Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri
Area Pareri, monitoraggio e vigilanza

VIGILANZA SUI SOGGETTI ISCRITTI NEGLI ELENCHI PUBBLICI

(*art. 14-bis, comma 2, lettera i del Codice dell'amministrazione digitale*)

MODALITÀ DI ESECUZIONE DELLE VERIFICHE SUI SOGGETTI QUALIFICATI O ACCREDITATI

30 MAGGIO 2017

Agenzia per l'Italia Digitale
Viale Liszt, 21
00144 Roma, Italia
t+39 06 85264.1
PEC: protocollo@pec.agid.gov.it
direzione.generale@agid.gov.it

INDICE

1 GENERALITÀ

1.1 STORIA DELLE MODIFICHE

Ed.	Descrizione delle modifiche	Data
1.0	Prima stesura	30/05/2017

1.2 RIFERIMENTI

[D.1] Decreto legislativo 7 marzo 2015, n. 82 e s.m.i. (Codice dell'amministrazione digitale)

[D.2] 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 e che abroga la direttiva 1999/93/CE

[D.3] DPCM dell'8 gennaio 2014 recante lo "Approvazione dello Statuto dell'Agenzia per l'Italia Digitale"

[D.4] Regolamento di organizzazione dell'Agenzia per l'Italia Digitale, approvato con DPCM 27 marzo 2017

[D.5] Determinazione del Direttore Generale N. 432/2016 del 30 dicembre 2016

[D.6] ENISA – Guidelines on supervision of qualified trust service providers – Final draft 0.4 September 2016

[D.7] ENISA- Incident reporting framework for eIDAS Article 19 – Decembre 2016

[D.8] UNI EN ISO 19011:2012 – Linee guida per audit di sistemi di gestione

1.3 TERMINI E DEFINIZIONI

AgID: Agenzia per l'Italia Digitale,

CAD: Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2015, n. 82, come modificato dal decreto legislativo 26 agosto 2016, n. 179.

CAB: Conformity Assessment Body – Organismo di certificazione di conformità accreditato da ACCREDIA o da altro ente di Accreditamento rientrante nell'ambito del Regolamento (CE) N. 2008/765, firmatario degli accordi di Mutuo riconoscimento nello schema specifico.

CAR: Conformity Assessment Report - Certificato di confromità rilasciato da un CAB.

gestore: il soggetto iscritto in uno o più elenchi tenuti da AgID ai sensi dell'art. 29 del CAD, al quale si applicano le funzioni di vigilanza

Regolamento UE 910/2014/Regolamento eIDAS: 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 e che abroga la direttiva 1999/93/CE.

verifica documentale: esame sistematico ed indipendente svolto attraverso la documentazione acquisita in fase di qualidicazione o accreditamento ed in corso d'opera, secondo le previsioni delle norme di rife-

rimento di ciascun elenco, per accertare l'effettiva e corretta applicazione, nel tempo, dei sistemi, delle regole e delle procedure definite e documentate per l'erogazione dei servizi.

verifica ispettiva: esame sistematico ed indipendente, conseguente alla verifica documentale, svolto sul campo per accertare l'effettiva e corretta applicazione, nel tempo, dei sistemi, delle regole e delle procedure definite e documentate per l'erogazione dei servizi.

vigilanza:funzione prevista all'art. 14-bis, comma 2, lettera i) del Codice dell'Amministrazione Digitale svolta sui soggetti iscritti negli elenchi pubblici di fiducia di cui all'art. 29 del CAD secondo le modalità indicate nelle norme di riferimento.

2 PREMESSA

In relazione alle previsioni indicate all'art. 14-bis, comma 2, lettera i) del Codice dell'Amministrazione Digitale l'Agenzia per l'Italia Digitale svolge funzioni di "*vigilanza sui servizi fiduciari ai sensi dell'articolo 17 del Regolamento UE 910/2014 in qualità di organismo a tal fine designato, sui gestori di posta elettronica certificata, sui soggetti di cui all'art. 44-bis, nonché sui soggetti pubblici e privati, che partecipano a SPID di cui all'art. 64*; *nell'esercizio di tale funzione l'Agenzia può irrogare per le violazioni accertate a carico dei soggetti vigilati le sanzioni amministrative di cui all'articolo 32-bis in relazione alla gravità della violazione accertata e all'entità del danno provocato all'utenza*". A norma dell'art. 17 del Regolamento UE 910/2014, l'organismo vigilante designato in uno Stato membro "*è responsabile di compiti di vigilanza nello Stato membro designante*"; ad esso "*sono conferiti i poteri necessari e le risorse adeguate*" per l'esercizio dei loro compiti.

I prestatori dei servizi di cui sopra, sottoposti alle attività di vigilanza, sono i soggetti iscritti negli elenchi pubblici di fiducia tenuti da AgID ai sensi dell'art. 29 del CAD e consultabili per via telematica. Per ciascuna tipologia di elenco trovano applicazione le specifiche norme di riferimento che, insieme alle norme sopra richiamate, definiscono gli obblighi dei gestori nell'erogazione dei servizi previsti e rispetto ai quali si esplicano le funzioni di vigilanza.

La vigilanza è il complesso di attività volte a verificare la persistenza, nel tempo, in capo a ciascun gestore, dei requisiti previsti per la qualificazione o l'accreditamento nonché la conformità del modo di operare alle norme di riferimento; oltre all'accertamento delle violazioni, ha lo scopo di rilevare in corso d'opera situazioni potenzialmente critiche o non conformi, al fine di sollecitare il gestore ad intraprendere le opportune azioni correttive o migliorative. Ha inoltre lo scopo di favorire il miglioramento continuo dei processi di erogazione dei servizi agli utenti finali e delle regole che li governano.

A prescindere dalle caratteristiche di ciascuna tipologia di elenco, la vigilanza è svolta sia con verifiche condotte su base documentale, attraverso la raccolta e l'esame dei documenti o delle informazioni di riepilogo dovuti dal soggetto qualificato/accreditato, sia attraverso l'esecuzione di verifiche ispettive presso i gestori.

3 APPLICABILITÀ

I contenuti del presente documento si applicano ai fini dell'esecuzione delle attività di vigilanza "ex post" sui prestatori di servizi fiduciari qualificati e sui certificatori di firma digitale accreditati in Italia, sui gestori di posta elettronica certificata accreditati, sui conservatori di documenti informatici accreditati di cui all'art. 44-bis del CAD, nonché sui soggetti pubblici e privati che partecipano a SpID di cui all'art. 64 del CAD.

Il documento può essere modificato al variare delle norme o a fronte di nuove esigenze, essendo nelle facoltà di AgID richiedere al soggetto qualificato o accreditato ogni ulteriore documento correlato all'espletamento del processo di gestione dei servizi che consideri necessario per poter svolgere le previste funzioni di vigilanza.

4 OBIETTIVI DELLE VERIFICHE

Tutte le verifiche eseguite in fase di vigilanza hanno lo scopo di accertare l'effettiva e corretta applicazione, nel tempo, dei sistemi, delle regole e delle procedure definite e documentate per l'erogazione dei servizi propri di ciascun elenco, valutandone, inoltre, l'adeguatezza in funzione delle esigenze evolutive in itinere.

Situazioni frequenti di violazioni normative, procedure o regole disattese o scostamenti ripetuti rispetto ai livelli di prestazioni previsti sono indice di degrado delle capacità tecniche dimostrate in fase di qualificazione/accreditamento e possono comportare l'adozione delle conseguenti azioni, inclusa l'irrogazione di sanzioni amministrative ai sensi dell'art. 32-bis del CAD.

Le verifiche sono finalizzate a rilevare:

- eventuali situazioni di non conformità su cui è necessario attivare tempestivamente azioni correttive;
- eventuali aree di criticità sulle quali occorre intervenire in via preventiva;
- l'evidenza di opportunità di interventi migliorativi.

5 PROGRAMMAZIONE DELLE VERIFICHE

Le verifiche su base documentale sono sono svolte in via continuativa e prendono in esame la documentazione di riscontro prevista nelle norme di riferimento per ciascun elenco, richiamate al § 10.

Le verifiche ispettive, in linea generale, sono programmate sulla base di eventi che, a titolo non esaustivo, includono:

- risultati delle verifiche condotte sui documenti di riferimento (cfr. § 6);
- esigenza di acquisire evidenze aggiuntive che richiedano audit ad hoc;
- notifiche relative a disservizi o violazioni di sicurezza o perdita di integrità;
- segnalazioni o richieste da utenti, altri operatori, amministrazioni o autorità nazionali;
- richieste da altri organismi di vigilanza o istituzioni europee (per quanto riguarda i servizi fiduciari qualificati)
- esiti di verifiche precedenti.

Le verifiche possono essere disposte anche in via estemporanea, a fronte di eventi o situazioni contingenti. Il processo per la conduzione delle verifiche ispettive è descritto al § 6.

6 DOCUMENTI DI RIFERIMENTO E METODI DI RISCONTRO

6.1 DOCUMENTI DI RIFERIMENTO A CARICO DEL SOGGETTO QUALIFICATO/ACCREDITATO

Le verifiche su base documentale sono condotte con riferimento alla seguente documentazione:

a. documenti depositati presso AgID ai fini della qualificazione o dell'accreditamento, indicati nelle norme di riferimento per ciascun elenco e ogni successivo aggiornamento a fronte di modifiche intervenute, che il soggetto qualificato/accreditato è obbligato a trasmettere ai sensi della stessa normativa.

b. documenti di riscontro indicati nelle norme. A titolo di esempio:

    1. CAR biennali;

2. piani di cessazione (art. 24, comma 2, lett. i) del Regolamento eIDAS)
3. rapporti periodici di riepilogo delle attività svolte;
4. certificati di rinnovo delle certificazioni ISO/IEC 27001, ISO 9001 e documentazione contenente le risultanze delle verifiche periodiche di mantenimento;
5. ogni altro documento correlato all'espletamento dei processi di erogazione dei servizi che AgID ha facoltà di richiedere.

Oltre alla documentazione indicata ai precedenti punti a) e b), le verifiche ispettive prendono in esame le registrazioni delle attività svolte in esecuzione delle procedure indicate nei manuali (Manuale operativo o equivalente), nel Piano della sicurezza e nell'ulteriore documentazione relativa ai sistemi utilizzati per l'erogazione dei servizi. Dette registrazioni, a titolo di esempio, includono:

c. i risultati generati dai processi, svolti secondo le procedure previste nell'ambito della documentazione del sistema. Tali risultati possono consistere in documenti, aggiornamenti di archivi, azioni, verbali, …;
d. documenti contenenti i risultati di verifiche ispettive interne o di audit di terza parte se previste dai sistemi di gestione della qualità e dai sistemi di gestione della sicurezza adottati dal soggetto qualificato/accreditato;
e. ogni fatto (documento, azione, …) che dimostri l'effettiva e corretta applicazione, nel tempo, dei sistemi, delle regole e delle procedure definite e documentate per l'erogazione dei servizi a norma.

6.2 DOCUMENTI DI RIFERIMENTO E STRUMENTI DI SUPPORTO PER IL VERIFICATORE

Il verificatore effettua le verifiche documentali e le verifiche ispettive basandosi sulla documentazione di cui al §6.1.

Sono, inoltre, documenti di riferimento per le valutazioni il complesso delle norme e degli standard di riferimento indicati nelle norme specialistiche di ciascun elenco.

Per l'esecuzione delle verifiche il verificatore utilizza apposite liste di riscontro (*check list*), contenenti i principali requisiti previsti dalle norme di riferimento rispetto ai quali sono condotte le valutazioni.

7 IL PROCESSO PER L'ESECUZIONE DI VERIFICHE ISPETTIVE

Le verifiche ispettive sono condotte di regola secondo i principi della norma UNI EN ISO 19011:2012 e s.m.i.

Il processo di verifica è articolato in tre fasi: pianificazione della verifica, esecuzione, documentazione ed azioni conseguenti. L'esecuzione della verifica può consistere in ispezioni sul posto, presso le sedi del gestore, ovvero, in funzione degli obiettivi che si intendono perseguire attraverso la verifica, in incontri attraverso sistemi di videoconferenza, nei casi possibili.

7.1 PIANIFICAZIONE DELLA VERIFICA

Per ciascuna verifica ispettiva, programmata o disposta in via estemporanea, si predispone, a seguito dell'esame preliminare della documentazione di riferimento un piano di verifica.

Il piano indica:

a. obiettivi e campo della verifica (elementi del sistema o componenti dei servizi o prodotti che saranno oggetto di verifica);
b. documenti di riferimento e tipologie di documenti di riscontro che dovranno essere esibiti nel corso della visita, con riferimento alle tipologie previste al § 6.1;
c. data di inizio delle attività di verifica e modalità di svolgimento;
d. stima del tempo e della durata delle attività;
e. composizione del gruppo di verifica, con indicazione di eventuali accompagnatori.

Il piano di verifica è trasmesso almeno 48 ore prima della data prevista di inizio delle attività di verifica. In casi particolari, a discrezione di AgID, il piano di verifica è comunicato 24 ore prima dell'inizio attività.

A completamento della fase di pianificazione, il gruppo di verifica predispone i documenti di lavoro, che possono comprendere liste di riscontro, piani di campionamento e moduli per la registrazione delle informazioni, delle risultanze della verifica e delle riunioni.

7.2 ESECUZIONE DELLA VERIFICA

Il momento di inizio delle attività è ufficializzato in un incontro del gruppo di verifica con un Responsabile del soggetto sottoposto a verifica o con persona da questi formalmente incaricata; ove appropriato, a discrezione del Responsabile, partecipano all'incontro i responsabili delle funzioni o dei processi da sottoporre a verifica.

Lo scopo della riunione di apertura è di riepilogare il piano, fornire una breve sintesi di come verranno eseguite le attività, confermare i canali di comunicazione.

Le evidenze raccolte che indichino un rischio immediato e significativo sono riportate tempestivamente all'organizzazione oggetto di verifica.

Nel corso della verifica si provvede a raccogliere e verificare le informazioni. Solo le informazioni verificabili possono costituire evidenze e sono oggetto di registrazione. I metodi per raccogliere informazioni comprendono:

- interviste;
- compilazione di liste di riscontro;
- osservazione di attività;
- riesame dei documenti.

A conclusione delle attività, si presentano le risultanze e le conclusioni della verifica. Essi possono indicare punti di forza, rilievi o raccomandazioni per il miglioramento. Sono discusse e, se possibile risolte, eventuali divergenze di opinione e, in caso di mancato accordo, tutte le opinioni sono registrate.

7.3 CLASSIFICAZIONE DEI RILIEVI

I rilievi possono derivare sia da verifiche svolte su base documentale, sia dalle verifiche ispettive. Sono distinti in Osservazione e Non Conformità, queste ultime classificate secondo livelli di gravità decrescente (grave). La classificazione è la seguente:

Osservazione: commenti o proposte finalizzati al miglioramento dei documenti o delle modalità operative. É richiesto al gestore di indicare le azioni ed i tempi necessari per adeguarsi, salvo i casi di motivate obiezioni.

Non Conformità Lieve; irregolarità che non ingenera presupposti di non conformità per continuare l'erogazione del servizio, risolvibili attraverso specifiche azioni correttive attuate secondo tempi prestabiliti (al massimo entro 90 giorni), pena la conversione automatica in livello Grave.

Non Conformità Intermedia: irregolarità che non ingenera presupposti di non conformità per continuare l'erogazione del servizio, che va risolta con specifiche azioni correttive attuate secondo tempi prestabiliti (al massimo entro 30 giorni), pena la conversione automatica in livello Grave.

Non Conformità Grave: irregolarità che generano significativi dubbi sulla capacità di erogare il servizio nel rispetto dei requisiti previsti (violazioni della normativa; totale assenza di documentazione o applicazione di uno o più requisiti; insieme di Non Conformità "Intermedie" o "Lievi" riconducibili ad un singolo elemento della normativa, indicante quindi una inadeguata applicazione del sistema relativamente a questo elemento). Va risolta con specifiche azioni correttive attuate secondo tempi stringenti (al massimo entro 7 giorni), pena l'attivazione della procedura per la comminazione di sanzioni o la cancellazione dall'elenco.

7.4 DOCUMENTAZIONE DEI RISULTATI ED AZIONI CONSEGUENTI

Il rapporto di verifica fornisce una completa registrazione delle attività svolte. Include o fa riferimento, quando appropriato, a:

a. piano della verifica
b. elenco dei rappresentanti dell'organizzazione oggetto di verifica
c. elenco della documentazione esaminata
d. sintesi del processo di verifica comprendente incertezze o eventuali ostacoli incontrati
e. eventuali aree non coperte
f. eventuali opinioni divergenti non risolte tra il gruppo di verifica e l'organizzazione
g. eventuali osservazioni, non conformità o raccomandazioni per il miglioramento
h. piani concordati delle azioni successive, se ce ne sono
i. lista di distribuzione del rapporto di verifica

Il rapporto, riesaminato nell'ambito della struttura AgID preposta alla vigilanza, è distribuito ai destinatari di cui alla precedente lettera i).

La verifica è completata quando tutte le attività descritte nel piano sono state attuate e il rapporto di verifica approvato è stato distribuito.

Le conclusioni della verifica possono indicare l'esigenza di azioni correttive, preventive e di miglioramento. Tali azioni sono decise ed effettuate dall'organizzazione oggetto di verifica secondo modalità e tempistiche in grado di rimuovere le non conformità o di implementare le varianti a scopo preventivo o migliorativo secondo tempi coerenti con quanto indicato nel rapporto di verifica. In caso di non conformità, le azioni correttive ed i relativi tempi di attuazione sono coerenti con i tempi massimi previsti in funzione del livello di gravità, indicati al § 7.3, e risultano da un piano di rientro, che il soggetto accreditato trasmette tempestivamente ad AgID per le azioni di verifica conseguenti.

Il completamento e l'efficacia delle azioni correttive e delle ulteriori azioni preventive o migliorative costituiscono oggetto di una nuova verifica.

8 GESTIONE DELLE COMUNICAZIONI E DELLA DOCUMENTAZIONE

Le comunicazioni finalizzate all'esecuzione delle verifiche e la trasmissione dei documenti a carico del gestore sono effettuate a mezzo PEC, salvo i casi di documenti che non possono essere divulgati all'esterno dell'organizzazione e che sono consultabili presso il gestore. La trasmissione dei documenti in formato elettronico è eseguita secondo le procedure definite dal gestore per la protezione dei dati e delle informazioni, ovvero secondo le indicazioni fornite da AgID per la trasmissione di documenti riservati.

I rapporti di verifica e le ulteriori registrazioni delle attività di verifica, che possono includere verbali riunioni, liste di controllo compilate, documentazione raccolta in fase di ispezione, sono conservati da AgID nel rispetto della normativa in vigore.

9 AZIONI CONSEGUENTI ALLE VERIFICHE

Le "Non Conformità" dovranno risolte entro i tempi massimi previsti in relazione al livello di gravità attribuito, pena la conversione automatica nel livello superiore. Per le "Non Conformità" di livello massimo ("Grave"), decorso il tempo stabilito senza che sia fornita evidenza dell'avvenuta risoluzione, si attiva il procedimento sanzionatorio ai sensi dell'art. 32-bis del d. lgs. 82/2005 e s.m.i.. La sanzione è stabilita con provvedimento motivato del Direttore Generale, sentito il Comitato di indirizzo, ed è commisurata alla gravità della violazione accertata e all'entità del danno provocato all'utenza, per importi da un minimo di euro 4.000,00 a un massimo di euro 40.000,00, fermo restando il diritto al risarcimento del maggior danno. Nei casi di particolare gravità AgID può disporre la cancellazione del soggetto dall'elenco dei soggetti qualificati.

Al permanere delle situazioni di non conformità ed ai provvedimenti sanzionatori adottati è data pubblicità attraverso le pagine del sito istituzionale.

10 ALLEGATO 1 - NORME DI RIFERIMENTO

10.1 ELENCO DEI CERTIFICATORI DI FIRMA DIGITALE ACCREDITATI IN ITALIA E DEI PRESTATORI DI SERVIZI FIDUCIARI QUALIFICATI

a) Decreto legislativo 7 marzo 2015, n. 82 e s.m.i. (Codice dell'amministrazione digitale)

b) 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 e che abroga la direttiva 1999/93/CE e relativi atti di esecuzione, tra i quali:

- Decisione di esecuzione 2015-1505 8 settembre 2015
- Decisione di esecuzione 2015-1506 8 settembre 2015
- Decisione di esecuzione 2015-1984 3 novembre 2015
- Decisione di esecuzione 2016-650 25 aprile 2016
- Regolamento di esecuzione 2015-806 22 maggio 2015_marchio di fiducia UE
- Regolamento di esecuzione 2015-806 22 maggio 2015_marchio di fiducia UE
- Regolamento di esecuzione 2015-1502 8 settembre 2015_livelli di garanzia

10.2 ELENCO DEI CONSERVATORI ACCREDITATI

a) Decreto legislativo 7 marzo 2015, n. 82 e s.m.i. (Codice dell'amministrazione digitale)

b) 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 e che abroga la direttiva 1999/93/CE e relativi atti di esecuzione applicabili

c) DPCM del 3 dicembre 2013 (G.U. n. 59 del 12-3-2014 – Suppl. Ordinario n. 20) - "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1 del Codice dell'amministrazione digitale"

d) Circolare Agid n.65/2014 (G.U. n. 89 del 16/04/2014) – "Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82" e documenti/norme richiamati, tra i quali in particolare il documento "Requisiti di qualità e sicurezza per l'accreditamento e la vigilanza"

e) Linee Guida sulla conservazione dei documenti informatici

f) Istruzioni per la conservazione dei log dei messaggi e dei messaggi di posta elettronica certificata con virus (luglio 2016)

10.3 ELENCO DEI GESTORI DI POSTA ELETTRONICA CERTIFICATA ACCREDITATI

a) Decreto legislativo 7 marzo 2015, n. 82 e s.m.i. (Codice dell'amministrazione digitale)

b) 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 e che abroga la direttiva 1999/93/CE e relativi atti di esecuzione applicabili

c) DPR 11 febbraio 2005, n. 68 (G.U. 28 marzo 2005, n. 97)) – " Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3").

d) Circolare 7 dicembre 2006, n. 51 - Espletamento della vigilanza e del controllo sulle attività esercitate dai Gestori di PEC

e) DM 2 novembre 2005 (Gazzetta Ufficiale n. 266 del 15-11-2005) – "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata"

f) "Linee Guida per la vigilanza sui Gestori PEC," pubblicate sul sito AgID

g) Istruzioni per la conservazione dei log dei messaggi e dei messaggi di posta elettronica certificata con virus (luglio 2016)

10.4 ELENCO DEI GESTORI DI IDENTITÀ DIGITALI SPID ACCREDITATI

a) Decreto legislativo 7 marzo 2015, n. 82 e s.m.i. (Codice dell'amministrazione digitale)

b) 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 e che abroga la direttiva 1999/93/CE e relativi atti di esecuzione applicabili

c) Regolamento recante le modalità per l'accreditamento e la vigilanza dei gestori dell'identità digitale (articolo 1, comma 1, lettera l) del DPCM 24 ottobre 2014)

d) Regolamento recante le modalità per la realizzazione dello SPID (articolo 4, comma 2 del DPCM 24 ottobre 2014)

e) Regolamento recante le regole tecniche (articolo 4, comma 2 del DPCM 24 ottobre 2014)

f) Regolamento recante le procedure per consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale ai sensi del DPCM 24 ottobre 2014.

g) Determinazione AgID N. 40/2016 – Modello Convenzione SPID tra AgID e Pubbliche Amministrazioni

h) Determinazione AgID N. 32/2016 – Modello Convenzione SPID tra AgID e Identity Provider

i) Determinazione AgID N. 16/2016- Pubblicazioni AVVISI SPID

j) Determinazione AgID N. 239/2016 – Modello Convenzione SPID tra AgID e privati in qualità di fornitori di servizi