A tutti gli Organismi di Certificazione accreditati

Loro Sedi

Ns. rif.: DC2016SSV439 *Milano,* 15/12/2016

Oggetto: **Dipartimento Certificazione e Ispezione Accredia - Circolare N° 35/2016**
Schema di accreditamento degli Organismi di Certificazione, per il processo di certificazione degli operatori SPID, secondo le disposizioni dell'Agenzia per l'Italia Digitale

1. Introduzione

SPID è il "Sistema Pubblico per la gestione dell'Identità Digitale". Si tratta di uno strumento che è stato disegnato in conformità al Regolamento eIDAS, e rappresenta una delle iniziative trasversali della Strategia per la Crescita Digitale 2014-2020.
SPID è un sistema aperto attraverso il quale soggetti pubblici e privati - previo accreditamento (processo della PA) da parte dell'Agenzia per l'Italia Digitale - possono offrire servizi di identificazione elettronica a cittadini e imprese.
I prestatori di tali servizi hanno il compito di garantire la corretta registrazione e messa a disposizione delle credenziali e degli strumenti di accesso in rete (PA) nei riguardi di cittadini e imprese.
Con l'istituzione del Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese (SPID) le pubbliche amministrazioni potranno consentire l'accesso in rete ai propri servizi, oltre che con lo stesso SPID, solo mediante la carta d'identità elettronica e la carta nazionale dei servizi. Il termine entro il quale la disposizione entrerà in vigore sarà stabilito con il decreto attuativo. La possibilità di accesso con carta d'identità elettronica e carta nazionale dei servizi resta comunque consentito indipendentemente dalle modalità predisposte dalle singole amministrazioni.

2. Contesto Normativo

Primo provvedimento di attuazione previsto dall'articolo 64, comma 2-sexies del D.lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale) è il decreto della Presidenza del Consiglio dei Ministri 24 ottobre 2014, pubblicato sulla Gazzetta Ufficiale n. 285 del 9 dicembre 2014.
Il 22 Luglio 2016, con la Determinazione n.189/2016, sono stati emanati gli aggiornamenti del "Regolamento SPID: accreditamento gestori" e del Regolamento modalità attuative". Il nuovo regolamento che norma le modalità di accreditamento è entrato in vigore il 1 agosto 2016. Ai fini della trasmissione all'Agenzia della documentazione è stato reso disponibile il certificato contenente la chiave per cifrare la documentazione riservata.
Restano vigenti gli altri due regolamenti previsti dall'articolo 4, commi 2, 3 e 4, del suddetto DPCM 24 ottobre 2014 che sono stati emanati il 28 luglio 2015, con la Determinazione n. 44/2015.
Con l'aggiornamento dei regolamenti si chiariscono alcuni aspetti relativi al processo di accreditamento (della PA) ed autorizzazione e si definiscono alcune modalità operative che tutti i gestori sono tenuti ad adottare.
Il 7 ottobre 2016 è stata pubblicata la Determinazione 239/2016 che consente anche ai privati di accedere al sistema SPID in qualità di fornitori di servizi

3. Nota per la lettura dello schema

Ovunque sia riportato il riferimento ad una Norma referenziata con la revisione o l'anno di emissione, vale esattamente quella Norma. Ove, invece, le Norme non siano referenziate con lo stato di revisione e/o l'anno

Sede operativa e amministrativa: Via Tonale, 26 | 20125 Milano - Italy | Tel. +39 02 2100961 | Fax +39 02 21009637
Sede legale: Via Guglielmo Saliceto, 7/9 | 00161 Roma - Italy | Tel. +39 06 8440991 | Fax +39 06 8841199
milano@accredia.it | www.accredia.it | Partita IVA - Codice Fiscale 10566361001

di emissione, dovrà essere considerata applicabile la Norma vigente al momento dello svolgimento delle attività operative: sia di accreditamento, sia di sorveglianza, sia di rinnovo.

4. Processo di Accreditamento degli Organismi di Certificazione

Di seguito si indicano le modalità previste per l'accreditamento degli Organismi di Certificazione e si forniscono alcune indicazioni mandatorie in ordine al processo di certificazione degli operatori SPID che intendono ottenere l'accreditamento pubblico di AgID.

1) Norma e regole di Certificazione AGID

Norma di Accreditamento	UNI CEI EN ISO/IEC 17065 (revisione corrente) integrata dalla Norma ETSI EN 319 403 (revisione corrente). Per richiedere l'accreditamento per lo schema SPID gli Organismi di Certificazione debbono essere già accreditati per lo schema eIDAS. L'accreditamento sarà rilasciato come estensione dello schema PRD.
Norma di Certificazione	ISO/IEC 27001 e Norma ETSI EN 319 401, con scopo di certificazione comprendente i servizi SPID, con copertura di tutti i siti interessati e di tutti i fornitori di servizi "underpinning" a questo riconducibili. Norma ISO/IEC 29115:2013 – "Entity authentication assurance program" [la conformità alla Norma citata sarà oggetto di valutazione a seguito di aggiornamento del presente schema, non appena sarà pubblicata la relativa Norma interpretativa ed attuativa UNI]. Requisiti tecnici definiti con il Regolamento di attuazione UE 2015/1502 della Commissione. Ove l'Organismo di Certificazione che ha rilasciato la certificazione a fronte della Norma ISO/IEC 27001 sia diverso da quello che svolge le attività riferite alla verifica di conformità di cui al presente schema, dovrà essere, comunque, un organismo accreditato da un Ente di Accreditamento nazionale ai sensi del Reg. (UE) 765/2008.
Criteri di competenza del Gruppo di Verifica dell'OdC	I membri del gruppo di audit debbono essere qualificati come segue: • Frequenza e superamento dello specifico corso SPID organizzato da AgID per la qualifica ETSI EN 319 401. • Qualifica come Lead Auditor ISO/IEC 27001. • Qualifica come Auditor UNI CEI EN ISO 20000-1:2012 ovvero qualifica come Auditor SGQ EA 33 e conoscenza architettura ITIL, rilasciata dallo stesso Organismo di Certificazione; • Conoscenza del DPCM 24 Ott. 2014 "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". • Conoscenza del Regolamento di attuazione UE 2015/1502 della Commissione.

Valutazioni di robustezza del sistema IT	In merito all'uso di infrastrutture "cloud", l'operatore SPID dovrà dare evidenza della capacità di reale "controllo operativo" di tali servizi e della adesione alle eventuali indicazioni di AgID in merito all'ubicazione dei server fisici e sui repository [sistemi di memorizzazione] nei quali avviene l'archiviazione dei dati/informazioni inerenti l'identificazione delle Persone Fisiche e Giuridiche. I controlli operativi, riferiti alla Norma ISO/IEC 27001 e relativi ai processi di VA (Vulnerability Assessment) e PT (Penetration Test), dovranno essere svolti da strutture interne o esterne all'operatore SPID, ovvero da strutture interne o esterne agli stessi Organismi di Certificazione, la cui qualificazione deve essere basata, a partire dal 01 Giugno 2017, sulla Norma ISO/IEC 17025 e che, sin da subito, forniscano evidenza almeno: - della chiara individuazione e diligente applicazione dei requisiti inerenti la metodologia di valutazione tecnica adottata, che richiami, preferibilmente, l'applicazione dei requisiti ISO/IEC TR 27008-1; - della competenza formale (quali qualifiche, da chi rilasciate, quale esperienza nel settore) delle Risorse Umane addette a tali test; e - della qualifica (certificazione in gergo IT) dei SW utilizzati (almeno la garanzia che le versioni siano compatibili e aggiornate ai rilasci dei SO e delle applicazioni da analizzare del operatore SPID). La valutazione di cui sopra, ove il Laboratorio di test sia scelto dall'operatore SPID è di pertinenza dello stesso operatore SPID e sarà oggetto di valutazione nell'ambito del processo di audit da parte dell'Organismo di Certificazione. Diversamente, se il Laboratorio sarà stato scelto dall'Organismo di Certificazione, si applicheranno le regole di qualifica previste dalla Norma di accreditamento 17065. A partire dal 01 Giugno 2018 tali Laboratori, da chiunque scelti, dovranno essere accreditati secondo la Norma ISO/IEC 17025.
Indicazioni specifiche sulla registrazione di NC	La registrazione di non conformità maggiori sistemiche o sui controlli operativi (ISO/IEC 27001 e/o ETSI EN 319 401) o sui requisiti riferiti al Regolamento eIDAS o sul Regolamento di Attuazione UE 2015/1502 della Commissione, che pregiudicano il corretto svolgimento dei servizi fiduciari di identificazione e fornitura dell'accesso SPID, deve condurre, a seconda della situazione rilevata, anche alla revoca della certificazione, non solo alla sospensione. Inoltre, nel caso di sospensione (e ovviamente di revoca) deve essere indicato all'operatore SPID che egli stesso è responsabile della comunicazione di tale evento ad AgID, ma che analoga comunicazione viene trasmessa dallo stesso OdC immediatamente ad AgID ed anche ad ACCREDIA. La registrazione da parte dell'Organismo di Certificazione di eventuali NC maggiori dovrà prevedere una risposta immediata, entro 5 gg lavorativi, con l'indicazione dei provvedimenti adottati per tamponare le criticità individuate. Entro i successivi 5 gg lavorativi dovrà essere definita l'analisi delle cause radice e la pianificazione delle azioni necessarie per eliminarle e/o mitigarle in

	modo da avere come risultato un rischio di disservizio / non conformità valutato accettabile. La mancata comunicazione di modifiche dell'organizzazione o dell'infrastruttura IT del operatore SPID, che abbiano un impatto diretto sulla sicurezza delle informazioni dell'infrastruttura oggetto di valutazione, è da considerare come NC Maggiore e come tale va trattata, valutando in modo formale, quindi con adeguata registrazione sul rapporto di verifica, se tali modifiche possano aver creato delle brecce di sicurezza nel periodo intercorrente dalla applicazione di tali modifiche sino alla data dell'audit in corso. L'operatore SPID dovrà collaborare attivamente a tale analisi. In casi di grave perdita di fiducia nella sicurezza delle informazioni gestita dall'operatore SPID, vista la responsabilità oggettiva dell'Organismo di Certificazione nei confronti di ACCREDIA e di AgID, lo stesso Organismo di Certificazione dovrà fare una specifica segnalazione ad ACCREDIA per ricevere specifiche istruzioni.
Criteri di competenza del Decision maker	Per almeno un membro dell'Organo di Delibera è richiesta agli Organismi di Certificazione la dimostrazione della: • Qualifica interna come ispettore UNI CEI ISO/IEC 27001:2014, rilasciata in conformità alla ISO 27006 in vigore e conoscenza della Norma ETSI EN 319 401; • Qualifica interna come Auditor UNI CEI EN ISO 20000-1:2012 ovvero qualifica come Auditor SGQ EA 33 e conoscenza architettura ITIL; • Conoscenza del DPCM 24 Ottobre 2014 – SPID; • Conoscenza del servizio IT SPID.
Criteri di competenza per il personale addetto alla funzione commerciale	Il personale dell'Organismo di Certificazione addetto alla gestione contrattuale con i potenziali clienti SPID dovrà essere qualificato internamente sulla conoscenza del servizio e delle relative criticità, nonché sul dimensionamento dell'offerta, in funzione della complessità dell'operatore.
Tempi di verifica	La valutazione di un operatore SPID si svolge in due specifici momenti, secondo un ciclo biennale: • prima valutazione e/o rinnovo; • sorveglianza periodica, La valutazione di sorveglianza necessita un terzo del tempo della valutazione iniziale e/o di rinnovo (che richiedono lo stesso tempo di valutazione). Gli Organismi di Certificazione effettueranno le verifiche di certificazione SPID secondo il seguente criterio: Se l'operatore che intende essere certificato come operatore SPID è già certificato per lo schema eIDAS, la verifica sarà limitata all'accertamento dell'applicazione dei requisiti sistemici e dei controlli operativi della ETSI EN 319 401 specifici per SPID e dei requisiti ex Reg. 2015/1502. [In una seconda fase dello schema, verrà introdotta la conformità alla Norma UNI-UNINFO in fase di pubblicazione, finalizzata a sostanziare la conformità ai requisiti della norma UNI CEI EN ISO/IEC 29115:2015, che richiederà un tempo aggiuntivo

	di valutazione e porterà alla revisione del presente schema]. Inoltre, l'Organismo di Certificazione prenderà atto in tutte le verifiche, dell'esito delle valutazioni a fronte della Norma ISO/IEC 27001 rilevando eventuali NC maggiori da dover investigare. Per tale investigazione sarà necessario un tempo di audit pari a una sorveglianza. Per tali operatori, già qualificati eIDAS, la verifica a fronte della Norma ETSI EN 319 401 e Regolamento UE 2015/1502 richiederà 5 gg in sede iniziale e di rinnovo e 3 gg in sede di sorveglianza. Non sono previste riduzioni di alcun tipo su tali livelli minimi di tempo. Se l'operatore che intende essere certificato come operatore SPID non è in possesso di certificazione eIDAS, dovranno essere adottati i tempi necessari a tale certificazione più quelli per la verifica dell'applicazione del Reg. UE 2015/1502 (minimo due gg). Ove, nel processo di valutazione (iniziale, rinnovo, sorveglianza), dovessero emergere delle NC maggiori riferibili anche alla Norma ISO/IEC 27001 si dovrà effettuare una verifica su tale Norma, con un tempo minimo assimilabile ad una sorveglianza, per verificarne la robustezza sistemica e tecnica, tenendo conto delle sinergie/interazioni con la Norma ETSI EN 319 401. Non è possibile applicare alcun fattore di riduzione del tempo di audit. Tutte le fasi delle verifiche (inziali, di rinnovo e di sorveglianza) dovranno essere svolte presso le sedi degli operatori SPID. Gli Organismi di Certificazione potranno valutare, caso per caso, l'esigenza di tempo aggiuntivo, sulla base della complessità del processo di identificazione e fornitura dell'accesso SPID: - numero dei siti coinvolti; - coesistenza di altri servizi IT erogati dalla società che svolge la funzione di operatore SPID, architettura di controllo della complessità sistemica e tecnica di tali servizi (sulla base dei criteri ITIL); - maturità e architettura del sistema di Business Continuity e Disaster Recovery; - presenza di fornitori "underpinning critici" per processi in outsourcing; - modalità e maturità nella gestione dell'outsourcing; - precedenti criticità severe registrate etc. Si applica il documento IAF MD01 per certificazione multi-site. Si applica il documento IAF MD 04 per l'utilizzo di procedure CAAT.
Certificato e rapporto	Il certificato avrà validità biennale, con obbligo di sorveglianza annuale. Lo scopo di certificazione dovrà riportare il riferimento al servizio di Identificazione e fornitura dell'accesso SPID in conformità al DPCM 24 Ott. 2014, al presente schema di certificazione e ai requisiti applicabili del Regolamento UE eIDAS. Il rapporto di Audit verrà sottoscritto dal Gruppo di Audit dell'Organismo di Certificazione al termine della riunione finale e ne verrà lasciata copia all'operatore SPID.

	In un periodo massimo di quindici giorni, l'Organismo di Certificazione si esprimerà sulla conferma o necessità di correzione / integrazione di tale rapporto. Una volta approvato definitivamente il rapporto, l'Organismo di Certificazione potrà emettere il proprio certificato di conformità, ma anche negare la certificazione, comunicando allo operatore SPID le ragioni di tale decisione. Dopo l'approvazione del Rapporto del Gruppo di Audit, per come eventualmente integrato a fronte delle decisioni dell'Organismo di Certificazione, lo stesso Organismo provvede alla firma digitale con marca temporale dello stesso rapporto e ad inviarlo via PEC al operatore SPID, affinché quest'ultimo possa inviarlo ad AgID per il prosieguo dell'iter di accreditamento pubblico come operatore SPID accreditato AgID. Per i rapporti di sorveglianza, pur valendo la stessa regola della conferma e dell'invio da parte dell'Organismo di Certificazione, dopo opportuna revisione e approvazione da parte del "Decision Maker" all'operatore SPID, via PEC, a fronte di firma digitale e marcatura temporale, non è richiesto che lo stesso operatore SPID ne invii copia ad AgID, se non dietro esplicita richiesta di quest'ultima, in quanto Autorità di Vigilanza. Il rapporto di valutazione iniziale e di rinnovo dovranno riportare la dicitura *Conforme all'Art. 24 e relativi requisiti del Regolamento UE 2014/910 eIDAS*.

2) Processo di Accreditamento ACCREDIA

Possono accreditarsi come Organismi di Certificazione per lo schema SPID solamente gli Organismi di Certificazione già in possesso di accreditamento eIDAS.

Documentazione da presentare ad ACCREDIA per l'esame documentale

a) Lista di riscontro predisposte dall'OdC per il GVI sulla base di analogo documento prodotto da AgID e lista di riscontro per la Norma ETSI EN 319 401 V2.1.1.;
b) Curricula degli ispettori e dei Decision Maker, da cui si deve si deve evincere rispettivamente: la frequenza e superamento del corso di formazione per Auditor organizzato da AgID e ACCREDIA e il rispetto dei requisiti di qualifica indicati nella sezione Decision Maker;
c) Modulo del Rapporto di Audit con dichiarazione in calce sulla conformità o meno allo schema SPID e al Regolamento eIDAS;
d) Attestato/Certificato rilasciato dall'OdC;
e) Lista delle prossime attività di verifica;
f) Procedura che descriva il processo di Valutazione per lo specifico schema SPID, comprensiva dei requisiti commerciali, requisiti tecnici di valutazione (iniziale, sorveglianza e rinnovo) e requisiti tecnici di delibera.
g) Ulteriori procedure interne per la gestione della pratica di certificazione;
h) Regolamenti contrattuali applicabili al processo di valutazione.

3) Mantenimento dell'Accreditamento

Per il mantenimento dell'accreditamento, durante l'intero ciclo di accreditamento, salvo situazioni particolari (Es: gestione reclami e segnalazioni, modifiche intervenute sullo schema di certificazione, cambiamenti nella struttura dell'Organismo…), verranno condotte le seguenti verifiche:

- se l'OdC ha emesso meno di 10 certificati nello schema di certificazione, devono essere effettuate una verifica in accompagnamento e una verifica in sede;

- se l'OdC ha emesso tra 11 e 50 certificati nello schema di certificazione, devono essere effettuate 2 verifiche in accompagnamento e 1 verifica in sede;
- se l'OdC ha emesso più di 51 certificati nello schema, devono essere effettuate 3 verifiche in accompagnamento e 1 verifica in sede.

Prescrizioni relative al processo di accreditamento

Condizione perché un OdC possa essere accreditato è il possesso dei requisiti di cui al Regolamento ACCREDIA RG-01 per l'accreditamento degli Organismi di Certificazione e di Ispezione e al Regolamento ACCREDIA RG-01-03 per l'accreditamento degli Organismi di Certificazione del Prodotto.

Accertato il possesso dei requisiti minimi, si darà avvio all'iter di accreditamento con la conduzione delle attività di verifica come previste nei Regolamenti di cui sopra e in conformità alle norme/documenti applicabili all'accreditamento.

Siamo a disposizione per chiarimenti e porgiamo cordiali saluti.

Con cordialità.

Il Direttore di Dipartimento
Dr. Emanuele Riva