Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

REGOLAMENTO

RECANTE LE MODALITÀ PER L'ACCREDITAMENTO E LA VIGILANZA DEI GESTORI DELL'IDENTITA' DIGITALE (articolo 1, comma 1, lettera l) , DPCM 24 ottobre 2014)

VISTO l'art. 64 comma 2-ter del decreto legislativo 7 marzo 2005, n. 82 e s.m.i. (Codice dell'amministrazione digitale, nel seguito "CAD") attribuisce all' Agenzia per l'Italia Digitale (nel seguito "Agenzia") il compito di accreditare i soggetti pubblici e privati che *"gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni, in qualità di erogatori di servizi in rete, ovvero, direttamente, su richiesta degli interessati".*

VISTO l'art. 64 comma 2-sexies prevede che con decreto del Presidente del Consiglio dei ministri, su 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, sono definite le caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), anche con riferimento alle modalità e ai requisiti necessari per l'accreditamento dei gestori dell'identità digitale;

VISTO l'art. 4 comma 1, lettera a) del DPCM 24 ottobre 2014, assegna all'Agenzia l'accreditamento dei gestori dell'identità digitale e al comma 3 stabilisce che "l'Agenzia, sentito il Garante per la protezione dei dati personali, emana con proprio regolamento le modalità di accreditamento dei soggetti SPID.";

VISTO l'art. 10 del DPCM 24 ottobre 2014 (nel seguito DPCM);

VISTO il 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;

SENTITO il Garante per la protezione dei dati personali;

RITENUTO opportuno emanare ai sensi dell'art. 4, comma 3 del DPCM 24 ottobre 2014, un regolamento concernente le modalità per l'accreditamento e la vigilanza dei gestori dell'identità digitale di cui all'art. 3, comma 1, lettera a) del medesimo decreto;

l'Agenzia per l'Italia Digitale emana il seguente Regolamento.

1. Accreditamento dei gestori dell'identità digitale

Sulla base delle disposizioni richiamate in premessa, possono richiedere l'accreditamento i soggetti di cui all'art. 64 comma 2-ter del CAD che, al fine di conseguire il riconoscimento dello status di "gestori dell'identità digitale" (nel seguito "gestori" o "gestore"), devono:

1. dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere l'attività di gestore dell'identità digitale nell'ambito del Sistema di cui all'Art. 64 comma 2-bis;
2. utilizzare congruo personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore e della dimestichezza con procedure di sicurezza appropriate e che sia in grado di rispettare le norme del CAD e le regole tecniche previste;
3. essere titolari di certificazione UNI EN ISO 9001 e ISO/IEC 27001 nelle edizioni applicabili e metodi e tecniche amministrative consolidate per la realizzazione dei servizi SPID di cui al DPCM;
4. adottare adeguate misure di protezione idonee a garantire la riservatezza, l'autenticità, l'immodificabilità, l'integrità dei dati e la fruibilità dei servizi;
5. fornire al personale preposto le conoscenze necessarie a garantire, nelle rispettive attività, la protezione dei dati personali.

Il gestore, se soggetto privato, in aggiunta a quanto previsto dai precedenti punti, deve inoltre:

6. avere forma giuridica di società di capitali e il capitale sociale previsto dal DPCM;
7. 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 recante il Testo unico delle leggi in materia bancaria e creditizia".

I soggetti interessati a ottenere l'accreditamento in qualità di gestori dell'identità digitale del Sistema Pubblico di Identità Digitale, presentano apposita domanda.

Oltre alla domanda, devono essere depositati presso l'Agenzia i documenti previsti

nell'allegato "DOCUMENTAZIONE PER L'ACCREDITAMENTO", che costituisce parte integrante del presente regolamento.

I gestori che conseguono l'accreditamento ai sensi del presente regolamento e che stipulano la Convenzione di cui all'art.10 comma 2 del DPCM sono iscritti nel registro SPID, di cui all'art. 1 comma 1 s) del DPCM, come soggetti abilitati ad operare in qualità di gestori dell'identità digitale, pubblicato sul sito istituzionale dell'Agenzia, accessibile anche in modalità applicativa attraverso delle API definite nelle Regole tecniche.

Sui soggetti accreditati l'Agenzia esercita attività di vigilanza, volta ad assicurare che siano mantenuti nel tempo i requisiti che hanno consentito l'iscrizione, pena la revoca dell'accreditamento e la conseguente cancellazione dal registro.

In caso vengano riscontrate difformità nel corso dell'attività di vigilanza, l'Agenzia comunica al gestore le modalità e il termine per la loro risoluzione.

Qualora il gestore non si adegui nel termine indicato, l'Agenzia, ove non sussistano adeguate motivazioni per prorogare il suddetto termine, dispone, con provvedimento motivato, la revoca dell'accreditamento e la conseguente cancellazione dall'elenco.

Il gestore per il quale sia stato disposto un provvedimento di revoca non può presentare una nuova domanda di accreditamento se non siano cessate le cause che hanno dato luogo alla cancellazione dall'elenco e, in ogni caso, non prima che siano trascorsi 6 mesi dall'emissione del provvedimento di revoca.

Per espletare le attività per l'accreditamento dei gestori e per svolgere le connesse funzioni di vigilanza, l'Agenzia si avvale di apposita struttura, istituita nell'ambito delle proprie dotazioni organiche. L'Agenzia si riserva di verificare, anche a campione, il rispetto delle Norme ISO/IEC 27001. Per espletare detta verifica, l'Agenzia può avvalersi di terze parti accreditate dall'Ente Unico di Accreditamento Nazionale, istituito a fronte del Reg. UE 765/2008 riconosciuto a fronte del medesimo Regolamento in uno dei Paesi dell'Unione Europea e firmatario dei patti di mutuo riconoscimento per le norme citate.

2. Presentazione domanda di accreditamento

La domanda di accreditamento redatta in lingua italiana, è predisposta in formato elettronico, o fornita in copia ai sensi dell'art. 22, comma 2, del CAD, sottoscritta con firma digitale o firma elettronica qualificata dal legale rappresentante del richiedente, ed è inviata alla casella di posta elettronica certificata dell'Agenzia. Con le medesime modalità deve essere predisposta la documentazione per l'accreditamento prevista dall'allegato al presente regolamento.

La domanda deve indicare:

1. la denominazione della società;
2. la sede legale;

3. le sedi operative utilizzate per l'attività di gestore dell'identità;
4. l'indirizzo PEC della società;
5. il/i rappresentante/i legale/i;
6. il nominativo e i recapiti (numeri telefonici, indirizzo fisico e di posta elettronica) di uno o più referenti tecnici cui l'Agenzia può rivolgersi in presenza di problematiche tecnico-operative che possono essere risolte per le vie brevi;
7. i nominativi e riferimenti telefonici e di posta elettronica dei seguenti soggetti individuati ai sensi dell'art. 10, comma 3, lettera e) del DPCM:
    a. responsabile della sicurezza;
    b. responsabile della conduzione tecnica dei sistemi;
    c. responsabile delle verifiche e delle ispezioni;
    d. responsabile delle attività di verifica dell'identità del soggetto richiedente e della gestione e conduzione del servizio;
    e. responsabile dell'istruzione dei soggetti coinvolti nelle diverse attività necessarie alla conduzione e gestione del servizio;
    f. responsabile per l'aggiornamento della documentazione depositata presso l'Agenzia;
    g. referente per la protezione dei dati personali

    Le cariche di cui alle lettere a) e c) sono incompatibili con le altre. Le cariche di cui alle lettere a) e d) sono ricoperte da personale alle dirette dipendenze del gestore, ferma restando la responsabilità del gestore per tutte le attività. La carica di cui alla lettera g) è incompatibile con la carica di cui alla lettera c) .
8. l'elenco dei documenti allegati, con preciso riferimento a quanto indicato nell'allegato "Documentazione per l'accreditamento".

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.

3. Iter istruttorio della domanda di accreditamento

L'istruttoria relativa alle domande e la valutazione della documentazione prodotta sono effettuate dall'Agenzia. In particolare:

a) L'attività istruttoria è volta a verificare che i processi tecnico organizzativi e le tecnologie adottati dal gestore e specificate nel

manuale operativo siano conformi a quanto previsto dal DPCM e dalle regole tecniche emesse ai sensi dell'art. 4 comma 2 dello stesso;

b) La domanda di accreditamento si considera accolta qualora non venga comunicato al richiedente il provvedimento di diniego entro centottanta giorni dalla data di presentazione della stessa;

c) L'agenzia nel corso dell'istruttoria può effettuare verifiche sulla rispondenza dei protocolli di autenticazione informatica a quanto previsto dalle regole tecniche e sulla adeguatezza ed usabilità degli strumenti e dalle tecnologie di autenticazione informatica di cui all'articolo 6, comma 2, del DPCM e da quant'altro concorre nel processo di autenticazione. Le prove, effettuate sulla base di un piano di test proposto dal gestore e preventivamente eseguito dallo stesso nelle finalità di collaudo interno, possono essere condotte in un ambiente di test, predisposto a tal scopo dallo stesso gestore, ed eventualmente anche in ambiente di produzione. Nel corso delle verifiche l'Agenzia può richiedere l'esecuzione di prove integrative rispetto a quelle previste dal piano di test presentato, al fine di accertare eventuali aspetti non evidenziati, in tutto o in parte, dal predetto piano di test; l'ambiente di test dovrà essere mantenuto operativo, ai fini della vigilanza, per tutta la durata dell'esercizio del servizio;

d) l'Agenzia si riserva la facoltà di svolgere verifiche presso le strutture dedicate allo svolgimento delle attività di gestore di identità;

e) Il termine di centottanta giorni di cui alla precedente lettera b), può essere sospeso una sola volta per i seguenti motivi:

   i. richiesta di documenti necessari a integrare o completare la documentazione presentata e che non siano già nella disponibilità dell'Agenzia o che questa non sia tenuta ad acquisire autonomamente. Il periodo di sospensione si conclude al momento della ricezione della documentazione integrativa da presentare improrogabilmente entro centottanta giorni dalla data di sospensione;

   ii. richiesta di modifica da parte dell'Agenzia del piano di test e o dell'ambiente di test predisposto, a seguito di richiesta di prove integrative ;

f) Al termine dell'istruttoria, l'Agenzia accoglie la domanda ovvero la respinge con provvedimento motivato e ne dà apposita comunicazione al richiedente.

g) Il soggetto la cui domanda sia stata respinta, non può presentare una

nuova domanda se non siano cessate le cause che hanno determinato il mancato accoglimento della precedente e, comunque, non prima che siano trascorsi sei mesi dalla data di deposito della domanda respinta.

4. Stipula della Convenzione

A seguito dell'accreditamento, l'Agenzia informa il richiedente e propone la sottoscrizione della convenzione di cui all'articolo 10, comma 2, del DPCM 24 ottobre 2014. A seguito della avvenuta stipula della Convenzione l'Agenzia dispone l'iscrizione del gestore di identità nell'apposito registro di cui all'Art.1 del DPCM, ai fini dell'applicazione della disciplina in questione.

Il gestore dell'identità digitale accreditato, ottenuta l'iscrizione nell'apposito registro, può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni nel rispetto delle indicazioni di cui al documento "SPID: modalità attuative".

Entro 10 giorni dalla data di iscrizione nel registro, il gestore deve pubblicare in una sezione del proprio sito web, denominata "soluzioni tecnologiche per l'autenticazione SPID" almeno l'elenco dei sistemi di autenticazione approvati dall'Agenzia con livello di sicurezza associato e la relativa data di approvazione;

5. Contenuti del Registro SPID

Le informazioni riportate nel registro SPID relative ai gestori dell' identità digitale, accreditati ai sensi del presente regolamento, sono, per ogni soggetto iscritto, le seguenti:

a) denominazione della società;
b) indirizzo della sede legale;
c) riferimenti al manuale operativo del soggetto;
d) riferimenti al manuale utente;
e) metadata dei servizi;
f) carta dei servizi;
g) data di iscrizione;
h) stato dell'accreditamento (attivo, se in corso di validità, o revocato, nel caso in cui sia intervenuta la revoca con indicazione della data di revoca).

Di queste informazioni quelle disponibili in maniera applicativa mediante API sono documentate nelle regole tecniche.

6. Presentazione della domanda di autorizzazione all'uso dei sistemi di autenticazione informatica

La domanda di autorizzazione all'uso dei sistemi di autenticazione informatica, costituiti dagli strumenti e dalle tecnologie di autenticazione informatica di cui all'art.6 comma 2 del DPCM, dai protocolli di autenticazione informatica e da quant'altro concorre nel processo di autenticazione, è presentata all'Agenzia, dai gestori di identità SPID, che avvia l'iter di valutazione della soluzione tecnologica proposta.
La domanda, redatta in lingua italiana, è predisposta in formato elettronico o fornita in copia ai sensi dell'art. 22, comma 2, del CAD, sottoscritta con firma digitale o firma elettronica qualificata dal legale rappresentante del richiedente, da persona dallo stesso delegata o dal responsabile per l'aggiornamento della documentazione depositata presso l'Agenzia di cui alla lettera f) del punto 7 del paragrafo 2, ed è inviata alla casella di posta elettronica certificata all'indirizzo PEC del protocollo dell'Agenzia con le modalità previste al paragrafo 2 del presente regolamento.

La domanda deve recare in allegato:

1. il rapporto di conformità di cui al successivo paragrafo 8;
2. il piano di test aggiornato comprendente le verifiche sulla rispondenza dei protocolli di autenticazione informatica a quanto previsto dalle regole tecniche e sull'adeguatezza ed usabilità degli strumenti e dalle tecnologie di autenticazione informatica - di cui all'articolo 6, comma 2, del DPCM - e di quant'altro concorre nel processo di autenticazione, per i quali si chiede l'autorizzazione all'uso;
3. la documentazione delle prove di collaudo interno effettuate secondo il piano di test di cui al punto precedente;
4. un documento contenente le modifiche da apportare al manuale operativo;
5. un documento contenente le modifiche da apportare al piano per la sicurezza di cui all'articolo 11, comma 1, lettera e) del DPCM.

L'Agenzia, sulla base del piano di test aggiornato, può effettuare verifiche sulla rispondenza dei protocolli di autenticazione informatica a quanto previsto dalle regole tecniche e sulla adeguatezza ed usabilità degli strumenti e dalle tecnologie di autenticazione informatica di cui all'articolo 6, comma 2, del DPCM - per i quali si chiede l'autorizzazione all'uso. A tal fine, i richiedenti, fin dalla presentazione della domanda di accreditamento, mettono a disposizione dell'Agenzia un ambiente di prova.
Le prove possono essere ripetute anche in ambiente di produzione.
Nel corso delle prove l'Agenzia può richiedere l'esecuzione di prove integrative rispetto a quelle previste dal piano di test, al fine di accertare eventuali aspetti non evidenziati, in tutto o in parte, dal predetto piano.
Per quanto riguarda i sistemi di autenticazione informatica, l'Agenzia, ai sensi del

comma 2 dell'articolo 6 del DPCM 24 ottobre 2014, esamina la documentazione presentata e l'esito degli eventuali test effettuati e, tenuto conto del rapporto di conformità o della relazione tecnica di cui al successivo paragrafo 8, valuta la sicurezza del sistema di autenticazione informatica assegnando il relativo livello di sicurezza di cui all'articolo 6 comma 1 del DPCM.

Qualora la valutazione dell'Agenzia circa il livello di sicurezza cui collocare le credenziali differisca da quanto indicato dal richiedente nella documentazione prevista al paragrafo 3, lettera t) dell'allegato al presente regolamento, l'Agenzia, prima di prendere una decisione definitiva, contatta il referente del richiedente per consentirgli di presentare, nei termini indicati dalla stessa, eventuali controdeduzioni.

L'esito di tale valutazione è comunicato formalmente dall'Agenzia al richiedente che, qualora decida di accettarlo, trasmette comunicazione in tal senso all'Agenzia allegando copia del manuale operativo e del piano della sicurezza aggiornati e rende nota la decisione dell'Agenzia pubblicando entro 10 giorni i riferimenti del sistema di autenticazione informatica nella sezione del proprio sito web istituzionale, di cui al paragrafo 4 del presente regolamento.

I richiedenti si conformano alle valutazioni dell'Agenzia pena l'adozione dei provvedimenti di cui all'articolo 12 del DPCM.

7. Vigilanza

Nell'ambito delle attività di vigilanza di cui all'articolo 4 comma 2 del DPCM, l'Agenzia verifica la persistenza dei requisiti previsti per l'accreditamento e la correttezza di quanto dichiarato nei documenti depositati.

La vigilanza è svolta attraverso l'esame della documentazione aggiornata in possesso dell'Agenzia, l'analisi dei documenti di riepilogo delle attività svolte dal gestore accreditato, la verifica della validità delle certificazioni di cui all'articolo 10 comma 3, lettere f) e h) del DPCM, l'esecuzione di verifiche ispettive da parte dell'Agenzia che può avvalersi anche di soggetti terzi con idonee competenze dalla stessa incaricati e designati quali responsabili del trattamento dei dati personali ai sensi dell'articolo 29 del Codice per la protezione dei dati personali, nel seguito "Codice".

Inoltre, nell'ambito dell'attività di vigilanza, l'Agenzia può ripetere le prove previste dal piano di test presentato in fase di accreditamento ed aggiornato ad ogni approvazione di nuove soluzioni tecnologiche, sia in ambiente di test che in ambiente di produzione.

Ai fini della vigilanza, pertanto, il gestore accreditato si obbliga a comunicare tempestivamente all'Agenzia ogni evento che modifichi i requisiti propri dell'accreditamento indicati nella documentazione in possesso dell'Agenzia.

Eventuali modifiche al manuale operativo devono essere sottoposte all'Agenzia per l'approvazione prima della loro adozione. L'Agenzia, se approva le modifiche al manuale operativo, lo sottoscrive con firma elettronica e lo pubblica sul proprio sito istituzionale

con le informazioni atte a identificare il gestore.

Alla scadenza dei certificati ISO/IEC 27001 e UNI EN ISO 9001 il gestore si obbliga a trasmettere all'Agenzia il nuovo certificato rilasciatogli ed inoltre, nel corso di validità dello stesso, annualmente, le risultanze delle verifiche periodiche di mantenimento.

Almeno ogni 24 mesi, a partire dalla stipulazione della convenzione, il gestore accreditato si sottopone ad una verifica di conformità del proprio sistema di gestione dell'identità SPID a quanto previsto nel DPCM da parte di un Ente di certificazione accreditato da un Ente Unico di Accreditamento Nazionale istituito a fronte del Reg. UE 765/2008 firmatario degli accordi di Mutuo riconoscimento per i Sistemi di Gestione (MS).

I gestori accreditati si impegnano a trasmettere all'Agenzia l'esito della verifica redatto in lingua inglese dall'organismo di valutazione entro tre giorni dalla ricezione.

Per l'esecuzione delle verifiche ispettive, il gestore accreditato si obbliga a prestare la massima collaborazione e a consentire l'accesso all'Agenzia, o a soggetti terzi dalla stessa incaricati, presso le strutture, proprie o di terzi, dedicate alle diverse fasi di erogazione dei servizi. L'Agenzia emana delle linee guida sulla vigilanza consultabili dal proprio sito istituzionale.

L'Agenzia si riserva, inoltre, la facoltà di richiedere al gestore accreditato ogni ulteriore documento correlato all'espletamento del processo di gestione dei servizi, che consideri necessario per poter svolgere le previste attività di vigilanza.

In caso vengano riscontrate difformità nel corso dell'attività di vigilanza, l'Agenzia indica al gestore le modalità e il termine per la loro risoluzione. In caso di particolare gravità, o nel caso di mancato rispetto del termine assegnato per l'eliminazione delle difformità riscontrate, l'Agenzia invia una diffida ad adempiere, indicando un nuovo termine, trascorso il quale dispone l'immediata revoca dell'accreditamento e la pubblicazione dell'informazione nell'elenco.

Nel caso in cui nel corso della vigilanza sorgano dubbi su possibili violazioni della normativa sulla protezione dei dati personali, l'Agenzia ne informa tempestivamente il Garante per la protezione dei dati personali.

8. Rapporto di conformità

L'Agenzia, entro il 31 dicembre 2016, predispone le norme tecniche e i criteri di accreditamento e individuazione degli organismi di certificazione, accreditati dall'Ente Unico di Accreditamento Nazionale istituito a fronte del Reg. UE 765/2008 e riconosciuto a fronte del medesimo Regolamento in uno dei Paesi dell'Unione Europea firmatario dei patti di mutuo riconoscimento per le norme tecniche citate, che effettuano la valutazione di conformità dei sistemi di autenticazione informatica ai livelli di sicurezza di cui all'Art. 6 comma 1 del DPCM.

I soggetti che presentano domanda di accreditamento dell'identità digitale sottopongono i propri sistemi di autenticazione informatica alla valutazione dei predetti organismi di certificazione i quali rilasciano il relativo rapporto di conformità.

In sede di prima applicazione, e nelle more della predisposizione delle norme tecniche e dei criteri di accreditamento sopra citati o dell'accreditamento di almeno due organismi di certificazione, i soggetti sono tenuti ad allegare alla domanda di valutazione di cui al paragrafo 6, in luogo del previsto rapporto di conformità, una relazione tecnica dettagliata che evidenzi il livello di sicurezza, così come definito all'Art. 6, comma 1 del DPCM, del sistema di autenticazione informatica, e si impegnano a sottoporre i propri sistemi di autenticazione informatica alla valutazione entro il termine massimo di quattro mesi dalla data di accreditamento del secondo organismo di certificazione dandone comunicazione all'Agenzia.

I gestori dell'identità trasmettono all'Agenzia il rapporto di conformità, che costituisce elemento per la valutazione del livello di sicurezza del sistema di autenticazione informatica, entro il termine massimo di 10 giorni dalla data del rilascio.

9. Ristoro dei costi

Al fine del ristoro dei costi sostenuti dall'Agenzia previsto dall'articolo 4 del DPCM, l'Agenzia determina entro il mese di aprile di ogni anno i costi derivanti dall'attività di vigilanza dei gestori di identità afferenti l'anno solare precedente. Tali costi sono ripartiti in misura del 50% in ugual misura su tutti i gestori dell'identità digitale attivi presenti nel registro di cui all'Art.1 del DPCM nel corso dell'anno solare di riferimento e sui gestori dell'identità digitale revocati o cessati nel corso del medesimo periodo. La quota restante è ripartita, sempre fra detti gestori dell'identità digitale, in misura proporzionale al numero di identità digitali gestite. Nel computo del numero di identità digitali gestite non rientrano le identità revocate o scadute precedentemente all'anno solare per il quale sono calcolati i costi sostenuti dall'Agenzia.
Sempre entro il mese di aprile di ogni anno, l'Agenzia determina i costi inerenti le procedure di accreditamento di cui al paragrafo 3 nel corso dell'anno di riferimento che sono ripartiti in ugual misura fra i gestori dell'identità digitale accreditati nel medesimo periodo.

10. Entrata in vigore

Il presente regolamento entra in vigore il 1 agosto 2016.

Allegato

"DOCUMENTAZIONE PER L'ACCREDITAMENTO"

Il presente allegato 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 devono allegare alla domanda di accreditamento.
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

Unitamente alla domanda di accreditamento devono essere presentati i seguenti documenti amministrativi:

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:
    a) 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;
    b) 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;
    c) 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:
    a) 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;
    b) 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 a quanto prescritto nei precedenti punti 1 e 2, 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, può 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 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;

i) 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%.

l) al fine di dimostrare la capacità di risarcire eventuali danni arrecati, documentazione attestante la disponibilità di risorse finanziarie e/o 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, determinate nei seguenti valori: 7,5 milioni di euro, fino a 100.000 identità; 10 milioni di euro, fino 1 milione di identità; 13 milioni di euro fino a 3 milioni di identità; 15 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. L'eventuale 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, una dichiarazione inerente eventuali aggiornamenti inerenti la documentazione presentata (disponibilità di risorse finanziarie e/o polizza assicurativa) congiuntamente ad una dichiarazione inerente il numero di identità digitali attive e scadute o revocate da meno di dodici mesi. In assenza di aggiornamenti, detta dichiarazione deve comunque essere presentata con cadenza annuale. L'eventuale polizza assicurativa deve prevedere una copertura non inferiore a 150.000 euro per singolo sinistro.;

2. Documenti tecnici e organizzativi generali

Unitamente alla domanda di accreditamento devono essere presentati i seguenti documenti:

m) piano di test per le verifiche dell'Agenzia previste al par. 3 lettera c);

il piano di test dovrà prevedere prove miranti ad effettuare verifiche sul comportamento del sistema in merito ai seguenti aspetti relativi al protocollo di autenticazione:

- formato della *SAML response* e delle asserzioni emesse;
- binding;
- gestione dei messaggi di richiesta (*AuthnRequest*) in presenza/assenza *AttributeConsumingServiceIndex*;
- gestione dei messaggi di richiesta (*AuthnRequest*) in presenza *AssertionConsumerServiceIndex*;
- gestione dei messaggi di richiesta (*AuthnRequest*) in presenza degli attributi *AssertionConsumerServiceURL e ProtocolBinding*;
- gestione dell'informativa utente sugli attributi richiesti;
- gestione dei livelli SPID 1, 2 e 3;
- gestione delle sessioni:
- gestione anomalie sui messaggi di richiesta;
- gestione dei metadata dei gestori di servizi;
- gestione dei log;

n) documentazione delle prove di collaudo interno comprovanti l'aderenza dei protocolli di autenticazione adottati a tutti gli aspetti previsti dalle regole tecniche;

o) domanda di autorizzazione all'uso dei sistemi di autenticazione informatica (punto 6) avente come allegati:

1. Il rapporto di conformità di cui al punto 8 del regolamento, o in via transitoria, una relazione tecnica dettagliata che evidenzi il livello di sicurezza del sistema di autenticazione informatica proposto; Tale relazione tecnica dovrà specificare le modalità di utilizzo ed il funzionamento logico dei dispositivi proposti, dando evidenza degli standard di riferimento adottati. Dovranno inoltre essere riportati le modalità di esecuzione e gli esiti dei controlli effettuati sui rischi previsti dallo standard ISO/IEC 29115 relativi alla gestione delle credenziali (credential management phase);

2. piano dei test aggiornato e la documentazione delle prove di collaudo interno dei dispositivi usati per l'autenticazione informatica;

si precisa che, al fine di distinguere i sistemi di autenticazione soggetti ad autorizzazione nello scambio documentale con l'Agenzia, ad ogni soluzione presentata deve essere assegnato un riferimento univoco composto da un codice identificativo univoco alfanumerico (massimo 6 caratteri) seguito dalla sequenza

aaaa_ss_mm ,dove *aaaa* rappresenta l'anno in cui il sistema di autenticazione è presentato 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 soluzione;

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 in cui devono essere particolarmente curate le modalità d'uso del sistema di autenticazione, le modalità con cui l'utente può richiedere la sospensione o la revoca delle credenziali, le cautele che l'utente deve adottare per la conservazione e protezione delle credenziali. La guida utente può costituire documento a se stante.
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 – tutti dipendenti diretti del gestore - di cui al punto 7 del paragrafo 2 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 e una specifica esperienza professionale almeno quinquennale se in possesso di laurea tecnica in ambito informatico ovvero di almeno otto anni;

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) relazione che descrive i trattamenti di dati personali effettuati riportandone le informazioni essenziali e le misure messe in atto per conformare tali trattamenti alla normativa sulla protezione dei dati personali, con particolare riferimento ai principi di necessità, pertinenza e non eccedenza dei dati, nonché di correttezza nel trattamento e all'obbligo di rendere previa e idonea informativa agli utenti del servizio di identificazione elettronica;

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. 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 r) 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;

ff) le informazioni fornite ai titolari dell'identità digitale SPID inerenti i rischi derivanti dal possesso della stessa, le cautele e le contromisure adottabili dagli stessi;

gg) dichiarazione di impegno, sottoscritto dal legale rappresentante, a corrispondere all'Agenzia quanto dovuto per il ristoro dei costi di cui al paragrafo 9, entro 120 giorni dalla richiesta.

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 già decorso, purché nella domanda di accreditamento dichiarino espressamente che essa è ancora attuale e la documentazione soddisfi quanto previsto per l'accreditamento.

I gestori, se soggetti pubblici, non presentano la documentazione elencata dalla lettera a) alla lettera i), ma 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 dipendente preposto alle attività necessarie all'esercizio e sua allocazione;

e) attribuzione delle responsabilità ai dipendenti del gestore;

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 della conservazione delle credenziali fornite agli utenti;

u) le idonee misure di sicurezza adottate, ai sensi dell'articolo 31 del Codice, rispetto ai rischi di accesso improprio, distruzione o perdita dei dati personali o della loro disponibilità e integrità, furto, uso abusivo, alterazione o usurpazione di identità, ripudio o disconoscimento di una transazione, trattamento non consentito o non conforme alle finalità della raccolta.

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 incaricato.
