Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

ACCREDITAMENTO DEI SOGGETTI CHE SVOLGONO L'ATTIVITÀ DI GESTORI DI IDENTITA' DIGITALE AI SENSI DEL DPCM 24 OTTOBRE 2014

DOCUMENTAZIONE PER L'ACCREDITAMENTO

Il presente documento elenca la documentazione che i soggetti, pubblici e privati, che intendono ottenere l'accreditamento ai sensi dell'art. 64, comma 2-ter, del decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (di seguito "CAD") devono allegare alla domanda di accreditamento da presentare all'Agenzia per l'Italia Digitale, nei modi indicati nel regolamento del ____2015 dalla stessa emanata (di seguito "regolamento dell'Agenzia").

Si applica quanto disposto dal D.P.R. 28 dicembre 2000, n.445 e s.m.i. in materia di dichiarazioni sostitutive e di acquisizione d'ufficio delle informazioni e di tutti i dati e documenti che siano in possesso di pubbliche amministrazioni.

1. Documenti amministrativi da presentare unitamente alla domanda di accreditamento

a) copia autentica dell'atto costitutivo della società;

b) dichiarazione attestante l'iscrizione nel registro delle imprese di data non anteriore a novanta giorni rispetto a quella di presentazione della domanda;

c) dichiarazione rilasciata dall'organo preposto al controllo, o dal soggetto incaricato della revisione contabile ai sensi della normativa vigente - di data non anteriore a trenta giorni rispetto a quella di presentazione della domanda - attestante l'entità del capitale sociale versato, nonché l'ammontare e la composizione del patrimonio netto;

d) prospetto della situazione patrimoniale, predisposto e approvato dall'organo amministrativo, di data non anteriore a duecentosettanta giorni rispetto a quella di presentazione della domanda;

e) relazione dell'organo preposto al controllo, o del soggetto incaricato della revisione contabile, redatta ai sensi della normativa vigente, sulla situazione patrimoniale di cui alla lettera d);

f) documentazione equivalente a quella prevista ai punti precedenti, legalizzata ai sensi dell'art. 33 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (per le società costituite in altro paese membro dell'Unione europea);

g) elenco nominativo dei rappresentanti legali, dei componenti dell'organo di amministrazione e dell'organo di controllo, nonché di eventuali altri soggetti preposti all'amministrazione, con l'indicazione dei relativi poteri. Ognuno dei suddetti soggetti deve risultare in possesso, all'atto della domanda, dei requisiti di onorabilità di cui all'art. 29, comma 3, lettera b, del CAD, comprovati:

1. per i cittadini italiani residenti in Italia:
   - dalla dichiarazione sostitutiva di atto di notorietà, di possedere i requisiti di onorabilità stabiliti dal decreto del Ministero del Tesoro, del Bilancio e della Programmazione economica 18 marzo 1998, n.161 e di non essere stato destinatario, in altri Stati, di provvedimenti corrispondenti a quelli che importerebbero, secondo l'ordinamento italiano, la perdita dei requisiti di onorabilità di cui al decreto suddetto;
   - dalla dichiarazione sostitutiva di certificazione attestante di non aver riportato condanne penali e di non essere a conoscenza di essere sottoposto a provvedimenti che riguardano l`applicazione di misure di prevenzione, di decisioni civili e di provvedimenti amministrativi iscritti nel casellario giudiziale;
   - dalla dichiarazione sostitutiva di certificazione attestante di non essere a conoscenza di essere sottoposto a procedimenti penali;
2. per le persone che non rientrano nella categoria di cui al precedente punto 1:
   - dalla dichiarazione sostitutiva di atto di notorietà, di possedere i requisiti di onorabilità stabiliti dal decreto del Ministero del Tesoro, del Bilancio e della Programmazione economica 18 marzo 1998, n.161 e di non essere stato destinatario, in altri Stati, di provvedimenti corrispondenti a quelli che importerebbero, secondo l'ordinamento italiano, la perdita dei requisiti di onorabilità di cui al decreto suddetto;
   - dalla dichiarazione sostitutiva di certificazione attestante di non trovarsi in stato di liquidazione o di fallimento e di non avere presentato domanda di concordato.

In alternativa, per i soggetti iscritti nell'albo di cui all'art. 13 del decreto legislativo 1 settembre 1993, n. 385, la dimostrazione del possesso dei requisiti di onorabilità da parte delle persone di cui alla presente lettera, potrà essere assolta mediante apposita dichiarazione sostitutiva di certificazione resa, ai sensi dell'art. 46 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, dal legale rappresentante, attestante l'iscrizione nel suddetto albo alla data di presentazione della domanda di accreditamento;

h) copia della polizza assicurativa di RC professionale per l'attività di gestore di identità SPID (o certificato provvisorio impegnativo, cui dovrà seguire copia della polizza entro l'avvio delle attività) stipulata per la copertura dei rischi dell'attività in questione e dei danni causati a terzi, rilasciata da una società di assicurazioni abilitata a esercitare nel campo dei rischi industriali a norma delle vigenti disposizioni, con un massimale minimo di € 150.000 per singolo sinistro e un massimale minimo per annualità assicurativa dipendente dal numero di identità digitali rilasciate determinata nei seguenti valori: 2,5 milioni di euro, fino a 100.000 identità; 5 milioni di euro, fino 1 milione di identità; 8 milioni di euro fino a 3 milioni di identità; 10 milioni di euro, oltre 3 milioni di identità digitali. Non rientrano nel computo delle identità digitali rilasciate le identità scadute o revocate da oltre dodici mesi dalla decorrenza dell'annualità assicurativa. La copertura assicurativa deve prevedere una retroattività dalla decorrenza dell'inizio dell'attività di gestore di identità SPID ovvero per un periodo di almeno cinque anni. Il gestore si impegna ad inviare tempestivamente all'Agenzia, e comunque entro venti giorni dalla data di scadenza della polizza assicurativa, le attestazioni dei successivi rinnovi congiuntamente ad una dichiarazione inerente il numero di identità digitali attive e scadute o revocate da meno di dodici mesi dalla data di decorrenza dell'annualità assicurativa;

i) copia dell'ultimo bilancio approvato e relativa certificazione. Se la società è stata costituita da meno di diciotto mesi tale documentazione deve essere depositata entro diciotto mesi dalla costituzione della società;

l) dichiarazione attestante la composizione dell'azionariato, per quanto nota, con l'indicazione, comunque, dei soggetti partecipanti, in forma diretta o indiretta, al capitale sociale in misura superiore al 5%.

2. Documenti tecnici e organizzativi generali

m) documentazione delle prove di collaudo interno comprovanti l'aderenza a tutti gli aspetti previsti dalle regole tecniche;

n) documentazione delle prove di collaudo interno dei dispositivi usati per l'autenticazione;

o) il piano di test per le verifiche dell'Agenzia previste in fase di accreditamento dal regolamento dell'Agenzia;

p) copia del manuale operativo, redatto in lingua italiana, contenente le seguenti informazioni inerenti il servizio di gestore di identità:

1. dati identificativi del gestore;
2. dati identificativi della versione del manuale;
3. responsabile del manuale operativo;
4. descrizione delle architetture, applicative e di dispiegamento, adottate per i sistemi run-time che realizzano i protocolli previsti dalle regole tecniche;
5. descrizione delle architetture dei sistemi di autenticazione e delle credenziali;
6. descrizione dei codici e dei formati dei messaggi di anomalia sia relativi ai protocolli che ai dispositivi di autenticazione utilizzati;
7. livelli di servizio garantiti per le diverse fasi della registrazione e della gestione del ciclo di vita delle identità;
8. livelli di servizio garantiti per le diverse fasi del processo di autenticazione;
9. descrizione dei contenuti delle tracciature degli accessi al servizio di autenticazione e delle modalità di acquisizione ai fini dell'opponibilità a terzi;
10. guida utente del servizio ;
11. descrizione dei processi e delle procedure utilizzate per la verifica dell'identità degli utenti e per il rilascio delle credenziali;
12. descrizione dei metodi di gestione dei rapporti con gli utenti;
13. descrizione generale delle misure anti-contraffazione;
14. descrizione generale del sistema di monitoraggio;
15. definizione degli obblighi del gestore e dei titolari dell'identità digitale;
16. indirizzo (o indirizzi) del sito web del gestore ove è resa direttamente disponibile la descrizione del servizio in lingua italiana e lingua inglese;
17. descrizione delle modalità disponibili agli utenti per richiedere la revoca e sospensione dell'identità digitale.

L'Agenzia per l'Italia Digitale se approva il manuale operativo, lo sottoscrive con firma

elettronica e lo pubblica sul proprio sito istituzionale con le informazioni atte a identificare il gestore. Eventuali modifiche al manuale operativo devono essere sottoposte all'Agenzia per l'Italia Digitale per l'approvazione prima della loro adozione. Il gestore accreditato è tenuto a fornire all'Agenzia copia del manuale operativo tradotto in lingua inglese entro novanta giorni dalla richiesta della stessa. A seguito di tale richiesta, le versioni successive dovranno essere fornite in lingua italiana e inglese.

q) modalità con cui si garantisce che agli eventi registrati (log) sia apposto un riferimento temporale che corrisponda alla scala di tempo UTC(IEN), di cui al decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591, con una differenza non superiore ad un minuto primo.

r) individuazione dei responsabili previsti nel regolamento dell'Agenzia e loro curriculum vitae redatto secondo il formato europeo, in cui viene attestato, mediante l'indicazione di specifici percorsi di studio ovvero di congrui periodi di specifica attività in contesti specialistici, il possesso di conoscenze peculiari e documentate coerenti con il ruolo assunto;

s) copia del piano per la sicurezza, redatto in conformità con quanto disposto al paragrafo 3, cifrato con la chiave pubblica resa disponibile dall'Agenzia;

t) dichiarazione di aver ottemperato a quanto previsto dalla normativa inerente il trattamento dei dati personali;

u) dichiarazione di disponibilità a consentire l'accesso di soggetti indicati dall'Agenzia per l'Italia Digitale presso le strutture dedicate allo svolgimento del servizio di gestore di identità SPID, di proprietà o di terzi, al fine di poter verificare il possesso dei requisiti di sicurezza e tecnico-organizzativi documentati all'atto della domanda e successivamente, al fine di consentire l'espletamento delle funzioni di vigilanza e controllo ai sensi del DPCM 24 ottobre 2014 e di adempiere alle disposizioni derivanti dal Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014.

v) dichiarazione d'impegno a comunicare all'Agenzia, entro il ventesimo giorno dal suo verificarsi, ogni eventuale variazione intervenuta rispetto a quanto risultante dai documenti presentati all'Agenzia. A seguito di tali variazioni, l'Agenzia potrà procedere ad una nuova - se del caso anche parziale - valutazione dei requisiti o richiedere ulteriore documentazione;

w) copia della certificazione ISO/IEC 27001:2013 del sistema di gestione della sicurezza delle informazioni nel dominio logico, fisico e organizzativo nel quale sono realizzati i servizi di gestione delle identità, rilasciata da un ente di certificazione accreditato da un ente di Accreditamento designato dal proprio Stato ai sensi del Regolamento (CE) N. 765/2008 del 9 luglio 2008 e firmatario degli accordi di Mutuo riconoscimento per i Sistemi di Gestione (MS). Sono considerate valide le certificazioni ISO/IEC 27001:2005

già rilasciate fino al termine di validità previsto e, comunque, non oltre il 31 dicembre 2015. Fino al predetto termine sono considerate valide le certificazioni prescritte alla presente lettera pur se non contenenti un chiaro riferimento al sistema SPID.

x) copia del certificato di conformità del proprio sistema di qualità alle norme UNI EN ISO 9001, successive modifiche o a norme equivalenti e copia del manuale della qualità. Il gestore deposita presso l'Agenzia le successive certificazioni entro sei mesi dalla scadenza della precedente;

y) nel caso in cui il gestore affidi ad un terzo le funzioni di continuità operativa (anche solo in parte), copia del relativo contratto stipulato;

z) descrizione delle procedure utilizzate nel processo di rilascio delle identità digitali, con particolare attenzione alle procedure utilizzate al fine di evitare furti di identità. Il gestore accreditato è tenuto a fornire all'Agenzia copia delle procedure tradotte in lingua inglese entro novanta giorni dalla richiesta della stessa. A seguito di tale richiesta, le versioni successive dovranno essere fornite in lingua italiana e inglese.

aa) dichiarazione, sottoscritta dal legale rappresentante, per l'eventuale conferimento in favore di uno o più dei responsabili di cui alla lettera n) del potere di sottoscrivere ed inviare aggiornamenti della documentazione depositata al fine dell'accreditamento;

bb) entro sei mesi dalla sottoscrizione della convenzione di cui all'art. 10, comma 2 del DPCM 24 ottobre 2014, documentazione comprovante l'adempimento di quanto prescritto dall'articolo 11, comma 1, lettera g) del medesimo decreto. Detta documentazione deve essere aggiornata con cadenza semestrale.

cc) descrizione delle modalità formative, dei loro contenuti e degli aggiornamenti, volti ad una adeguata preparazione dei soggetti deputati alla verifica dell'identità dei titolari;

dd) copia delle procedure cui devono attenersi i soggetti di cui al punto cc) nell'esecuzione delle attività loro affidate;

ee) copia della dichiarazione che sarà fatta sottoscrivere ai soggetti di cui al punto cc) contenente l'impegno degli stessi ad operare come indicato nelle procedure di cui al punto dd) e la presa d'atto delle responsabilità civili e penali eventualmente derivanti dalla mancata applicazione delle procedure previste.

I gestori, se soggetti pubblici, dovranno allegare solo la documentazione elencata dalla lettera m) in poi.

I soggetti che hanno già depositato per altri scopi presso l'Agenzia la documentazione amministrativa prevista dalla lettera a) alla lettera l), sono esentati dalla presentazione di tale documentazione per la quale non sia richiesto uno specifico termine di validità, purché nella domanda di accreditamento dichiarino espressamente che essa è ancora valida e la documentazione soddisfi quanto previsto per l'accreditamento.

I gestori, se soggetti pubblici, devono allegare una relazione di sostenibilità tecnica,

organizzativa ed economica. L'analisi economica, per il buon fine dell'istruttoria, deve dimostrare la convenienza economica del soggetto pubblico ad accreditarsi anziché utilizzare i servizi di altri gestori accreditati.

3. Piano per la sicurezza del gestore di identità

1. Il gestore redige un piano per la sicurezza nel quale, al fine di descrivere l'attività di gestore di identità SPID, sono contenuti almeno i seguenti elementi inerenti alla attività di gestore di identità:

a) struttura generale, modalità operativa e struttura logistica;

b) descrizione dell'infrastruttura di sicurezza fisica;

c) allocazione dei servizi e degli uffici negli immobili;

d) descrizione delle funzioni del personale e sua allocazione;

e) attribuzione delle responsabilità;

f) algoritmi crittografici o altri sistemi utilizzati per garantire la sicurezza delle informazioni;

g) descrizione delle procedure utilizzate;

h) descrizione dei dispositivi installati;

i) descrizione dei flussi di dati;

l) procedura di gestione delle copie di sicurezza dei dati;

m) procedura di continuità operativa del servizio di autenticazione, revoca e sospensione;

n) analisi dei rischi;

o) descrizione delle contromisure;

p) descrizione delle verifiche e delle ispezioni;

q) procedura di gestione dei disastri;

r) procedura di gestione degli incidenti;

s) misure di sicurezza per la protezione delle credenziali degli utenti;

t) descrizione delle credenziali fornite agli utenti e loro analisi al fine di sostenere la loro collocazione nel livello di sicurezza di cui al comma 1 dell'articolo 6 del DPCM 24 ottobre 2014 ritenuto appropriato. Al fine di distinguere nello scambio documentale con l'Agenzia le tipologie di credenziali fra loro, ad ogni tipologia è assegnato un riferimento univoco composto da *aaaa_ss_mm* dove, *aaaa* rappresenta l'anno in cui la tipologia di credenziali è presentata per la prima volta all'Agenzia per la valutazione prevista dal comma 2 del citato articolo del DPCM, *ss* è un numero sequenziale univoco nell'ambito di ogni singolo anno che individua la tipologia presentata nell'anno, *mm* è un numero sequenziale che afferisce alle eventuali modifiche successivamente presentate per la singola tipologia.

Nella redazione del piano per la sicurezza deve essere particolarmente curata la descrizione dei rischi di contraffazione, delle misure per mitigarli e del sistema di monitoraggio (obiettivi, allarmi, reazioni).

2. Quanto previsto al comma precedente può essere contenuto in più documenti.

3. Il piano per la sicurezza si attiene alle misure di sicurezza previste dal Titolo V della Parte I del decreto legislativo 30 giugno 2003, n. 196.

4. Il piano per la sicurezza è sottoscritto dal legale rappresentante del gestore, ovvero dal responsabile della sicurezza da questo delegato.

5. L'Agenzia, ai sensi del comma 2 dell'articolo 6 del DPCM 24 ottobre 2014, valuta il contenuto del piano per la sicurezza e, vista in particolare la documentazione di cui alla lettera t), colloca le credenziali al livello di sicurezza ritenuto adeguato. Qualora le deduzioni dell'Agenzia circa il livello di sicurezza cui collocare le credenziali differisca da quanto indicato dal richiedente ai sensi della precedente lettera t), l'Agenzia contatta il referente del richiedente per consentirgli di presentare, nei termini indicati dalla stessa Agenzia, eventuali controdeduzioni prima di prendere una decisione definitiva. La decisione è comunicata formalmente al richiedente.