Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

REGOLAMENTO

RECANTE LE MODALITÀ PER L'ACCREDITAMENTO E LA VIGILANZA SUI SOGGETTI PUBBLICI E PRIVATI CHE SVOLGONO ATTIVITÀ DI GESTIONE DEI SERVIZI DI REGISTRAZIONE E DI MESSA A DISPOSIZIONE DELLE CREDENZIALI E DEGLI STRUMENTI DI ACCESSO IN RETE DI CUI ALL'ARTICOLO 64, COMMA 2-TER, DEL DECRETO LEGISLATIVO 7 MARZO 2005, N. 82.

Premessa

L'art. 64 comma 2-ter del decreto legislativo 7 marzo 2005, n. 82 e s.m.i. (Codice dell'amministrazione digitale, di seguito "CAD") attribuisce all' Agenzia per l'Italia Digitale (di 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".*

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;

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.";

In attuazione dell'art. 10 del DPCM 24 ottobre 2014 (nel seguito DPCM), sopra richiamato, il presente regolamento definisce le modalità per l'accreditamento presso l'Agenzia e per la vigilanza

dei soggetti di cui all'art. 64 comma 2-ter del CAD.

1. Accreditamento dei gestori di 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 tale riconoscimento, devono:

1. dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere l'attività di gestore di identità digitale nell'ambito del Sistema di cui all'Art64 comma 2-bis;
2. utilizzare 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.

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

1. avere forma giuridica di società di capitali e un capitale sociale di almeno 5.000.000 Euro;
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 recante il Testo unico delle leggi in materia bancaria e creditizia".

Le modalità per dimostrare il possesso dei requisiti sopra indicati, la documentazione richiesta ed i criteri di valutazione adottati per espletare il processo di accreditamento sono indicati in appositi documenti consultabili per via telematica, sul sito istituzionale dell'Agenzia.

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

Oltre alla domanda, devono essere depositati presso l'Agenzia i documenti previsti nel documento "ACCREDITAMENTO DEI SOGGETTI CHE SVOLGONO L'ATTIVITÀ DI GESTORI DI IDENTITA' DIGITALE AI SENSI DEL DPCM 24 OTTOBRE 2014 - DOCUMENTAZIONE PER L'ACCREDITAMENTO", pubblicato sul

sito istituzionale dell'Agenzia.

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 f) del DPCM, come soggetti abilitati ad operare in qualità di gestori di 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. Per la verifica del rispetto delle Norme ISO/IEC 27001, 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 all'indirizzo protocollo@pec.agid.gov.it. Con le medesime modalità deve

essere predisposta la documentazione per l'accreditamento.

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 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:
    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

    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.
8. l'elenco dei documenti allegati, con preciso riferimento a quanto indicato nel documento "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) La domanda di accreditamento si considera accolta qualora non venga comunicato al richiedente il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa;

b) L'agenzia nel corso dell'istruttoria può effettuare verifiche sulla rispondenza dei protocolli di autenticazione a quanto previsto dalla regole tecniche e prove sull'adeguatezza e l'usabilità delle soluzioni tecnologiche di autenticazione informatica. Le prove, effettuate sulla base di un piano di test proposto dal gestore, possono essere condotte in un ambiente di test-bed, 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-bed dovrà essere mantenuto operativo, ai fini delle vigilanza, per tutta la durata dell'esercizio del servizio;

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

d) Il termine di novanta giorni di cui al periodo precedente, 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 prova predisposto, a seguito di richiesta di prove integrative ;

e) Al termine dell'istruttoria, l'Agenzia accoglie la domanda ovvero la respinge con

provvedimento motivato e ne dà apposita comunicazione al richiedente.

f) 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 di identità 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 delle soluzioni di autenticazione approvate 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 domanda per l'approvazione delle soluzioni tecnologiche di cui all'art.6 comma 2 del DPCM

Gli strumenti e le tecnologie di autenticazione devono essere presentati all'AgID che avvia l'iter di valutazione e approvazione della soluzione tecnologica proposta.

La richiesta di approvazione, 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 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 medesime modalità previste per l'accreditamento.

La domanda deve allegare:

1. il rapporto di conformità delle nuova soluzione tecnologica di autenticazione informatica che intende adottare, rilasciato da un ente certificazione, accreditato 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, secondo quanto indicato al successivo Art.8, rispetto ai livelli di sicurezza definiti all'Art.6 comma 1 del DPCM;
2. nel caso di protocollo conforme alle regole tecniche, documentazione delle prove di collaudo interno comprovanti l'aderenza a tutti gli aspetti previsti dalle stesse regole tecniche;
3. il piano di test aggiornato comprendente le verifiche sulle funzionalità aggiunte;
4. documento riportante le modifiche da apportare al manuale operativo, ovvero l'intero manuale operativo se ma presentato in precedenza;
5. documento riportante le modifiche da apportare al piano per la sicurezza di cui all'articolo 11, comma 1, lettera e) del DPCM, ovvero l'intero piano per la sicurezza se mai presentato in precedenza;

Nel caso di introduzione di un nuovo protocollo di autenticazione l'Agenzia può effettuare

verifiche sulla rispondenza di questi a quanto previsto dalla regole tecniche sulla base dell'aggiornamento del piano di test;

Nel caso di introduzione di nuovo un nuovo dispositivo per l'autenticazione di cui all'art.6 comma 2 del DPCM l'Agenzia può effettuare verifiche sull'adeguatezza e l'usabilità delle soluzioni tecnologiche di autenticazione informatica, sulla base dell'aggiornamento del piano di test.

In entrambi i casi precedenti le prove possono essere condotte sull'ambiente di test-bed aggiornato a tale scopo dal gestore, ed eventualmente ripetute in ambiente di produzione.

Nel corso delle prove l'Agenzia può richiedere l'esecuzione di prove integrative rispetto a quelle previste dell'aggiornamento del piano di test, al fine di accertare eventuali aspetti non evidenziati, in tutto o in parte, dal predetto aggiornamento del piano di test;

Nel caso dell'introduzione di nuovi strumenti di autenticazione, l'Agenzia, ai sensi del comma 2 dell'articolo 6 del DPCM 24 ottobre 2014, valuta il contenuto del piano per la sicurezza e, tenuto conto del rapporto di conformità, colloca le credenziali al livello di sicurezza ritenuto adeguato. La decisione è comunicata formalmente al richiedente che, qualora decida di accettare la classificazione dell'Agenzia, trasmette comunicazione in tal senso allegando copia del manuale operativo e piano della sicurezza aggiornati e rende pubblica la decisione dell'Agenzia pubblicando entro 10 giorni i riferimenti alla nuova soluzione tecnologica nella sezione del proprio sito web, di cui al paragrafo 4 punto 3.

7. Vigilanza

Nell'ambito delle attività di vigilanza di cui all'articolo 4 comma 2 del DPCM, l'Agenzia verifica la persistenza del possesso dei requisiti previsti per l'accreditamento e della veridicità 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 del possesso delle previste certificazioni e l'esecuzione di verifiche ispettive da parte dell'Agenzia, o di soggetti terzi dalla stessa incaricati.

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-bed 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'Italia Digitale 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, 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 stipula della convenzione, il gestore accreditato deve sottoporsi 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 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) .

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.

8. Disposizioni transitorie e finali

I soggetti, alla data di presentazione della domanda di accreditamento, mettono a disposizione dell'Agenzia un ambiente di prova per le verifiche della rispondenza dei protocolli di autenticazione a quanto previsto dalla regole tecniche e per le prove sull'adeguatezza e l'usabilità delle soluzioni tecnologiche di autenticazione informatica presentate.

I soggetti che presentano domanda di accreditamento prima della disponibilità di almeno due enti di certificazione accreditati 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. possono depositare un'autocertificazione di conformità delle soluzioni tecnologiche di autenticazione informatica che si intendono adottare rispetto ai diversi livelli di sicurezza definiti all'Art.6 comma 1 del DPCM.

Il rapporto di conformità delle soluzioni tecnologiche di autenticazione informatica, di cui al paragrafo 6.1, rilasciato da un ente di certificazione accreditato 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, deve comunque essere presentato entro i quattro mesi successivi alla data di accreditamento o alla decorrenza della disponibilità di almeno due enti di certificazione accreditati. L'Agenzia, entro il 30 Giugno 2015, predisporrà, con l'ausilio di un ente di certificazione accreditato 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. i criteri di accreditamento ed individuazione degli Enti di certificazione.

L'Agenzia, ai sensi del comma 2 dell'articolo 6 del DPCM 24 ottobre 2014, valuta il rapporto di conformità e colloca le credenziali al livello di sicurezza ritenuto adeguato. La decisione è comunicata formalmente al richiedente che, qualora decida di accettare la classificazione dell'Agenzia, trasmette comunicazione in tal senso allegando copia del manuale operativo e piano della sicurezza aggiornati e rende pubblica la decisione dell'Agenzia pubblicando entro 10 giorni i riferimenti alla nuova soluzione tecnologica nella sezione del proprio sito web, di cui al paragrafo 4 punto 3.