Purpose>
    [...]
</samlp:Extensions>
```

5. L'*IdP* consente il processo di autenticazione con *identità digitale uso professionale per la persona giuridica* esclusivamente se la richiesta di autenticazione contiene l'estensione di cui al precedente comma 4.

Articolo 6

Ulteriori definizioni

1. Negli articoli che seguono si intende per:
   a) *utenza di governo*: *identità digitale uso professionale per la persona giuridica* abilitata per l'accesso al *sistema di gestione* delle identità;
   b) *utente di governo*: uno o più soggetti dotati di *utenza di governo*;
   c) *utenza di gestione*: *identità digitale uso professionale per la persona giuridica* abilitata per l'accesso al *sistema di gestione* delle identità;
   d) *utente di gestione*: uno o più soggetti dotati di *utenza di gestione*;
   e) *gestori*: i soggetti dotati di *utenze di governo o di gestione*.

Si applicano, inoltre, le definizioni di cui all'articolo 2.

Articolo 7

Condizioni per la delega della funzione di verifica dell'identità all'organizzazione

1. Il gestore dell'identità digitale SPID che demanda ad una *organizzazione* la verifica dell'identità dei soggetti cui fornire l'*identità digitale uso professionale per la persona giuridica,* deve:
   a) formalizzare l'impegno da parte dell'*organizzazione* al rispetto di tutti gli obblighi di legge derivanti dal *RGPD* e, per quanto di competenza, degli obblighi afferenti alla verifica dell'identità del soggetto cui si rilascia tale identità digitale;
   b) assicurarsi che i trattamenti dei dati da parte dei *gestori* siano disciplinati da un contratto o da altro atto giuridico ai sensi dell'art. 28 del *RGPD;*
   c) fornire le istruzioni necessarie ai *gestori* per svolgere l'attività cui sono designati nel rispetto della normativa vigente in materia e dei vincoli giuridici derivanti dall'accordo stipulato con l'*organizzazione*;
   d) assicurarsi che i *gestori* siano consapevoli delle conseguenze penali derivanti dal furto di identità;

e) assicurarsi che i *gestori* siano consapevoli che le credenziali loro fornite sono strettamente personali e che rispondono delle conseguenze del loro utilizzo improprio;
f) assicurarsi che i *gestori* siano consapevoli che le operazioni effettuate sono tracciate;
g) assicurarsi che i *gestori* siano consapevoli del divieto assoluto di operare o avere le credenziali sia in qualità di *utente di governo* che di *utente di gestione*;
h) rendere disponibile online un servizio che consenta ai *gestori* di revocare immediatamente le proprie credenziali, modificare la password, verificare le operazioni effettuate con le proprie credenziali;
i) acquisire l'impegno formale dell'*organizzazione* di garantire che nessun operatore possa operare sia in qualità di *utente di governo* sia di *utente di gestione* e, per quanto di competenza, che le credenziali dei *gestori* siano utilizzate esclusivamente dai legittimi titolari;
l) acquisire l'impegno formale dell'organizzazione a richiedere l'immediata revoca delle credenziali dei *gestori* nel caso in cui abbia rilevato un utilizzo promiscuo delle stesse ovvero nel caso in cui il titolare della stessa lasci l'organizzazione;
m) acquisire la presa d'atto e l'accettazione da parte dell'organizzazione in merito al divieto assoluto di dotare il medesimo soggetto di *utenza di governo* e di *utenza di gestione*;
n) inviare all'*organizzazione* via posta elettronica certificata una comunicazione mensile con cui sono comunicati i codici fiscali dei soggetti cui è stata rilasciata l'*identità digitale per uso professionale per la persona giuridica*, la data di rilascio, l'evidenza delle identità rilasciate nel periodo, l'indicazione dei *gestori* che hanno concorso al rilascio, nonché quelle cui sono state rilasciate tutte le utenze di gestione e dell'utenza di governo attualmente attive.

Articolo 8

Rapporti fra le parti

1. Prima di sottoscrivere l'atto che regola il rapporto fra le parti, l'*IdP* deve verificare la reale esistenza del soggetto giuridico che costituisce parte del rapporto.
2. L'atto giuridico che instaura il rapporto fra le parti deve contenere:
   a) i nominativi dei soggetti dell'*organizzazione* che hanno il potere di autorizzare il rilascio e la revoca delle credenziali dei *gestori* e le modalità con cui tali richieste devono pervenire all'*IdP*. Tali modalità, devono assicurare l'integrità, l'autenticità, il non ripudio, la tracciabilità e la conservazione delle richieste per il periodo di cui all'art. 7, comma 8, del DPCM;
   b) un indirizzo di posta elettronica certificata dell'*organizzazione*;
   c) il nominativo e i recapiti dei rispettivi responsabili del rapporto.

Articolo 9

Rilascio e funzioni dell'utenza di governo e di gestione

1. Le *utenze di governo e di gestione* sono rilasciabili dall'*IdP* ai soggetti per i quali sia stata ottenuta l'autorizzazione ai sensi dell'art. 8, comma 2, lettera a) che dimostrano la propria identità ai sensi

della normativa vigente in materia di rilascio dell'identità digitale SPID.

2. L'*utenza di governo* è utilizzabile per l'accesso al *sistema di gestione* al fine di:
   a) visualizzare l'elenco delle identità digitale uso professionale per la persona giuridica rilasciate in favore della propria organizzazione;
   b) richiedere la revoca delle *identità digitale uso professionale per la persona giuridica* rilasciate in favore della propria organizzazione;
   c) rendere disponibile l'elenco dei soggetti eleggibili ad ottenere l'identità digitale uso professionale per la persona giuridica indicandone il codice fiscale e l'indirizzo di posta elettronica del soggetto;
   d) visualizzare l'elenco di cui alla precedente lettera c) con possibilità di revoca.
3. L'*utenza di gestione* è utilizzabile per l'accesso al *sistema di gestione* al fine di:
   a) visualizzare l'elenco di cui al precedente comma 2 lettera c);
   b) inserire i dati identificativi del soggetto per il quale si sta operando la verifica dell'identità a condizione che tale soggetto sia nell'elenco di cui al precedente comma 2 lettera c). I dati da inserire sono: nome, cognome, data e luogo di nascita, sesso, codice fiscale, numero seriale della Tessera Sanitaria ovvero della Tessera del Codice Fiscale, tipo e numero del documento di riconoscimento, numero di cellulare con prefisso preceduto dal carattere "+" (es. +39123456789), un numero di almeno tre cifre (*codice di controllo*) scelte dal soggetto. Tale numero non può essere costituito da tre numeri identici. Sono ammessi i seguenti documenti di riconoscimento: carta di identità, passaporto, patente. L'indirizzo di posta elettronica del soggetto è quello fornito al comma 2, lettera c) e non è modificabile dall'u*tente di gestione*.
   c) dichiarare di aver ottemperato alla verifica dell'identità del soggetto in ottemperanza alla procedura prevista;
   d) visualizzare l'elenco dei soggetti per i quali ha effettuato la verifica dell'identità e la data della stessa.

Articolo 10

Token di autorizzazione

1. Il *token di autorizzazione* è il risultato dell'algoritmo di hash SHA-256 della stringa di dati contenente i dati personali del soggetto cui rilasciare l'*identità digitale uso professionale per la persona giuridica*, un *token* costituito da una stringa alfanumerica casuale di cinque caratteri e il *codice di controllo* di cui al precedente art. 9, comma 3, lettera b).
   Il contenuto di tale stringa è il seguente:

nome_cognome_codiceFiscale_numeroDocumento_indirizzoMail_numeroCellulare_token_codiceControllo

Articolo 11

Sistema di gestione

1. Il *sistema di gestione* è realizzato a cura degli *IdP*, reso accessibile ai *gestori*, realizza le funzionalità di cui all'art. 9 commi 2 e 3, garantendo la netta separazione dei ruoli.
2. Il *sistema di gestione* deve garantire:
   a) la sicurezza del trattamento dei dati ai sensi dell'articolo 32 del RGPD;
   b) la tracciabilità delle operazioni effettuate con le utenze dei *gestori*, l'indirizzo IP dal quale sono state effettuate, la loro collocazione temporale e la loro conservazione per il periodo di cui all'art. 7, comma 8, del DPCM;
   c) la sicurezza del canale;
   d) l'impossibilità per l'*IdP* di accedere ai dati di cui all'art. 9, comma 3, lettera b).
3. Il *sistema di gestione*, a seguito della dichiarazione di cui all'art. 9, comma 3, lettera c):
   a) invia al titolare il *token* via sms o via email;
   b) rende disponibile all'IdP il *token di autorizzazione* all'emissione dell'identità digitale e, al buon esito dell'operazione, distrugge il *codice di controllo* di cui all'art. 9, comma 3, lettera b).
4. L'*organizzazione* deve garantire adeguata protezione delle stazioni di lavoro utilizzate per accedere al *sistema di gestione* adeguandosi quantomeno a quanto prescritto dalla Circolare № 2/2017 del 28 aprile 2017 recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni." Dette stazioni di lavoro sono accedute dai *gestori* previa autenticazione con credenziali senza particolari privilegi (non administrator/root).

Articolo 12

Rilascio dell'identità

1. Al fine di ottenere l'*identità digitale per uso professionale per la persona giuridica*, l'interessato, dopo essere stato autorizzato dall'*utente di gestione*:
   a) accede al servizio di rilascio dell'identità reso disponibile dall'*IdP* su canale protetto su cui inserisce il *token* ricevuto ai sensi dell'art. 11, comma 3, lettera a), i dati personali e il *codice di controllo* di cui all'art. 9, comma 3, lettera b);
   b) il servizio di rilascio dell'identità dell'*IdP*, dopo aver ricalcolato il *token di autorizzazione* con i dati inseriti dall'interessato e averne verificata la corrispondenza con quanto ricevuto dal *sistema di gestione* ai sensi dell'art. 11, comma 3, lettera b), provvede a rilasciare l'identità digitale inviando almeno una delle credenziali SPID via sms o email ai recapiti ottenuti ai sensi della precedente lettera a). In ogni caso, invia all'indirizzo email dichiarato dall'interessato all'*utente di governo* una comunicazione in cui si informa di aver rilasciato l'identità digitale.

Articolo 13

Livello delle credenziali dei *gestori*

1. Le credenziali SPID rilasciate ai gestori sono di livello pari o superiore alle credenziali delle *identità digitali per uso professionale per la persona giuridica* rilasciabili ai sensi dell'art. 12.

Articolo 14

Entrata in vigore

1. Al fine di consentire ai gestori di identità digitale SPID di predisporre quanto necessario, per ottemperare a quanto disposto dall'articolo 5, comma 5, il presente provvedimento entra in vigore a decorrere dal 1 dicembre 2019.